Estonian Information Security Standard. Baseline Security Catalogue.

TABLE OF CONTENTS

ISMS: SECURITY GOVERNANCE 6

ISMS.1 Security Governance 6

ORP: ORGANISATSION AND PERSONNEL 16

ORP.1 Organisation of information security 16
ORP.2 Personnel 21
ORP.3 Raising awareness and providing training on information security 27
ORP.4 Management of identity and rights 32
ORP.5 Compliance management (requirements management) 40

CON: CONCEPTS AND METHODOLOGIES 44

CON.1 Cryptography concept 44
CON.2 Personal data protection 51
CON.3 Data backup concept 65
CON.6 Data erasure and destruction 72
CON.7 Information security for business trips 76
CON.8 Software development 84
CON.9 Exchange of information 94
CON.10 Web applications development 98

OPS: OPERATIONS 106

OPS.1 Own operations 106
OPS.1.1 Main IT operations 106
OPS.1.1.1 IT management in general 106
OPS.1.1.2 IT management 118
OPS.1.1.3 Patch and change management 127
OPS.1.1.4 Protection against malware 134
OPS.1.1.5 Logging 139
OPS.1.1.6 Software testing and onboarding 145
OPS.1.1.7 Systems management 150
OPS.1.2 Supporting operations 161
OPS.1.2.2 Archiving 161
OPS.1.2.4 Remote work 170
OPS.1.2.5 Remote maintenance 176
OPS.1.2.6 Synchronising clocks with the NTP server 184
OPS.2 Operations as a service 189
OPS.2.2 Using cloud services 189
OPS.2.3 Outsourcing 199
OPS.3 Operations of the service provider 210
OPS.3.2 Information security of the service provider 210

DER: DETECTION AND REACTION 220

DER.1 Detection of security incidents 220

DER.2 Management of security incidents 227
DER.2.1 Handling of security incidents 227
DER.2.2 Enabling computer forensics 235
DER.2.3 Resolution of large-scale security incidents 240
DER.3 Assessment of information security 246
DER.3.1 Audits and reviews 246
DER.3.2 Information security compliance audits 256
DER.4 Emergency management 262

INF: INFRASTRUCTURE 268

INF.1 The building in general 268
INF.2 Server room and data centre 281
INF.5 Technical infrastructure room or cabinet 291
INF.6 Data media archive 300
INF.7 Office workplace 304
INF.8 Home workplace 309
INF.9 Mobile workplace 313
INF.10 Meeting, event, and training rooms 320
INF.11 IT components of vehicles 325
INF.12 Cabling 332
INF.13 Technical building management 342
INF.14 Building automation and control systems 356

NET: NETWORKS AND COMMUNICATION 373

NET.1 Networks and communication 373
NET.1.1 Network architecture and solution 373
NET.1.2 Network management 386
NET.2 Wireless networks 395
NET.2.1 Operating wireless local area networks 395
NET.2.2 Using wireless local area networks 405
NET.3 Network components 409
NET.3.1 Routers and switches 409
NET.3.2 Firewall 418
NET.3.3 Virtual private network (VPN) 427
NET.3.4 Network access control (NAC) 432
NET.4 Communications 443
NET.4.1 Telephone exchange 443
NET.4.2 IP phone (VoIP) 451

SYS: IT SYSTEMS 458

SYS.1 Server 458
SYS.1.1 Server in general 458
SYS.1.2 Windows Server 471
SYS.1.2.2 Windows Server 2012 471

SYS.1.2.3 Windows Server 477
SYS.1.3 Linux and Unix server 481
SYS.1.5 Virtualisation system 485
SYS.1.6 Containerisation 494
SYS.1.8 Storage solutions 504
SYS.1.9 Terminal server 513
SYS.2 Client computers 523
SYS.2.1 Client computer in general 523
SYS.2.2 Windows clients 537
SYS.2.2.3 Windows 10 client 537
SYS.2.3 Linux and Unix client 545
SYS.2.4 macOS client 550
SYS.3 Mobile devices 556
SYS.3.1 Laptop computers 556
SYS.3.2 Smartphones and tablets 563
SYS.3.2.1 Smartphones and tablets in general 563
SYS.3.2.2 Mobile device management (MDM) 574
SYS.3.2.3 iOS of the organisation 580
SYS.3.2.4 Android 585
SYS.3.3 Mobile phone 588
SYS.4 Other systems 596
SYS.4.1 Printer and multifunction printer 596
SYS.4.3 Embedded systems 604
SYS.4.4 Device in the Internet of Things (IoT) in general 613
SYS.4.5 Removable data media 622
SYS.EE Estonian IT systems 628
SYS.EE.1 X-tee security server 628
SYS.EE.2 eID components 638

APP: APPLICATIONS 648

APP.1 Client applications 648
APP.1.1 Office software 648
APP.1.2 Web browser 653
APP.1.4 Mobile applications (apps) 658
APP.2 Directory services 663
APP.2.1 Directory service in general 663
APP.2.2 Active Directory 670
APP.2.3 OpenLDAP 680
APP.3 Network services 683
APP.3.1 Web applications 684
APP.3.2 Web server 689
APP.3.3 File server 696
APP.3.4 Samba 701
APP.3.6 DNS server 706

APP.4 Business applications 714
APP.4.3 Database systems 714
APP.4.4 Kubernetes 721
APP.5 Group software 729
APP.5.2 Microsoft Exchange and Outlook 729
APP.5.3 Email server and client in general 734
APP.5.4 Unified communications and collaborations (UCC) 741
APP.6 Software in general 751
APP.7 Custom software development 759
APP.EE Estonian applications 765
APP.EE.1 X-tee data service 765

IND: INDUSTRIAL IT 774

IND.1 Operational technology. Process control and automation technology 774
IND.2 Industrial control system 788
IND.2.1 Components of an industrial control system in general 788
IND.2.2 Programmable logic controllers 794
IND.2.3 Sensors and actuators 796
IND.2.4 Robot devices 798
IND.2.7 Safety automation 800
IND.3 Operational technology networks 805
IND.3.2 Remote maintenance of operational technology components 805

ISMS: SECURITY GOVERNANCE

ISMS.1 Security Governance

1 Description

1.1 Purpose

To propose measures to establish and improve the Information Security Management System (ISMS). To provide guidance on the development of a security concept.

1.2 Responsibility

The information security manager is responsible for security governance measures.
Additional responsible persons: The management of the organisation, the director.

1.3 Limitations

The module is based on the baseline security methodology and the requirements document of the Estonian Information Security Standard (Estonian Information Security Standard. Requirements). Personnel measures related to information security are addressed in the module ORP.2 Personnel.

2 Threats

2.1 Lack of personal responsibility in the security process

If the security process of an organisation does not define the job responsibilities with sufficient precision, the employee lacks personal responsibility for information security. In most cases, employees avoid additional responsibilities, which means that security measures are not implemented.

2.2 Lack of support from the management of the organisation

If the information security manager is not part of the management of the organisation, it is difficult for them to demand the implementation of information security measures from those in a more senior position. Employees will not comply with information security requirements if the management does not lead by example.

2.3 Inadequate plan to implement the information security strategy

The strategic objectives contained in the security concept may be seen as a mere declaration of intent, and insufficient resources are allocated to their implementation.

2.4 Sub-optimal investments

In situations where the management of the organisation is not aware of the situation of information security, adequate resources for information security are either not allocated or not used in the best way. Shortcomings in resource allocation can lead to over-investment in one area while there are resource constraints in other areas. Excessively expensive and complex technical security solutions can create new security weaknesses.

2.5 Failure to implement security measures

If an organisation has not set clear information security objectives, the need for information security in the organisation can be interpreted in many ways. If information security is not considered necessary or important enough, security measures will not be implemented.

2.6 Failure to update the security process

If the organisation does not continually invest in reviewing and improving its security process, the level of security of the organisation will decline or slowly be replaced by a dangerous semblance of security. The organisation's resilience to new information security threats is therefore reduced.

2.7 Non-compliance with laws and contracts

If the employees of an organisation lack knowledge of the law, they may inadvertently breach its requirements. Failure to comply with the security terms and conditions set out in contracts may result in contractual penalties or even the termination of the contract and of business relations.

2.8 Security incidents that disrupt business processes

A security event (often compounded by a bad coincidence of circumstances) can trigger a security incident that has a negative impact on the organisation's critical business processes. Even if the security incident does not become public knowledge, it can have a detrimental effect on relationships with business partners and clients.

2.9 Inefficient use of resources due to inadequate security governance

In the case of uneven and uncoordinated implementation of security products, money and manpower are used inefficiently. Inadequate security governance can mean that the processes that bring the most added value to the organisation are left without adequate investment in information security.

3 Measures

3.1 Life cycle

Planning

ISMS.1.M1 Assumption of overall responsibility for information security at the management level

Implementation

ISMS.1.M2 Security objectives and security strategy

ISMS.1.M3 Information Security Policy

ISMS.1.M4 Appointment of the information security manager

ISMS.1.M5 Contract for the services of an external information security manager

ISMS.1.M6 Establishment of the organisation of information security

ISMS.1.M7 Establishment of security measures

ISMS.1.M13 Documentation of the security process

Operation

ISMS.1.M8 Integration of employees into the security process

ISMS.1.M9 Integration of information security into cross-organisational processes

ISMS.1.M10 Security concept

ISMS.1.M11 Information security continuity

ISMS.1.M12 Information security reports to the management

ISMS.1.M15 Economic use of information security resources

ISMS.1.M16 Development of detailed security policies

Additional advanced measures

ISMS.1.M17 Conclusion of insurance contracts

3.2 Key measures

ISMS.1.M1 Assumption of overall responsibility for information security at the management level [management of the organisation]

a. The management of the organisation will take overall responsibility for the information security of the organisation. The management's commitment shall be visible and clearly understood by all concerned.
b. The management initiates the security process, manages and controls the process, and leads by example in the management of information security.
c. The management of the organisation shall:
- assign roles and tasks for information security;
- ensure the competence of information security employees;
- provide the necessary resources to perform the information security tasks.

d. The management of the organisation is regularly informed of the information security situation.

ISMS.1.M2 Security objectives and security strategy [management of the organisation]

a. Taking into account the organisation's objectives, business processes, and other relevant information, the management of the organisation determines the security objectives and the security strategy.
b. The security objectives and the security strategy are documented. The objectives shall be realistic, practical, justified, and understandable.
c. The management of the organisation regularly reviews the security strategy to ensure that it remains appropriate and up to date.

ISMS.1.M3 Information Security Policy [management of the organisation]

a. The management of the organisation clearly and unambiguously defines the information security network.
b. The management of the organisation approves and establishes the information security policy.
c. At a minimum, the information security policy shall include the following aspects:
- the importance and relevance of information security to the organisation;
- the key elements of the security strategy;
- the management's commitment;
- the organisational basis for implementing the security process;
- the principles for performance evaluation.

d. The information security policy connects the security objectives to the organisation's objectives in a way that is understandable and motivating for each employee.
e. The information security policy is communicated to all employees and partners of the

organisation, including the public where appropriate. Access to relevant information is granted to employees and partners only after acceptance of the policy.
f. The information security policy is updated regularly (at least annually) or in the event of significant changes to IT systems, organisational objectives, or security strategy.

ISMS.1.M4 Appointment of the information security manager [management of the organisation]

a. The management of the organisation appoints a person responsible for information security - the information security manager, whose responsibilities include:

- managing and coordinating the information security process;
- supporting the management in establishing information security policies;
- developing and coordinating security concept(s);
- enforcing information security policy (or policies) and measures;
- developing, initiating, and monitoring the implementation plan for security measures;
- keeping the management informed of the current situation of information security;
- coordinating information security projects;
- handling information security incidents;
- raising awareness on information security, organising trainings.

b. The management of the organisation ensures that the information security manager has the necessary conditions for their work and has access to information and facilities.
c. The information security manager has adequate professional qualifications and is provided with opportunities to update their knowledge.
d. In addition to professional skills, the competence and personal qualities of the information security manager are:

- knowledge of the organisation's objectives and business processes;
- ability to work collaboratively, teamwork skills;
- ability to work independently;
- willingness to develop professionally;
- assertiveness;
- experience in project management.

e. e. In the performance of their duties, the information security manager cooperates with the data protection specialist and external regulators.

f. The information security manager is involved in IT projects and in the development process of IT systems.

ISMS.1.M5 Contract for the services of an external information security manager [management of the organisation]

a. If the role of the information security manager cannot be fulfilled by in-house employees, the information security manager is procured as a service from outside the organisation.
b. The external information security manager shall have the necessary qualifications.
c. The service contract for the information security manager shall include the work tasks and the associated rights and obligations of the information security manager. At a minimum, the following shall be provided:

- qualification requirements;
- work tasks;
- minimum resources required to perform the tasks;
- notification and reporting chain, contact persons;
- workplaces, premises, presence- and availability times;
- access rights;
- reporting obligations;
- obligation to cooperate with the contracting authority.

d. A confidentiality agreement shall be concluded with the external information security manager.
e. The information security manager's service contract shall reflect the full life cycle of the contractual relationship, including:

- the procedures for the replacement of persons performing the work;
- the definition and resolution of conflicts of interest;
- the consequences of a breach of contract;
- the procedures for terminating the contractual relationship;
- the costs associated with the performance of the contract.

ISMS.1.M6 Establishment of the organisation of information security [management of the organisation]

a. The management of the organisation establishes the organisation of information security, defines the roles necessary to achieve the security objectives, provides the resources, and appoints suitably qualified persons to fulfil those roles.

b. The following professionals cooperate to manage the different aspects of information security:

- the information security manager;
- the head of IT;
- the managers of business units;
- the data protection specialist.

c. The security governance tasks are clearly articulated and responsibilities clearly defined.

d. Replacement procedures are in place for all individuals with a significant information security role.

e. Communication channels for the organisation of information security are planned, described, organised, and communicated. Role descriptions include who is to be notified of information security events and to what extent.

f. The suitability and effectiveness of the information security organisation is regularly reviewed and, if necessary, adapted to the changing circumstances.

ISMS.1.M7 Establishment of security measures

a. Security measures are defined based on the security objectives and the protection requirement and meet the following key requirements:

- the choice of security measures takes into account effectiveness, efficiency, and economic functionality;
- the choice of measures is justified and traceable to the underlying considerations;
- the persons responsible for the security measures are designated;
- the description of the implementation of the measure is provided with the level of detail required to fulfil the security task.

b. The security measures implemented are systematically documented, and the description of the implementation of the measure is updated as necessary.

c. In the case of a measure identified but not implemented:

- an additional risk analysis has been conducted to provide a basis for the management to accept or not accept the risk;
- the reason and the circumstances of non-implementation have been documented.

ISMS.1.M8 Integration of employees into the security process [director]

a. Employees are involved in the security process. Employees are aware of information security risks, familiar with the security measures, and able to comply with them in their work.

b. Employees are able to participate in the design and implementation of security measures.
c. Employees are made aware of the need to implement the measures prior to the enforcement of security policies and security measures.
d. The implementation of security measures has the least possible impact on the day-to-day tasks of employees.
e. Employees are informed of the potential consequences of non-compliance with information security policies and security measures.

ISMS.1.M9 Integration of information security into cross-organisational processes [management of the organisation]

a. Information security is embedded in all business and support processes of the organisation, and business process assets have designated responsible persons to implement information security measures.
b. Information security considerations are taken into account both when introducing new business processes and when modifying existing business processes.
c. The information security governance within the organisation is consistent with other areas related to security and risk management.
d. The information security manager is involved at all times and to the extent necessary in sectoral decisions involving information security.

ISMS.1.M10 Security concept

a. A security concept has been developed to implement the information security strategy and to meet the information security objectives. The security concept is the underlying document of the security process. The organisation may have several different security concepts in place at the same time, applicable to different parts of the organisation.
b. The security concept takes into account the IT-dependent business processes and the risks that may negatively affect them.
c. At a minimum, the security concept defines the following:
- the information network and the assets within it;
- the business processes to be protected;
- the business processes and data protection requirements;
- the process for modelling the security measures (including priorities and sequence of measures, see ISMS.1.M7 Establishment of security measures);

- the organisation of the risk analysis;
- the obligation to document security processes;
- the organisation of information security training;
- the organisation of information security reporting.

d. The security concept takes into account the relevant normative documents and the legislation.

ISMS.1.M11 Information security continuity

a. The effectiveness, completeness, and timeliness of the security process, security concept, information security policy, and information security organisation is regularly reviewed.
b. Regular security reviews are planned to identify who will perform the audit, when, and which specific areas and security measures will be audited. The reviews are conducted by appropriately qualified and independent persons.
c. In addition to regular security reviews, security measures and the security concept are reviewed on a case-by-case basis when:

- new business processes, applications, and IT components are added;
- significant infrastructure changes are made;
- major organisational changes are implemented;
- threats change significantly;
- significant vulnerabilities or incidents occur.

d. The results of the security review are documented and the reasons for discrepancies explained. Corrective actions to address deficiencies identified during the review are documented.
e. The discovered deficiencies are rectified, and if necessary, security measures or the security concept are adjusted.

ISMS.1.M12 Information security reports to the management [management of the organisation]

a. Regular reports are provided to the management on the information security situation, in particular on the risk situation and the effectiveness and efficiency of the security process.
b. In addition, an information security report is provided on an event-by-event basis, for example after a security incident or at a critical point in the security process.
c. The reports to the management include relevant and pertinent information, issues, progress, and opportunities for improvement. The reports also include proposals for improvement, with priorities and estimates of time and workload for the implementation.

d. Decisions by the management to modify security measures, residual risks, and security processes are documented in a traceable way.

ISMS.1.M13 Documentation of the security process

a. Procedures, key decisions, and results of the security process are documented. In particular, the following is documented:

- the reports to the management (see ISMS.1.M12 Information security reports to the management);
- the documentation on the organisation of the security process;
- the documentation on security activities;
- the documentation on security incidents;
- the technical documentation (for example, technical manuals, test results, application licences);
- the process guides for employees.

b. A set of rules is in place for the preparation and maintenance of documentation and for ensuring that it is kept up to date and confidential.
c. Current versions of existing documentation are readily available to the intended readership. Previous versions of the same documents are archived and accessible in one place.

ISMS.1.M15 Economic use of information security resources [management of the organisation]

a. The use of information security resources takes into account the economic aspects. The resource requirements for security measures are quantified.
b. The management of the organisation allocates the necessary information security resources (money, workforce, tools).
c. Resources planned for information security are available in a timely manner. Employees have sufficient time and opportunities to perform security-related tasks.
d. Additional employees can be added at peak times or for specific tasks.

3.3 Standard measures

ISMS.1.M16 Development of detailed security policies

a. Security policies with a narrower scope are drawn up at least in the following areas:

- network management;
- firewall management;

- anti-malware;
- data backup and archiving;
- email and groupware;
- use of mobile devices;
- outsourcing services.

3.4 Advanced measures

ISMS.1.M17 Conclusion of insurance contracts (A)

a. As part of the residual risk assessment, the need for the following types of insurance has been assessed:
- insurance against damage from fire and natural forces;
- financial loss insurance;
- property insurance;
- accident insurance;
- liability insurance;
- civil liability insurance.

b. The functionality and effectiveness of existing insurance contracts is regularly reviewed.

ORP: ORGANISATSION AND PERSONNEL

ORP.1 Organisation of information security

1 Description

1.1 Purpose

To provide measures for aligning the arrangement of information security within the organisation and to manage and maintain information security. The module regulates the management of information security processes and the division of information security roles within an organisation.

1.2 Responsibility

The management of an organisation is responsible for the implementation of the measures of the module 'Organisation of information security'.
Additional responsible persons: The user, technical department, IT department, head of information security, employees.

1.3 Limitations

The module deals with the general measures for the organisation of security. Additional organisational measures are presented in the modules with a narrower scope.

2 Threats

2.1 Missing or inadequate regulations

If information security measures are not in place or if the instructions for implementing the measures are not clearly documented, the necessary security measures will remain essentially unimplemented. Inadequate regulations and a lack of accountability can lead to major losses. This is especially the case in situations that require immediate action. Problems are also caused by regulations that are not kept up to date, do not reflect reality, or are presented in an incomprehensible way.

2.2 Breach of the regulations

Failure by an employee to comply with the established regulations may compromise the confidentiality, integrity, or availability of information, business processes, or IT systems. Depending on the protection requirements of the information or systems and the access rights granted to the violator of the security regulations, the damage may be extensive. Failure to comply with the requirements for data processing may result in data loss. Failure to comply with access rights management procedures may result in unauthorised access to IT systems.

2.3 Missing, inappropriate, or incompatible tools

The absence of the necessary tools as well as broken or obsolete tools can significantly hamper an organisation's business processes. For example, the battery of a UPS (uninterruptable power supply) loses some of its capacity over time and is not able to ensure power supply for IT devices in the event of a power cut. When tools are acquired, new tools may be incompatible with the older existing technological environment.

2.4 Hazards due to auxiliary and external personnel

Persons from outside the organisation cannot be expected by default to use the information and IT resources available to them in accordance with the organisation's procedures. Visitors, cleaners, and other external employees can compromise information security, business processes, and systems in a number of ways, from the inappropriate use of technical tools and probing of the IT system's capabilities to the theft of documents and IT resources.

3 Measures

3.1 Life cycle

Planning

ORP.1.M1	Establishment of responsibilities and regulations
ORP.1.M2	Designation of the persons responsible for information, applications, and IT components
ORP.1.M4	Separation of operational and control responsibilities
ORP.1.M16	Regulations for the secure use of IT resources

Operation

ORP.1.M3	Supervising or accompanying persons from outside the organisation
ORP.1.M15	Contact person for information security
ORP.1.M13	Relocation security

Implementation

ORP.1.M8	Management of tools and equipment

Additional advanced measures

ORP.1.M17	Restrictions on carrying smart phones

3.2 Key measures

ORP.1.M1 Establishment of responsibilities and regulations

a. The organisation has established tasks and responsibilities related to information security.
b. The regulations establish the organisation of security in at least the following areas:

- backup and archiving;
- handling data media;
- maintenance and repair;

- data protection;
- emergency response.

c. The regulations are introduced to all employees and reviewed regularly.

ORP.1.M2 Designation of the persons responsible for information, applications, and IT components [management of the organisation]

a. Security officers are assigned for all information and for all business processes, applications, and IT components.
b. Responsibilities for the implementation of information security measures are clearly articulated and determined, and the implementation of measures is regularly monitored.
c. Employees know who is responsible for implementing information security measures and how.

ORP.1.M3 Supervising or accompanying persons from outside the organisation [employee, administrative department]

a. Persons from outside the organisation move around the organisation's premises with an employee accompanying them.
b. The presence of external employees in areas with a high protection requirement is permitted only under the direct supervision of an employee of the organisation.
c. Employees are instructed not to leave persons from outside the organisation on the premises of the organisation without supervision.

ORP.1.M4 Separation of operational and control responsibilities

a. The separation of the roles of a person who performs an information security operation and a person who monitors the operation is ensured within the organisation; these tasks are performed by separate individuals.
b. The separation of operational and monitoring responsibilities also applies when an employee is replaced.

ORP.1.M15 Contact person for information security [information security officer]

a. The organisation has a designated person (or several) for dealing with security issues, whom employees can contact in the event of any information security problems.
b. Employees are encouraged to report suspected security incidents immediately, and if necessary,

anonymously.
c. The contact person for information security and the means of reporting are known to all employees or, if necessary, easily accessible.

3.3 Standard measures

ORP.1.M8 Management of tools and equipment [IT department]

a. The organisation has an overview of all the tools and equipment that may have an impact on the information security situation. In addition to IT systems and industrial automation components, the equipment includes Internet of Things (IoT) devices.
b. Compatibility and security is taken into account when procuring tools and equipment. Wherever possible, new equipment is tested before it is purchased.
c. Tools and equipment (including their consumables, associated software, data media, etc.) are accounted for (for example, in the asset register).
d. Instructions are drawn up for the safe disposal of tools and equipment and the necessary tools (for example, document compressor) are purchased. The disposal of data media is carried out in accordance with module CON.6. Data erasure and destruction.

ORP.1.M16 Regulations for the secure use of IT resources [information security manager, user]

a. The organisation has regulations in place on the secure use of IT resources.
b. The regulations on the secure use of IT resources include at least the following:
- the organisation's security objectives;
- the important terms and their explanations;
- the information security roles and work tasks;
- the contact persons for information security contacts and the information routes;
- the security measures to be implemented.

c. The regulations on the secure use of IT resources are made known to all employees and are easily accessible (for example, on the intraweb) where necessary.
d. New employees confirm in writing that they have read the regulations before taking up the use of IT resources.
e. The regulations for the secure use of IT resources are reviewed periodically and after significant changes to the IT systems.

ORP.1.M13 Relocation security [IT management, technical department, administrative department]

a. Before a planned move, a relocation plan is developed or updated, which, among other things, defines the responsibilities of the employees.
b. Employees are informed of the security measures to be followed before, during, and after the move.
c. Data is backed up and assets to be moved are labelled before the relocation.
d. During the relocation, access controls are implemented, with external employees moving at the point of departure and destination only in the company of the employees of the organisation.
e. After the relocation, it is verified that the equipment and other assets transported during the move are complete, undamaged, and unaltered upon arrival.
f. The necessary infrastructure is set up, IT and automation equipment is installed and tested, and user accounts are verified before employees relocate to their new location

3.4 Advanced measures

ORP.1.M17 Restrictions on carrying smart phones [administrative department, information security manager] (C)

a. Bringing mobile phones to confidential meetings and work places requiring a high level of security is prohibited.
b. If necessary, a detector is used for detecting mobile communication devices on people entering a secured area.

ORP.2 Personnel

1 Description

1.1 Purpose

To present measures to the human resources department and managers to ensure that their own employees and external employees act with the organisation's security objectives in mind.

1.2 Responsibility

The human resources department is responsible for the implementation of the measures of the document 'Personnel'.
Additional responsible persons: The IT department, the director.

1.3 Limitations

The measures covered in the module are generic. The personnel measures related to a specific function are presented in the relevant modules.

2 Threats

2.1 Personnel shortages

Personnel shortage in terms of numbers and qualifications leads to the impossibility of completing the required work tasks in a timely and comprehensive manner. The number of mistakes made through negligence increases.

2.2 Lack of knowledge of the requirements

If information security measures are not in place or if the instructions for implementing the measures are not clearly documented, the necessary security measures will remain essentially unimplemented. Unless all employees are made aware of the established policies and regulations, it cannot be expected for all employees to follow them.

2.3 Negligence in the use of data

Organisational and/or technical security measures set by the organisation may be ignored or circumvented for reasons of personal convenience or lack of concern. The use of the same passwords on social networks and in the working environment can lead to the misuse of the IT systems through password revocation. Manipulation or misuse of IT equipment and software can lead to sensitive data leaks or damage to the IT systems.

2.4 Insufficient employee qualifications

Many day-to-day IT problems and incidents are caused by the fact that employees are not sufficiently qualified to do the job or have received insufficient training. Due to outdated knowledge and poor computer skills, information security failures may not be detected, or abnormal software

behaviour may not be addressed in a timely manner. A person replacing another employee may skip an important activity in the work process or perform it incorrectly. This may cause the IT system to malfunction or cause an information security incident.

3 Measures

3.1 Life cycle

Planning

ORP.2.M1	Procedure for the onboarding of new employees
ORP.2.M2	Procedure for the departure of an employee
ORP.2.M14	Establishment of work tasks and responsibilities

Operation

ORP.2.M3	Procedure for the replacement of an employee
ORP.2.M4	Procedure for the replacement of an external employee
ORP.2.M5	Confidentiality agreement for the use of external employees
ORP.2.M15	Sufficiently qualified employees
ORP.2.M7	Verification of the reliability of a candidate

Additional advanced measures

ORP.2.M11	Security culture analysis
ORP.2.M13	Employee background checks

3.2 Key measures

ORP.2.M1 Procedure for the onboarding of new employees [director]

a. The onboarding procedure for new employees includes an introduction to information security requirements, practices, and codes of conduct.
b. A checklist has been drawn up containing all the activities required for a new employee to start working.
c. Day-to-day work procedures, information security measures and their impact on the business process, and the working environment are explained to the employees.
d. A mentor is assigned to the new employee for the onboarding period to assist with any issues that may arise.

ORP.2.M2 Procedure for the departure of an employee [director, IT department]

a. Before an employee leaves or is transferred to another post, a successor is trained. This is preferably done by the departing employee. If the tasks cannot be handed over directly, a detailed job description is created for the new employee.
b. The departing employee hands over to the organisation all documents, keys, and devices received during the period of employment, as well as their employment certificate and access cards.
c. The former employee's access rights to IT systems are revoked in a timely manner.
d. When an employee is transferred to another post, the employee's access rights and the range of organisational assets in their possession are adapted to their new tasks.
e. The obligation of confidentiality and the avoidance of potential conflicts of interest are once again explained to the employee in clear terms before leaving the post.
f. Relevant employees, including security personnel, are informed of the employee's departure.
g. Where necessary, contingency plans or other action plans which included the employee who is leaving or being transferred are updated.
h. An appropriate checklist is used to coordinate activities in the event of the departure of an employee, similarly to onboarding.

ORP.2.M3 Procedure for the replacement of an employee [director]

a. The management has drawn up a procedure for replacing employees and has put in place the conditions to comply with it. Replacement procedures are in place for work tasks in all relevant business processes.
b. The procedure for the replacement of an employee describes the allocation of tasks to be performed in the event of the replacement of an employee.
c. When appointing a replacement, it is ensured that they possess the necessary knowledge for the replacement. If necessary, the replacement is trained, and working procedures are documented in such a way that a person with less knowledge is able to carry out the replacement.
d. If, in exceptional circumstances, a competent replacement cannot be appointed and trained for a particular employee, a decision is taken as to whether an external replacement can be found.

ORP.2.M4 Procedure for the replacement of an external employee

a. When an external employee is used to replace an employee, they undertake to comply with the organisation's policies and internal regulations in the same way as the organisation's employees.

b. An external employee engaged for a short term or on a one-off basis is treated as a visitor who is not left alone in an area with protection requirements.
c. External employees recruited for a longer period of time are taught and trained to perform their duties in the same manner as the employees of the organisation. External employees are also subject to the procedure for the replacement of an employee (see ORP.2.M3 Procedure for the replacement of an employee).
d. When an external employee leaves the organisation, they hand over the results of their work and their access rights are revoked in the same way as those of an internal employee.

ORP.2.M5 Confidentiality agreement for the use of external employees

a. A written confidentiality agreement is concluded with a person from outside the organisation before they are given access to confidential information.
b. The confidentiality agreement specifies at least the following:
- what information is treated as confidential;
- what requirements apply to the use and disclosure of confidential information;
- the duration of the confidentiality agreement;
- how information ownership is regulated;
- the consequences for breaching the agreement.

ORP.2.M14 Establishment of work tasks and responsibilities [director]

a. All employees are explicitly committed to comply with the relevant legislation, organisational policies, and internal regulations.
b. The employee's tasks and responsibilities are documented and communicated to the employee. Employees confirm compliance with the requirements by signing the appropriate checklist.
c. Employees are aware that information obtained in the course of their work is for internal use only, unless otherwise indicated.
d. Employees are required to protect the organisation's assets and data after working hours and outside the organisation's premises.

ORP.2.M15 Sufficiently qualified employees [director]

a. Employees receive regular training and retraining appropriate to their activities.
b. Retraining for employees is encouraged and employees are motivated to continuously develop

their skills.
c. When recruiting new employees, the education, the qualifications, and the skills required are clearly described.
d. The suitability of employees for the post and the accuracy of the job descriptions and qualifications required for the post are periodically checked.

3.3 Standard measures

ORP.2.M7 Verification of the reliability of a candidate

a. Recruiters verify, with due diligence, the accuracy of the information provided by the candidate before recruitment.
b. Particular care is taken to check the completeness, credibility, and accuracy of the CV submitted. Relevant facts are verified by asking for and providing further evidence.

3.4 Advanced measures

ORP.2.M11 Security culture analysis (C-I-A)

a. Security measures are implemented taking into account the organisation's employees, their background, knowledge, and experience of using IT systems. Security is improved by analysing the security behaviour of employees.
b. A culture of trust and openness is fostered to ensure that security incidents are handled effectively and efficiently, so that such incidents are reported and resolved immediately.
c. In the case of a larger organisation, an analysis is carried out to determine whether the security culture may be affected by transnational, regional, or inter-unit cultural differences.

ORP.2.M13 Employee background checks (C-I-A)

a. In areas with high protection requirements, in addition to the basic employee background check (see ORP.2.M7 Verification of the reliability of a candidate), additional background checks are carried out to the extent permitted by the law, for example, by asking for confirmation of the absence of criminal convictions.
b. Applying for and working in certain positions is only allowed if the employee has applied for a personnel security clearance to state secrets in accordance with the applicable legislation.

ORP.3 Raising awareness and providing training on information security

1 Description

1.1 Purpose

To propose measures to raise awareness on security among employees and develop a training plan for employees, taking into account the specificities of the organisation and the knowledge and skills needed by the employees.

1.2 Responsibility

The information security manager is responsible for taking the measures for raising awareness on information security and training activities.
Additional responsible persons: The human resources department, the IT department, the management of the organisation, the director.

1.3 Limitations

The module ORP.3 Raising awareness and providing training on information security deals with the area of information security. For other topics, training is planned, scheduled, and conducted by the organisation's human resources department or the training coordinator.

2 Threats

2.1 Lack of knowledge of the requirements

A security incident is often caused by non-compliance with the security requirements. Security weaknesses resulting from a lack of knowledge of the requirements can compromise the confidentiality, availability, and integrity of the information being processed.

2.2 Lack of information security awareness

If employees are not sufficiently aware of information security measures, the organisation's security culture and compliance with security objectives will suffer. Employees are unable to make concrete

connections to their working environment because they are not made aware of the importance of security measures.

2.3 Low effectiveness of awareness and training

The reasons for the low effectiveness of awareness and training activities include lack of support from the management, unclear training objectives, shortcomings in the conduct of training, or a lack of resources. If the organisation does not give sufficient priority to raising awareness and training, low security awareness can directly hamper the performance of work tasks.

2.4 Inadequate training on security functions

Employees often fail to implement security applications and functions introduced in the organisation due to a lack of knowledge. A lack of knowledge of security functions can lead to software usage errors and downtime. The impact of misuse can be significant for critical IT systems.

2.5 Undetected security events

The day-to-day operation of IT and automation components can be subject to many disruptions and failures. Due to inadequate training, employees are unable to distinguish between security incidents and technical failures, security incidents are not responded to, and weaknesses remain uncorrected. This can hamper business processes, cause financial loss, or lead to regulatory sanctions.

2.6 Failure to comply with security measures

There is a risk that confidential documents may be left open on the desk, doors left unlocked, windows left open, or computer screens left unlocked due to employee negligence or haste.

2.7 Negligence in the handling of information

When security measures established in the organisation are ignored, for example by writing passwords on a sticky note on a display, even the best technical security measures become ineffective. If documents containing confidential information are left in the printer or thrown in the bin for anyone to access, encrypting the files on the hard drive is useless.

2.8 Inadequate acceptance of information security

There may be a lack of acceptance of information security requirements within the organisation and a lack of awareness of the importance of implementing security measures. Non-acceptance may, for example, be due to the organisational culture ('we have always done it this way') or a lack of leadership. Employees' resistance to security measures may also be the result of unreasonable or excessive security requirements.

2.9 Social engineering

Social engineering can result in an attacker gaining unauthorised access to information or IT systems by establishing contacts via telephone, email, or social networking and exploiting people's helpfulness. If an employee is not sufficiently aware of such an attack, skilful communication will lead the employee to act in an unauthorised manner. As a result of social engineering, the attacker may obtain confidential information, distribute malware, or even force the employee to transfer money to an alleged business partner.

3 Measures

3.1 Life cycle

Planning

ORP.3.M1	Increasing awareness of information security among the management
ORP.3.M3	Instruction on the secure use of information technology
ORP.3.M4	Awareness and training plan on information security

Operation

ORP.3.M6	Design and implementation of measures for information security awareness and training activities
ORP.3.M7	Training on information security management methods

Improvement and enhancement

ORP.3.M8	Measurement and evaluation of learning outcomes

Additional advanced measures

ORP.3.M9	Specific training for vulnerable persons and organisations

3.2 Key measures

ORP.3.M1 Increasing awareness of information security among the management [director, management of the organisation]

a. The management is regularly informed about information security risks, the potential damage they can cause, and their impact on business processes.
b. The management is aware of information security requirements imposed by legislation.
c. The management is aware of information security implementation practices in other similar organisations and of opportunities for the certification of information security processes.
d. The management of the organisation supports the implementation of security awareness campaigns and other training activities for employees.
e. Senior employees set an example in information security by following the security measures themselves and by drawing the attention of other employees to the need to comply with these measures.

ORP.3.M3 Instruction on the secure use of information technology [director, human resources department, IT department]

a. Employees have completed a basic training in cyber hygiene and have proven their level of knowledge by taking a respective test.
b. Employees and users from outside the organisation are instructed on the secure use of IT, industrial automation, and IoT components as well as the rights and responsibilities associated with their use.
c. The organisation establishes policies for the secure use of IT, industrial automation, and IoT components. The regulations are clear and up to date and are approved by the management to clearly define the responsibilities.
d. When changes are made to the regulations or the instructions for use, it is ensured that the changes are communicated to the users.

3.3 Standard measures

ORP.3.M4 Awareness and training plan on information security

a. An information security awareness and training plan is developed and approved by the management to raise employees' awareness.
b. Information security awareness and training plans are developed taking into account the needs of

the specific target groups. Employees with similar backgrounds, expertise, or tasks are grouped together in the same target group. In practice, target groups are also formed on the basis of structural units.
c. The timeliness of the information security awareness and training programme is regularly monitored and adapted or improved as needs change.

ORP.3.M6 Design and implementation of measures for information security awareness and training activities

a. Information security training for employees is designed based on the employees' tasks and responsibilities. The content of the training is sufficient to implement the applicable security requirements and measures.
b. All employees receive information security training appropriate to their work tasks and responsibilities.

ORP.3.M7 Training on information security management methods

a. The persons responsible for information security are trained on information security management and on the implementation of the information security standard.
b. Information security management training includes examples and practical exercises, including real-life examples of the implementation of the information security standard.

ORP.3.M8 Measurement and evaluation of learning outcomes [human resources department]

a. Learning outcomes in the area of information security are measured and evaluated based on target groups to determine the extent to which the objectives set out in the information security awareness and training plan have been achieved (see ORP.3.M4 Awareness and training plan on information security).
b. The evaluation of learning outcomes measures both qualitative and quantitative aspects of the awareness and training plan, using training evaluation forms, end-of-training tests, employee surveys, or periodic knowledge checks (such as the cyber test of the Information System Authority, https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/kubertest).
c. The human resources department works with the information security manager, the data protection specialist, the working environment representative, the fire safety officer, and other key personnel to assess the content and effectiveness of training.

d. The results of learning outcome tests are taken into account when modifying and improving the awareness and training plan of information security.

3.4 Advanced measures

ORP.3.M9 Specific training for vulnerable persons and organisations (C-I-A)

a. Particularly exposed persons (for example, those performing critical functions) and employees of particularly security-sensitive organisations receive comprehensive training on the threats, the plan of action in the event of a threat, and the precautions to be taken.
b. The reinforcement of the learning materials is chosen to suit the culture and the size of the organisation; for example, simulation exercises may be organised for employees to practice how to respond to a stressful situation.

ORP.4 Management of identity and rights

1 Description

1.1 Purpose

To propose measures to organise the management of identity and rights. Both users and IT components should have access only to the necessary IT resources and information.

1.2 Responsibility

The IT department is responsible for the management of identity and rights.
Additional responsible persons: User, information security manager, management of the organisation.

1.3 Limitations

Measures for the management of identity and rights in IT system components, operating systems, or directory services are presented in the corresponding modules (for example, SYS.1.3 Linux and Unix server, SYS.1.2.2 Windows Server 2012; APP.2.1 Directory service in general, APP2.2 Active Directory).

2 Threats

2.1 Absence or inadequacy of the processes for the management of identity

If the processes for the management of identity and rights are incomplete or if the procedures are not followed, the responsible system administrator will not receive adequate information on personnel changes. As a result, the departing employee's user account may remain unlocked and they may continue to have access to sensitive information or cloud applications. Similarly, an employee who has moved to another department may retain their previous rights.

2.2 Lack of a central suspension of user rights

An employee may have multiple user accounts to access different IT systems. In the absence of a central overview of access to the IT systems, system administrators cannot immediately suspend all rights of an employee in the event of an attack or password theft. Similarly, when an employee leaves, some access paths may remain unlocked.

2.3 Inadequate management of access rights

If different persons are responsible for granting rights in different departments and the management of the access rights is poorly organised, access rights may be unduly complicated or, on the contrary, made too easy. In the first case, a lack of access rights may hamper day-to-day operations, while in the second, unnecessary access rights may create a security risk.

3 Measures

3.1 Life cycle

Planning

ORP.4.M1	Rules for user account management
ORP.4.M2	Granting, modifying, and revoking rights
ORP.4.M3	Documentation of user rights
ORP.4.M4	Allocation and segregation of responsibilities
ORP.4.M8	Procedure for the use of passwords
ORP.4.M22	Establishment of password quality requirements
ORP.4.M23	Requirements for IT systems processing passwords

ORP.4.M11 Resetting and changing passwords

ORP.4.M12 Authentication procedure for IT systems and applications

ORP.4.M13 Selection of appropriate authentication mechanisms

Implementation

ORP.4.M5 Management of physical access

ORP.4.M6 Management of access to IT resources

ORP.4.M7 Management of data access

ORP.4.M16 Regulating access to IT systems

ORP.4.M17 Appropriate identity and rights management system

Operation

ORP.4.M9 Identification and authentication

ORP.4.M10 Protection of privileged accounts

ORP.4.M14 Controlling the use of user accounts

ORP.4.M15 Procedures for the management of identity and rights

ORP.4.M18 Use of a central authentication service

ORP.4.M19 Instructing employees on the use of authentication procedures and mechanisms

Additional advanced measures

ORP.4.M20 Emergency response of the identity and rights administration system

ORP.4.M21 Multi-factor authentication

ORP.4.M24 Implementation of the four eyes principle in IT management

3.2 Key measures

ORP.4.M1 Rules for user account management [IT department]

a. The organisation has prepared and approved rules for user account management.

b. The user account is assigned on an identity basis and linked to a specific user.

c. Impersonal administration and guest accounts which are actually not used and which are defined in the standard IT system conventions are deactivated or deleted.

d. User accounts that have not been used for a long period of time are deactivated.

e. User groups are assigned on a role basis.

ORP.4.M2 Granting, modifying, and revoking rights

a. An IT system user account is created and access rights are granted on the basis of business necessity only, using the principle of minimisation.
b. In the event of changes in the composition of the personnel, access rights that are no longer needed are revoked.
c. The deletion of unnecessary user accounts is allowed only in exceptional cases and only if the re-use of the same user IDs does not create identity management problems (for example, in systems using AD/LDAP services).
d. Permissions are set in accordance with the user role.
e. Greater than normal privileges are granted to employees at the request of their director and after the justification and specification of the need.

ORP.4.M3 Documentation of user rights

a. User accounts, user groups created, and rights profiles are documented.
b. The documentation of user accounts, user groups created, and rights profiles is regularly verified to ensure that it is up to date and complies with the user's work tasks and information security requirements.
c. User rights documentation is protected against unauthorised access.
d. User rights documentation stored in electronic format is backed up in accordance with the backup procedure.

ORP.4.M4 Allocation and segregation of responsibilities [management of the organization]

a. The organisation defines the responsibilities and work tasks where the use of information technology is necessary.
b. It is defined which responsibilities or work tasks cannot be performed by the same person.
c. The principles for the segregation of responsibilities are respected in the assignment of work tasks, and any role conflicts between work tasks are taken into account when establishing additional controls.

ORP.4.M5 Management of physical access [administrative department]

a. The organisation defines the physical access rights necessary for the performance of the employee's responsibilities and work tasks.
b. The issuance or revocation of security tokens used as means of access is documented.

c. All persons with physical access rights are instructed on the correct use of the access tokens.
d. In the event of an individual's prolonged absence, access rights are temporarily suspended.

ORP.4.M6 Management of access to IT resources

a. The organisation defines the access rights to IT resources necessary for the performance of the employee's responsibilities and work tasks.
b. The issuance or revocation of smart cards or other security tokens used as access media is documented.
c. All persons with access rights are instructed on the correct use of the access tools.
d. In the event of an individual's prolonged absence, access rights are temporarily suspended.

ORP.4.M7 Management of data access [information security manager]

a. The organisation defines the data access rights necessary for the performance of the person's responsibilities and work tasks.
b. If a security token is used to access data, its issuance or revocation is documented.
c. All persons with data access rights are instructed on the correct use of the access tools.
d. In the event of an individual's prolonged absence, data access rights are temporarily suspended.

ORP.4.M8 Procedure for the use of passwords [user, information security manager]

a. The organisation establishes procedures for the use of passwords (see also ORP.4.M22 Establishment of password quality requirements and ORP.4.M23 Requirements for IT systems processing passwords).
b. The procedure for the use of passwords clearly stipulates the user's obligation to keep passwords secret from others.
c. Passwords are changed on a regular basis, at reasonable intervals.
d. If there is a suspicion that unauthorised persons have gained knowledge of the password, the password is changed immediately.
e. It is prohibited to use passwords that are easy to guess or that appear on published lists of most frequently used passwords.
f. The same password may not be used more than once.
g. A different password is used for each IT system or application.
h. Written storage of passwords is only allowed in exceptional cases, and they are kept in a secure

location.
i. The use of an electronic password manager is only allowed if a security analysis has been carried out on the use of the password manager and the use has been approved by the information security manager. Particular care is taken with password managers that synchronise data with a third-party cloud service.
j. If password complexity rules can be set in the IT systems, the complexity rules are enforced.
k. If the IT system allows it, multi-factor authentication is used instead of password-only authentication.

ORP.4.M9 Identification and authentication

a. Access to all IT systems and services is protected by user identification and authentication (including other IT systems).
b. When using a password access tool, the password is changed the first time the access tool is used.

ORP.4.M22 Establishment of password quality requirements [user, information security manager]

a. Password quality requirements are established taking into account the protection requirements of the IT systems and the users' profiles.
b. The password is sufficiently complex to prevent guessing it.
c. Passwords of at least 12 characters are recommended.
d. The password should not be too complex for the user to remember it with reasonable effort in regular use.

ORP.4.M23 Requirements for IT systems processing passwords

a. Passwords are not stored in an IT system or application in cleartext.
b. Passwords for networked IT systems and applications are only transmitted in encrypted form. This measure also applies to applications used on the intranet.
c. There is always a specific reason for the password change required by an IT system or application.
d. Passwords for standard user and system accounts of an IT system or application are changed as soon as possible. Default passwords are replaced by sufficiently strong passwords, default login settings are changed.

e. In the case of an unsuccessful login attempt, the IT system does not give any indication whether the password or the username is incorrect.

3.3 Standard measures

ORP.4.M10 Protection of privileged accounts

a. Multi-factor authentication is used to protect privileged accounts from external attackers and unauthorised extension of privileges.

ORP.4.M11 Resetting and changing passwords

a. Sufficiently secure procedures are in place within the organisation to reset or change passwords.
b. Support personnel involved in resetting or changing passwords is appropriately trained.
c. In case of higher protection requirements, a plan of action is in place to change and transmit the password securely without the involvement of support personnel.

ORP.4.M12 Authentication procedure for IT systems and applications [information security manager]

a. The organisation has defined authentication requirements and established authentication procedures for each IT system and application.
b. Authentication data is stored in encrypted form.
c. Authentication data is transmitted over data networks in encrypted form.

ORP.4.M13 Selection of appropriate authentication mechanisms [information security manager]

a. Identification and authentication mechanisms appropriate to the protection requirements are used within the organisation.
b. The authentication data of IT systems or applications is protected against unauthorised access, modification, and destruction throughout their processing.
c. After unsuccessful login attempts, the IT system or application increases the time period after which a new login is allowed.
d. The IT system or application may specify the number of unsuccessful login attempts after which the IT system or application user account is locked.

ORP.4.M14 Controlling the use of user accounts

a. Regular checks are carried out to determine whether the users of IT systems are using their user account and whether they always log out of the system after completing a task.
b. Logging on to the IT system under another physical user name is strictly prohibited.

ORP.4.M15 Procedures for the management of identity and rights

a. The organisation establishes and implements the following procedures:
- management of access policies;
- management of user accounts and user groups;
- management of rights profiles and user roles.

ORP.4.M16 Regulating access to IT systems

a. The established access policies are complied with when granting access to IT systems.
b. Standard rights profiles are used in accordance with the employee's tasks.
c. Procedures are in place to manage access to each IT system.
d. User access to IT systems and services is granted after user identification and authentication.

ORP.4.M17 Appropriate identity and rights management system [information security manager]

a. Identity and access rights management system:
- is tailored to the organisation and its business processes and meets their protection requirements:
- meets the access management requirements in place within the organisation;
- enables the implementation of the principle of segregation of responsibilities.

b. The identity and access rights management system is protected against internal and external attacks.

ORP.4.M18 Use of a central authentication service [information security manager]

a. A centralised single sign-on access authentication service is used to implement unified identity and rights management.
b. The security requirements for the central authentication service are designed and documented prior to deployment.

ORP.4.M19 Instructing employees on the use of authentication procedures and mechanisms [user]

a. Employees are briefed on authentication procedures and instructed on how to correctly use the authentication procedures.
b. Clear instructions for authentication are provided to all employees.

3.4 Advanced measures

ORP.4.M20 Emergency response of the identity and rights administration system [management of the organisation, information security manager] (C-I-A)

a. To ensure business continuity, the security criticality of the identity and rights management system from a business process perspective is identified, and the readiness of the identity and rights management system for an emergency situation is verified.
b. A specific concept of user rights for emergency response is developed, and rights profiles for emergency response are defined in accordance with the different responsibilities of the employees in the event of an emergency.

ORP.4.M21 Multi-factor authentication (C)

a. In case of high protection requirements, secure multi-factor authentication, for example, by ID-card or token, is used for authentication purposes.

ORP.4.M24 Implementation of the four eyes principle in IT management (C)

a. Two administrators are used to carry out administrative activities with high protection requirements.
b. In the case of multi-factor authentication, authentication tools are shared between the administrators. In the case of a password-only authentication, the password is split into two parts, each administrator knowing only their part.

ORP.5 Compliance management (requirements management)

1 Description

1.1 Purpose

To provide measures to establish and comply with security requirements based on the organisation's objectives, legislation, contracts, and policies.

1.2 Responsibility

The compliance manager is responsible for compliance management measures.
Additional responsible persons: The information security manager, the management of the organisation, the administrative department, the director.

1.3 Limitations

This module deals with information security compliance management in general. Sector-specific legislation and individual agreements are not covered by the measures.

2 Threats

2.1 Breach of legal or contractual provisions

Failure to properly implement information security measures may result in the inadvertent or intentional violation of legal or contractual provisions.

2.2 Unauthorised disclosure of information

If an employee fails to comply with the established security requirements, confidential information may be leaked.

2.3 Failure to verify the identity of the interlocutor

When communicating via electronic channels, the identity of the interlocutor is often not verified. This is either considered impolite or technically difficult. There is an unfounded assumption that the content of the conversation or email is confidential and that the information will not fall into the wrong hands.

2.4 Accidental disclosure of inside information

When information is transmitted, for example, by telephone or by means of a removable storage device and email, it is possible that, in addition to the information requested, something unwelcome may be inadvertently disclosed. If an employee uses a cloud service carelessly, they may inadvertently leak confidential information.

3 Measures

3.1 Life cycle

Planning

ORP.5.M1 Determining legal framework conditions

ORP.5.M4 Planning and organisation of compliance management

Operation

ORP.5.M2 Compliance with legal framework conditions

ORP.5.M5 Management of exceptions

Improvement and enhancement

ORP.5.M8 Regular review of compliance management

3.2 Key measures

ORP.5.M1 Determining legal framework conditions [administrative department, director, management of the organisation]

a. The organisation has developed a process to identify all legal, contractual, and other requirements that have an impact on security management. The relevant requirements are documented.
b. The identified legal frameworks are taken into account in the design of business processes, applications, and IT systems, and in the procurement of IT components.
c. The legal framework is reviewed and the documented requirements are regularly updated.
d. Specific requirements arising from legislation are taken into account, in particular in the following areas:

- protection of personal data;
- protection of business confidentiality;
- protection of intellectual property;
- use of cryptography;
- logging and monitoring IT systems;

• long-term data retention;
• emergency response.

ORP.5.M2 Compliance with legal framework conditions [director, administrative department, management of the organisation]

a. When designing business processes or developing IT systems, information security requirements arising from the legal framework are already taken into account in the planning and design stages.
b. The overall responsibility for compliance with the legal requirements lies with the management of the organisation.
c. Compliance with the legal framework and legal requirements is the responsibility of specific employees with approved work tasks.
d. Appropriate measures are taken to remedy non-compliances.

3.3 Standard measures

ORP.5.M4 Planning and organisation of compliance management [management of the organisation]

a. To ensure an overview of the legal requirements in each specific area, responsible persons and their compliance management tasks have been designated.
b. Structured summaries of compliance requirements are provided to target audiences.
c. Additional information security measures arising from compliance requirements are integrated into regulations and procedures in cooperation with the information security manager.
d. The implementation of information security measures related to compliance management is regularly monitored.

ORP.5.M5 Management of exceptions [information security manager]

a. In exceptional cases, concessions may be made to comply with the security policy. Exceptions to the security policy are justified and a risk assessment is carried out.
b. Exceptions are agreed with the management and an overview of all exceptions is maintained.
c. In the case of temporary derogations, their continued need is regularly reviewed.

ORP.5.M8 Regular review of compliance management

a. Compliance management and the efficiency and effectiveness of the resulting measures is regularly reviewed (see DER.3.1 Audits and reviews).
b. The regular review verifies the compliance of the organisation and business processes with the evolving compliance management requirements.

3.4 Advanced measures

There are no advanced measures in this module.

CON: CONCEPTS AND METHODOLOGIES

CON.1 Cryptography concept

1 Description

1.1 Purpose

To provide organisational measures for the use of cryptographic tools and guidelines for the development of a cryptography concept.

1.2 Responsibility

The information security manager is responsible for cryptography concept measures.
Additional responsible persons: The responsible specialist, the IT department, the director.

1.3 Limitations

IT procedures regarding the utilisation of cryptographic tools (hardware or software units performing cryptographic functions) are explained in the module group OPS.1.1 Main IT operations. The protection of individual applications or IT systems using cryptography is described in the relevant application modules.

2 Threats

2.1 Inadequate key management

Confidential information might be disclosed as a result of inadequate key management. If encrypted data and cryptographic keys reside on the same data medium due to having no process guidelines, then in the case of a symmetric cryptographic procedure, all persons with access to the data medium or communication channel can decrypt the data.

2.2 Breach of legal framework conditions when implementing cryptographic modules

Legal framework conditions for the implementation of cryptographic devices may vary from country to country. Some countries do not allow the use of cryptographic modules without national authorisation or have restrictions on the export of high-security cryptographic products. If data protection regulations require the application of such cryptographic procedures for data protection which the laws of other countries do not support, data exchange between data protection subjects is impossible.

2.3 Loss of the confidentiality or integrity of data due to operational errors

If an organisation adopts a cryptographic tool that is too complex or counter-intuitive to use, users may abandon the cryptographic device and instead transmit data in the form of cleartext. This allows attackers to eavesdrop on the data being transmitted.

2.4 Software errors or vulnerabilities of a cryptographic tool

The security of cryptographic mechanisms may be compromised by weaknesses or errors in the software of cryptographic tools. For example, random numbers generated by a cryptographic module may be predictable, making the reconstruction of a cryptographic key involving random numbers considerably easier. An attacker may be able to take advantage of vulnerabilities in hardware or software performing cryptographic functions to manipulate vital systems and for the unauthorised alteration of data.

2.5 Cryptographic module failure

Technical defects, power failures, or intentional destruction may cause a cryptographic module to fail. This means that encrypted data cannot be used until the hardware required for decryption is replaced. Business-critical processes of the organisation may come to a standstill.

2.6 Unsafe cryptographic tools

Cracking unsafe or outdated cryptographic algorithms does not require expensive resources. Even if only secure and certified products are used within an organisation, the communication may be crackable if the communication partner outside the organisation does not use up-to-date cryptographic devices.

2.7 Errors in the encrypted data or cryptographic keys

If a cryptogram is modified after data has been encrypted, the encrypted text cannot be decrypted. Replacing a single bit in a cryptographic key would mean that the decryption of encrypted data becomes impossible. Where backup copies of data have not been made, all data becomes inaccessible.

2.8 Revealing a cryptographic key

The security of a cryptographic mechanism depends on whether cryptographic keys remain confidential. An attacker will usually try to identify the key used. Knowing the key and the cryptographic mechanism allows the attacker to decrypt the data. To this end, the attacker may attempt to restore the cryptographic key based on the memory dump of the device that used it or search for it in configuration files or backup copies of data. In the case of an encrypted hard disk, an attacker might install a keylogger between the keyboard and the computer to decrypt the hard disk and gain access to the password.

2.9 Forged certificate

Certificates are used to bind a public cryptographic key to a private key of a specific individual, which, in turn, is cryptographically protected by a digital signature. When a certificate is forged, the digital signatures are either incorrectly associated with the person named in the digital signature certificate or the data is encrypted and transmitted with an unsafe key

3 Measures

3.1 Life cycle

Planning

CON.1.M1	Planning the implementation of cryptographic mechanisms
CON.1.M9	Establishing selection criteria for cryptographic tools

Operation

CON.1.M2	Ensuring data security when using cryptographic mechanisms
CON.1.M4	Secure key management
CON.1.M10	Cryptography concept
CON.1.M15	Reacting to the impairment of cryptographic mechanisms
CON.1.M19	List of cryptographic tools in use

Disposal

CON.1.M5	Secure erasure and destruction of cryptographic keys

Additional advanced measures

CON.1.M11	Testing hardware with cryptographic functions
CON.1.M16	Physical security of cryptographic hardware modules
CON.1.M17	Emission security measures
CON.1.M18	Replacing hardware with cryptographic functions
CON.1.M20	Identifying manipulations of hardware and software with cryptographic functions

3.2 Key measures

CON.1.M1 Planning the implementation of cryptographic mechanisms [responsible specialist]

a. When selecting cryptographic mechanisms, cryptography algorithms approved by independent studies are preferred, having been thoroughly checked and without any known vulnerabilities.
b. The cryptographic tool uses currently recommended key lengths.
c. When determining the length of a key, its suitability for the planned duration of use of the cryptographic key is taken into account. In the event of longer periods of use, we recommend a longer key.

CON.1.M2 Ensuring data security when using cryptographic mechanisms [IT department]

a. When backing up encrypted data, cryptographic keys are protected against unauthorised access.
b. Long-life cryptographic keys are stored in a location without a network connection outside of the IT system in use.
c. When storing encrypted data for a long period, access to the data is ensured. The cryptographic algorithms and key lengths used for encryption are regularly checked against currently recommended values.

d. Decommissioned encryption tools are archived and the respective hardware and software configuration is backed up.

CON.1.M4 Secure key management

a. An appropriate key management system and a secure environment have been created for the management of the cryptographic keys of cryptographic tools.
b. The key management system handles the maintenance of the integrity and authenticity of cryptographic keys during the entire life cycle of a key (creation, maintenance, updating, and destruction of keys).
c. An appropriate key generator and a secure environment are used to generate cryptographic keys.
d. When using keys generated by third parties, the origin and integrity of the key data is checked. Cryptographic tools with an uncontrolled key repository are not used.
e. Default keys of cryptographic tools (except public key certificates) are replaced.
f. If possible, a cryptographic key is used for a single purpose only. Different keys are used for encryption and signature generation.
g. Secret keys are protected from unauthorised access and secure channels are used for their transport.
h. Cryptographic keys are modified according to the requirements of the IT system and at fixed intervals.
i. Procedures for handling incidents have been established for instances where secret keys and private keys are disclosed.

3.3 Standard measures

CON.1.M5 Secure erasure and destruction of cryptographic keys [IT department]

a. Decommissioned cryptographic keys and certificates are securely erased and destroyed.
b. Procedures for the secure erasure and destruction of cryptographic keys are documented in the cryptography concept.

CON.1.M9 Establishing selection criteria for cryptographic tools [responsible specialist]

a. Before choosing a cryptographic tool, the requirements that the product must meet are established. The following aspects are taken into consideration:

- functionality;

- interoperability;
- economic feasibility;
- performance and being fail-safe;
- technical aspects;
- personnel and organisational aspects;
- cryptographic mechanisms, algorithms, and key lengths in use;
- data protection requirements;
- legal framework conditions (including international legal aspects).

b. The need to use only certified cryptographic devices is determined on the basis of the intended use and the site of deployment.

CON.1.M10 Cryptography concept

a. The establishment of the cryptography concept of an organisation is based on the general security policy of the organisation. The organisation's cryptography concept presents the technical and organisational requirements for the cryptographic mechanisms and tools in use.

b. As a minimum, the following is stipulated in the cryptography concept:

- who is responsible for cryptographic tools;
- secure configuration of cryptographic tools and the required technical parameters;
- testing of cryptographic tools;
- secure utilisation of cryptographic tools;
- secure management of cryptographic tools;
- management of cryptographic keys (including secure backups of keys);
- replacing cryptographic tools; secure erasure and destruction of cryptographic tools.

c. Users of cryptographic tools are provided with training materials, codes of conduct, and reporting channels to report problems and security events.

d. The involved employees follow codes of conduct.

e. Compliance with the cryptography concept is checked regularly. The results of the inspections are documented. The cryptography concept is updated whenever necessary.

CON.1.M15 Reacting to the impairment of cryptographic mechanisms

a. The organisation checks the up-to-date status and security of all of its cryptographic tools, methods, and parameters at least once a year, relying on trustworthy sources.

b. A procedure has been prepared for instances when vulnerabilities in cryptographic mechanisms

are identified to restore the required level of security of a cryptographic mechanism or replace the impaired cryptographic tool with a suitable alternative.

CON.1.M19 List of cryptographic tools in use [IT department]

a. The organisation has created a list of cryptographic tools in use (including hardware and software with cryptographic functions). As a minimum, the list must include the following:

- IT systems that use the cryptographic tool in question;
- objective of using the cryptographic tool (such as encryption of a computer hard drive);
- cryptographic methods and mechanisms;
- security parameters of the cryptographic tool (e.g. key length).

3.4 Advanced measures

CON.1.M11 Testing hardware with cryptographic functions (C-I) [IT department]

a. Prior to adopting hardware with cryptographic functions, new cryptographic keys are created and the organisation checks whether the cryptographic functions work as expected.
b. Test procedures for hardware with cryptographic functions are described in the cryptography concept.
c. The performance of utilised cryptographic functions is tested following any changes to the IT system.
d. The correctness of the configuration of hardware with cryptographic functions is verified regularly.
e. If possible, the organisation uses cryptographic hardware that enables conducting self-tests.

CON.1.M16 Physical security of cryptographic hardware modules (C-I) [IT department]

a. Measures have been implemented to prevent unauthorised physical access to hardware with cryptographic functions.

CON.1.M17 Emission security measures (C) [IT department]

a. Additional measures are taken to improve emission security based on the need for confidentiality of the information.

b. Emission security measures and thresholds for the implementation of measures are documented in the cryptography concept.

CON.1.M18 Replacing hardware with cryptographic functions (C-I-A) [IT department]

a. The organisation has spare pieces of hardware to replace hardware with cryptographic functions, such as a sufficient supply of hardware-based cryptographic tokens used for multifactor authentication.
b. The organisation has prepared guidelines describing the replacement of hardware with cryptographic functions.

CON.1.M20 Identifying manipulations of hardware and software with cryptographic functions (C-I)

a. Adopted cryptographic modules cannot be switched off undetected or ignored.
b. The operation of hardware or software performing cryptographic functions is monitored to identify possible attempts at manipulation.

CON.2 Personal data protection

1 Description

1.1 Purpose

To show the connection of the protection of personal data to baseline security. The aim of this module is to safeguard the exercise of the fundamental rights of natural persons with regard to the processing of personal data within the organisation.

1.2 Responsibility

The data protection specialist is responsible for ensuring the implementation of the measures for the protection of personal data.
Additional responsible persons: The management of the organisation.

1.3 Limitations

Compliance with data protection requirements established by legal acts, including the principles of personal data processing, is obligatory for a data controller or a processor.

A data protection specialist is responsible for analysing and verifying the legality of personal data processing activities in an organisation by providing advice and recommendations in relation to their duties. For this reason, the activities of a data protection specialist are not described in the following modules.

The measures explained in the modules are applied to target objects that record and store personal data.

In addition, appropriate measures from the following modules must be implemented to protect personal data:

- ORP.2 Personnel
- ORP.4 Administration of identity and rights
- ORP.5 Compliance management (requirements management)
- CON.1 Cryptography concept
- CON.3 Data backup concept
- CON.6 Data erasure and destruction
- CON.8 Software development
- CON.9 Exchange of information
- OPS.1.1.3 Patch and change management
- OPS.1.1.4 Protection against malware
- OPS.1.1.5 Logging
- OPS.1.1.6 Software testing and onboarding
- OPS.1.2.2 Archiving
- OPS.2.2 Using cloud services
- OPS.2.3: Outsourcing
- OPS.3.2 Information security of a service provider
- DER.1 Detection of security incidents
- DER.2.1 Handling of security incidents
- DER.3.1 Audits and reviews
- NET.3.2 Firewall
- NET.3.3 Virtual private network (VPN)

2 Threats

2.1 Ignoring data protection regulations

The General Data Protection Regulation of the European Union, the Personal Data Protection Act, and in certain instances, other legal acts establish requirements for the processing of personal data. The objective of the legal acts is to protect the rights of natural persons (data subjects).

2.2 Inadequate data processing procedures

The risk of misuse of data increases when an organisation lacks procedures to ensure legitimate access to IT systems and data or when employees have access to personal data that is not required for performing their specific tasks.

2.3 Insufficient resources

If an organisation underestimates the protection requirements of personal data and does not allocate sufficient manpower, means, and other necessary resources for the protection of personal data, the organisational and technical measures for the protection of personal data are not implemented in part or in full. The result might not ensure sufficient protection for personal data and the legal requirements go unmet.

2.4 Inadequate privacy

The processing of personal data may violate the right of a data subject to the privacy of family and private life.

2.5 Loss of confidentiality of personal data

Whenever processing personal data, there is always a danger of the information falling in the hands of an unauthorised person. For instance, this could happen due to a breach of database security, an attack by hackers, or losing a physical data carrier. As a result of data leaks, personal data might be misused or it might be used as a basis for identity theft or other illegal activities detrimental to the right of self-determination of an individual.

2.6 Processing of inaccurate data

Processing of personal data comes with a risk of data becoming inaccurate, incorrect, or outdated. This may happen as a result of an error on part of an individual or mistakes in IT systems. When

mass processing data, the identification of such errors is extremely difficult. Processing incorrect data about a person may lead to wrong decisions and affect the rights, freedoms, and interests of individuals.

2.7 Reputational damage of the data controller or processor

Any leaks of the personal data of employees, customers, or partners through the fault of the organisation may cause great damage to the reputation of the organisation. Customers may terminate agreements that they have concluded with the organisation, leading to financial losses due to a decrease in turnover. Employees and partners lose trust in the organisation.

3 Measures

3.1 Life cycle

Planning

CON.2.M1	Planning personal data protection
CON.2.M2	Appointing a data protection specialist (data protection officer)
CON.2.M3	Mapping the processing of personal data

Implementation

CON.2.M4	Developing a data protection policy and data protection guidelines
CON.2.M7	Documenting the requirements for data protection

Operation

CON.2.M5	Increasing awareness among employees of the organisation
CON.2.M6	Ensuring the lawfulness, purposefulness, and minimality of personal data processing
CON.2.M8	Ensuring the rights of a data subject
CON.2.M9	Pseudonymisation and anonymisation of personal data
CON.2.M10	Restricting access to personal data
CON.2.M11	Compliant storage of personal data
CON.2.M12	Implementation of technological measures for the protection of personal data
CON.2.M13	Impact assessments in regard to data protection
CON.2.M14	Management of data processors
CON.2.M15	Secure encryption of personal data
CON.2.M16	Personal data storage rules

CON.2.M17	Central access management system
CON.2.M18	Protecting the processing of personal data
CON.2.M19	Logging data processing operations
CON.2.M20	Physical security of data processing locations
CON.2.M21	Guaranteeing network security
CON.2.M22	Implementation of data protection by design and data protection by default principles in applications
CON.2.M23	Testing applications that contain personal data
CON.2.M24	Privacy settings on websites
CON.2.M25	Deleting personal data upon leaving employment
CON.2.M26	Conducting a data protection audit

Additional advanced measures

CON.2.M27	Temporary access rights
CON.2.M28	Automatic monitoring of personal data processing
CON.2.M29	Classifier system of access restrictions
CON.2.M30	Automatic identification of personal data
CON.2.M31	System of digital privilege management

3.2 Key measures

CON.2.M1 Planning personal data protection

a. The organisation has analysed the locations, categories, and protection requirements of the personal data that it processes.
b. The organisation has mapped and documented data protection requirements arising from legislation and agreements concluded with third parties.
c. The organisation has identified the obligation to implement personal data protection measures and assigned persons responsible for the measures of personal data protection.

CON.2.M2 Appointing a data protection specialist (data protection officer)

a. The management of the organisation has appointed a data protection specialist if required by Article 37 of the General Data Protection Regulation (GDPR), section 40 of the Personal Data Protection Act, or by other relevant legislation.
b. The organisation ensures that the data protection specialist is able to update their know-how

regularly (through trainings) and has a chance to stay informed about developments and events in the field of data protection.
c. The organisation guarantees the compliant and timely inclusion of the data protection specialist in all issues involving the protection of personal data.

CON.2.M3 Mapping the processing of personal data

a. The organisation has mapped the processing of personal data throughout the entire life cycle of the data.
b. The results of the mapping are documented in an overview of personal data processing.

CON.2.M4 Developing a data protection policy and data protection guidelines

a. The organisation has prepared and established a data protection policy and data protection guidelines.
b. The data protection policy describes the principles for granting access to personal data as well as collecting, processing, storing, and deleting data.
c. The data protection policy establishes the responsibilities of the staff of the organisation in ensuring personal data protection.
d. The data protection guidelines include instructions for the employees of the organisation for responding to incidents impacting the security of personal data and to enquiries of data subjects.

CON.2.M5 Increasing awareness among employees of the organisation [data protection specialist, information security manager, human resources department]

a. The organisation arranges regular data protection trainings, involving external experts where necessary.
b. The organisation conducts cyber hygiene trainings (such as using a screen lock when leaving the computer).
c. The level of knowledge of the employees is regularly verified with tests that include questions about data protection and exercises for solving common incidents.

CON.2.M6 Ensuring the lawfulness, purposefulness, and minimality of personal data processing

a. The organisation processes personal data only when a legal basis stipulated in Article 6 of the GDPR exists or pursuant to section 15 of the Personal Data Protection Act.
b. The organisation processes personal data only for predetermined purposes and to the extent necessary for fulfilling these objectives.

CON.2.M7 Documenting the requirements for data protection

a. The organisation has prepared data protection rules in accordance with Article 5 (1) a) and 5 (2), Articles 12-22, as well as recitals (39), (58)-(72) of the GDPR or pursuant to section 23 of the Personal Data Protection Act.
b. The data protection rules are clear to the employees and other data subjects and, if needed, readily available.

CON.2.M8 Ensuring the rights of a data subject

a. The organisation ensures that the rights of data subjects established by the GDPR can be implemented in technological terms in its IT systems.
b. Clear and comprehensible information regarding the rights of data subjects is provided to them.
c. A data subject can easily exercise their rights.

CON.2.M9 Pseudonymisation and anonymisation of personal data

a. The organisation minimises the use of data that can be directly or indirectly linked to a natural person when processing personal data.
b. If possible, personal data is pseudonymised (a method of replacing personal data with a unique identifier or a code that does not allow the direct identification of a person when processing data) or anonymised (a method where personal data is altered so that it is no longer possible to link it to a specific person directly or indirectly).
c. Wherever possible, only anonymised data is used for statistical data processing.

CON.2.M10 Restricting access to personal data [IT department]

a. When granting access to personal data, the principle of minimality is observed; i.e. an employee is only given access to the part of the IT system and to data that the employee needs for performing their professional duties.
b. Restriction of access also entails limiting physical access and access privileges.

CON.2.M11 Compliant storage of personal data

a. The organisation has set retention periods for all personal data that it stores.
b. The objective of storage and retention periods comply with the relevant legislative acts.
c. The organisation stores personal data only as long as is necessary for achieving the objective of storage.
d. Once the purpose of storage has been fulfilled or the personal data is no longer necessary, the organisation arranges its safe destruction.

CON.2.M12 Implementation of technological measures for the protection of personal data [IT department]

a. The organisation has adopted secure authentication methods in its IT systems to prevent unauthorised access to personal data (see ORP.4 Administration of identity and rights).
b. The organisation has installed a firewall to protect network traffic and restricted unnecessary traffic in the network (see NET.3.2 Firewall).
c. When processing personal data (incl. sending it), the organisation encrypts personal data wherever appropriate.
d. Activities and circumstances of personal data protection are logged (see OPS 1.1.5 Logging).
e. Backups of personal data are regularly created. Backup copies are stored in a location that is away from the data that is copied (see CON.3 Data backup concept).
f. The organisation regularly verifies and tests the implementation of technological measures when processing personal data to make sure that they are efficient, secure, and comply with the GDPR, the Personal Data Protection Act, and this standard.

3.3 Standard measures

CON.2.M13 Impact assessments in regard to data protection

a. The organisation has prepared an impact assessment on data protection when required by Article 35 of the GDPR or section 38 of the Personal Data Protection Act. The data protection specialist is in an advisory role when preparing an impact assessment.
b. The data protection specialist or the management of the organisation has prepared a guideline for conducting impact assessments, based on which employees without a prior thorough training are capable of completing an impact assessment.

CON.2.M14 Management of data processors

a. The organisation has concluded data protection agreements in compliance with Article 28 of the GDPR or section 30 of the Personal Data Protection Act. Data protection agreements are not concluded when data is processed pursuant to a binding legal act under EU or Member State law.
b. The organisation has verified that the data processors are implementing the required security measures when processing personal data and are complying with the principles of data processing. If necessary, the data controller conducts compliance audits.
c. The organisation has selected its data processors carefully by relying only on data processors who provide sufficient guarantees for the risk level of the specific data processing operation, primarily regarding professional knowledge, trustworthiness, and means, indicating that they are capable of implementing technological and organisational measures compliant with the requirements of the GDPR or the Personal Data Protection Act, including requirements regarding the security of processing activities.
d. The organisation has reviewed the data protection rules, procedures, and security measures of data processors when recruiting them, and is convinced that they comply with the requirements of the GDPR or the Personal Data Protection Act.
e. Whenever requirements for personal data protection are amended, the organisation ensures that the data processors are informed of the changes. If a data processing agreement has been concluded between the organisation and the data processor, it will be updated if necessary.
f. Upon changes to personal data protection requirements, the organization ensures that authorized processors are aware of the changes and that the concluded data processing agreements comply with the new requirements. If necessary, the data processing agreements are updated.

CON.2.M15 Secure encryption of personal data [IT department]

a. The organisation has implemented a secure key control procedure and uses a strong and reliable encryption algorithm for ensuring the security of personal data.
b. The organisation ensures that encryption is implemented in appropriate cases as early as during the collection or forwarding of data.
c. The organisation ensures that the option to decrypt encrypted personal data is strictly limited to authorised persons only.
d. The employees of the organisation must be trained in and informed about the best practices of encryption and the organisation must ensure that the employees know how to use the tools of encryption properly to protect personal data.

CON.2.M16 Personal data storage rules

a. The organisation has prepared rules that describe the manner of storing various types of personal data, their retention periods, and the methods for the destruction of personal data.
b. The rules include the retention periods of all personal data backups or archived personal data.
c. The organisation uses automatic notifications or automatic deletion to comply with retention periods.
d. The organisation audits compliance with the retention periods regularly.

CON.2.M17 Central access management system [IT department]

a. The organisation uses a central access management system to manage the access of its employees to personal data.
b. The organisation logs the activities of employees to identify the misuse of personal data, accelerate responses to security events, and reduce the risk of data leaks.
c. The organisation arranges reviews of access rights at least once a year. Excess access rights are revoked.

CON.2.M18 Protecting the processing of personal data [IT department, information security manager]

a. The organisation uses multifactor authentication when granting access to sensitive personal data to ensure that only authorised persons have access.
b. The organisation uses a virtual private network (VPN) for remote work. The VPN ensures a secure and encrypted connection to the intranet of the organisation, allowing employees to access personal data safely from outside the organisational network.
c. A privacy filter is used for protecting sensitive data from prying eyes. Employees who regularly work remotely on laptops have privacy filters.

CON.2.M19 Logging data processing operations [IT department]

a. All personal data processing operations are logged.
b. The data processing logs contain the following information:
- the person who processed personal data;
- the time when personal data was processed;
- the type of personal data that was processed;

• the types of operations that took place involving personal data (operations include all forms of data processing, including viewing, changing, downloading, and deleting the data).

c. Where third parties have been involved in data processing activities (including data processors and joint controllers), clear roles are determined for storing and access to data processing logs.

d. An automatic log analyser is implemented in respect to data processing logs for the identification of potential violations regarding data protection.

e. The organisation has established a procedure for reviewing data processing logs. Data processing logs are checked regularly, and if necessary, on a case-by-case basis.

f. Data processing logs are stored based on the principles of minimality and purposefulness. Above all, it is important that data processing logs would not be stored unreasonably long, but still long enough to identify potential violations.

g. Retention periods have been established for data processing logs, and after the periods end, the logs are automatically deleted.

CON.2.M20 Physical security of data processing locations

a. The organisation has established restricted areas for the secure processing and storage of personal data (such as locked rooms or server rooms).

b. The organisation has established access rules for the rooms, and implemented technical access and security systems for enforcing them (e.g. electronic locking systems, key cards, biometric authentication, security cameras).

c. The organisation regularly conducts reviews to evaluate the efficiency of physical security measures (including checking the state of doors and locks, testing security systems and the functioning of video surveillance, reviewing key card logs, etc.).

d. The organisation has prepared procedures for managing visitors who enter these areas of the organisation where personal data is processed. This entails registering visitors, prior approval of visits, informing visitors of the rules of the organisation, and accompanying the visitors (i.e. a visitor can only move around the premises of the organisation when accompanied by a chaperone who is an employee of the organisation).

CON.2.M21 Guaranteeing network security [IT department]

a. The organisation uses intrusion detection and prevention systems (IDS, IPS) for the detection of network attacks as well as the identification and prevention of unusual activity involving personal

data.
b. Secure encrypted protocols are used for sending personal data through a public network.

CON.2.M22 Implementation of data protection by design and data protection by default principles in applications

a. Applications which are based on personal data processing or which process personal data take into account the principles of data protection by design and data protection by default as early as in the stages of selecting and planning the development of the application.
b. Data protection rules established for the applications are complied with and checked during the entire lifespan of the application.
c. Applications only use personal data needed for achieving the purpose of processing.

CON.2.M23 Testing applications that contain personal data [tester]

a. The organisation has prepared the principles for testing applications, which prohibit the disclosure of personal data and unauthorised access to personal data as well as limit the activities of the testers in systems containing personal data. Testing means testing before adopting an application as well as penetration testing of applications to detect vulnerabilities.
b. Agreements have been concluded for testing, explaining the extent of testing, its objectives, and activities permitted during testing. The objective is to ensure that responsibilities are clear and to protect the confidentiality and privacy of personal data.
c. Prior to testing, personal data that is absolutely necessary for testing is determined, and if possible, anonymised or pseudonymised.
d. Where possible, testers are granted rights that are more limited than the ones of the regular users of the IT system. A tester only has access to the resources that are necessary for completing the tests.
e. The organisation ensures that all personal data stored by the testers is securely deleted after the tests are completed. To this end, appropriate agreements are concluded (including a data processing agreement).
f. After the testing, the organisation carries out a follow-up test to assess the efficiency of data protection and security measures.

CON.2.M24 Privacy settings on websites

a. Cookies and tracking tools used on the web pages of the organisation comply with the GDPR and other relevant legal acts.
b. The visitors of the website are given clear and unambiguous information regarding the cookies and tracking tools that are used. When required, consent is asked from the visitors of the website for the use of cookies.
c. The visitors of the website can check and manage their cookie preferences.
d. The organisation has published its data protection rules on its website, which describe the nature of the personal data that is collected (incl. cookies), processing methods, objectives of processing, retention periods, and privacy protection measures. Articles 12-22 of the GDPR must be complied with when preparing additional elements of data protection rules.
e. The organisation applies security measures on its website to protect personal data.
f. The organisation implements a secure data transfer protocol (HTTPS) on its web page containing personal data.
g. The use of third-party services to protect the website or network connections (such as Google Analytics, Matomo, CloudFare) is clearly stated in the data protection rules.
h. The organisation has done everything possible to make sure that data processors would implement appropriate security measures to protect personal data.

CON.2.M25 Deleting personal data upon leaving employment [human resources department]

a. The organisation has established rules for handling and deleting personal data in computer workstations.
b. The rules include stipulations regarding the options that an employee leaving employment has for retrieving their personal documents (including personal data) which they have stored in the IT systems of the employer. The rules should stipulate, for example, that the employee stores their personal data and personal documents only in a folder marked for this purpose.
c. The rules include the retrieval of information needed by the organisation from the data of the employee who is leaving (such as retrieving emails or documents from an online mailbox that are essential for the organisation).
d. When an employee leaves the organisation, personal data is deleted from the devices and data carriers allocated for their personal use (including removable media).
e. The organisation stores the personal data of a former employee to the extent stipulated by law and for the stipulated retention period.

CON.2.M26 Conducting a data protection audit

a. The organisation conducts regular independent reviews or audits to assess the actual status of personal data protection within the organisation and to identify potential risks and shortcomings.
b. A data protection audit is conducted at least once in four years.

3.4 Advanced measures

CON.2.M27 Temporary access rights (C)

a. The organisation implements temporary access rights to ensure the lawfulness of access rights and reduce the risk of unauthorised processing of personal data.
b. When determining the expiry of access rights, the principle of minimality is observed - primarily because the employees of the organisation might be replaced and this measure would help to avoid a situation where former employees of the organisation would have access to personal data.

CON.2.M28 Automatic monitoring of personal data processing (C)

a. The organisation uses an automatic monitoring system for personal data processing, which identifies personal data that someone is attempting to transfer out of the organisation, notifies authorised persons of the situation, and if necessary, blocks the transfer of personal data.
b. Upon receiving a notification, the legality and necessity of the transfer of personal data are evaluated.

CON.2.M29 Classifier system of access restrictions (C)

a. The organisation (public sector) implements a classifier system of access restrictions to make it easier to assign access restrictions to documents based on the content of the documents as required by the Public Information Act.
b. Among all else, the classifier system of access restrictions is able to identify automatically whether a document contains personal data or if it should be deemed confidential for other reasons.

CON.2.M30 Automatic identification of personal data (C)

a. The organisation uses an automated system capable of identifying personal data in the network traffic and information systems of the organisation (including special categories of personal data as defined in the GDPR) as well as classify the data without involving users.

b. The locations of special categories of personal data are mapped automatically. The organisation has implemented tougher security measures for the protection of special categories of personal data.

CON.2.M31 System of digital privilege management (C-I-A)

a. The organisation has implemented a system of digital privilege management to ensure privacy, allowing to assign strictly need-based privileges for various folders, IT systems, and documents. For example, it is possible to give specific employees only the right to view a document, whereas altering it (including downloading it) would require additional privileges.

CON.3 Data backup concept

1 Description

1.1 Purpose

To provide guidelines on how to develop an organisation's data backup concept.

1.2 Responsibility

The information security manager is responsible for the implementation of data backup concept measures.
Additional responsible persons: The IT department, the responsible specialist, employee.

1.3 Limitations

The storage and maintenance measures for the long-term storage of electronic documents are set out in module OPS.1.2.2 Archiving. System and application specific logging measures are provided in the relevant modules, that is, SYS.1.1 Server in general, APP.3.2 Web server, and NET.3.2 Firewall. Deleting data and destroying backup copies is based on the module CON.6 Data wipe and destruction.

2 Threats

2.1 Lack of data backup

In the absence of data backup, data loss (caused by malware, technical failures, or fires, for example) could result in irreparable damage to the organisation.

2.2 Lack of recovery testing

Unless regular recovery tests are performed to recover data from a backup, there is no assurance that the data will be recoverable in the event of an actual recovery need and within the agreed time frame.

2.3 Unsafe preservation of backup data media

If data media containing backup copies are stored in an unsafe location, an attacker could access, steal, or manipulate the data. Data media used for backup may become unusable due to unsuitable storage and environmental conditions.

2.4 Lack of or inadequate documentation

If backup procedures are not documented, or are incompletely documented, recovery may take longer than expected or fail.

2.5 Non-compliance with the legal requirements

Failure to comply with the legal requirements in data backup may result in a fine or a claim for damages following a data incident (data theft, data loss).

2.6 Unsafe cloud service provider

If an organisation backs up data in the cloud, an attacker may be able to access the backups. Data backed up to the cloud may not be restored quickly enough.

2.7 Insufficient storage capacity on the storage media

If storage media do not have sufficient storage capacity, data backup may stop at some point. Backup software may automatically overwrite older backups that may still be needed.

2.8 Lack of a data backup concept

If a data backup concept has not been prepared for backup procedures or the concept is not complied with (for example, data is backed up too rarely or the actual recovery time of data is longer than agreed in the organisation), the recovery of data is difficult.

2.9 Insufficiency of the data storing speed

When the amount of data to be backed up increases, more time is needed to back up the data. In the worst-case scenario, the next data backup might be launched before the scheduled backup of data has been completed. This may result in various issues; for example, a data backup process is interrupted or the load on the backup system increases because several data backup processes are running at the same time.

2.10 Ransomware attack

Ransomware is a special type of malware which encrypts the data of the infected IT systems. After this, the attackers demand that the victim pay a ransom for the decryption of data. If the data has not been backed up, the encrypted information is lost or can be retrieved only by paying a ransom. However, there is no guarantee that the data is retrieved even in the event of paying a ransom.

3 Measures

3.1 Life cycle

Planning

CON.3.M1	Delimitation of data backup factors
CON.3.M2	Data backup guidelines
CON.3.M4	Data backup plans
CON.3.M6	Data backup concept

Operation

CON.3.M5	Regular data backup
CON.3.M12	Secure storage of backup data media
CON.3.M14	Protection of backup copies
CON.3.M15	Regular testing of backup

Acquisition

CON.3.M7	Acquisition of an appropriate data backup system

Implementation

CON.3.M9 Establishing conditions for remote data backup

Additional advanced measures

CON.3.M13 Application of cryptography in data backup

3.2 Key measures

CON.3.M1 Delimitation of data backup factors [responsible specialist, IT department]

a. For IT systems and, where appropriate, for critical individual IT applications, a register of data to be backed up is established and the data backup factors are determined. The owners of IT systems and the owners of the business side of IT applications participate in deciding the data backup factors.
b. As a minimum, the following are considered data backup factors:

- composition of the data to be backed up;
- availability, integrity, and confidentiality requirements of the data to be backed up;
- legal requirements;
- the necessary data volume;
- the storage period of data;
- the required frequency of backups;
- the tolerable recovery time;
- requirements for the deletion of data and the destruction of data media.

c. When evaluating the necessary data volume, presumed future increase in the data volume is taken into account.
d. The backup frequency is determined based on an estimate of the frequency of data changes and additions and the maximum allowable data loss.
e. The maximum tolerable downtime (MTD) of an IT system is used as a basis for determining the allowable recovery time for the data to be backed up.
f. The same confidentiality requirements apply to the backed-up data as to the data in the operating system.
g. Data backup factors have been documented. Documentation is updated when new requirements are added or the existing ones are amended.

CON.3.M2 Data backup guidelines [responsible specialist, IT department]

a. The IT department prepares data backup guidelines that contain data backup procedures.
b. When preparing the data backup guidelines, data backup factors are taken into consideration (CON.3.1 Delimitation of data backup factors).
c. As a minimum, the data backup guidelines include the following about each IT system and dataset:

- the type of data backup;
- the backup method and data media;
- the procedures for data backup and recovery;
- the frequency and time of backup;
- the storage location;
- the transport and storage conditions of the data media;
- retention time;
- the allocation of responsibilities for implementing the backup.

d. Data is backed up on a data carrier that is separate from the operational data.
e. Data media with a higher protection requirement are connected to an intranet or IT system only during the backup or recovery of data.
f. Where a virtual infrastructure is in place, the extent to which data backup based on server snapshots is relied upon is determined.

CON.3.M4 Data backup plans

a. Data backup plans for backing up various types of data and software have been prepared.
b. The principles of backup and data recovery are described in the data backup plans, including:

- the hardware and software used for backup;
- the configurations of hardware and software;
- the order of backing up and recovering data;
- the number of generations of data to be retained.

c. As a minimum, data backup plans consider the following:

- the acquired or proprietary software is backed up with a full backup as a single generation of data;
- the system data is backed up at least once a month in one data generation;
- the application data is backed up at least once a week with a full backup and is retained for at least three generations of data;

• the log data is backed up at least once a month with a full backup and is retained for at least three generations of data.

CON.3.M5 Regular data backup [IT department, employee]

a. Data is backed up with the intervals provided in the data backup plan and data backup guidelines.
b. Employees are informed of the data backup arrangements.
c. Employees involved in the data backup process know what their tasks are.
d. Employees carry out their assigned data backup tasks.

CON.3.M12 Secure storage of backup data media [IT department]

a. Backup data media are kept in a storage location that is separate from the source system.
b. In the case of storage in the same building, the backed-up data is located in a part of the building separated by a fire barrier.
c. The environmental conditions of the storage location are suitable for the long-term storage of data media.
d. As a minimum, the secure storage of data is ensured to the extent of data storage deadlines.

CON.3.M14 Protection of backup copies [IT department]

a. Data media used for backup are protected from unauthorised access.
b. Only authorised persons have access to the data media.
c. Data media used for backup are protected from unauthorised overwriting.
d. Write access is given to backup data media only for backing up data or conducting authorised administrative operations.

CON.3.M15 Regular testing of backup [IT department]

a. The functioning of the data backup and the recovery of backed-up data is tested regularly.
b. The recovery of data must remain within the allowed recovery time and function flawlessly.

3.3 Standard measures

CON.3.M6 Data backup concept [responsible specialist, IT department]

a. A data backup concept has been prepared which corresponds to the business continuity plan (BCP) and the recovery point objective (RPO) of the organisation.
b. The data backup concept is developed by taking into account all relevant IT systems and applications and data backup factors.
c. The data backup concept is agreed with the responsible persons.
d. Employees are familiar with the concept at least to the extent necessary for the performance of their work tasks.
e. The data backup concept and the related documents are securely backed up and usable even when vital IT systems (including the document management system) are unavailable.
f. The implementation of the data backup concept is regularly monitored.

CON.3.M7 Acquisition of an appropriate data backup system [IT department]

a. Criteria for the selection of a data backup system are established prior to the procurement of a data backup system.
b. The data backup system meets the following requirements derived from the concept of data backup:

- detecting incorrect or corrupted data media;
- working seamlessly with the existing hardware;
- allowing automatic scheduling;
- allowing automatic messaging to one or more users;
- allowing data media security with a password or encryption;
- allowing data compression;
- allowing data categorisation based on data logs;
- allowing data to be selected by creation or modification time;
- being able to perform full backup and incremental backup;
- allowing to automatically compare the backup with the original;
- allowing data to be restored to the original or selected location;
- allowing the recovery of files with the same name.

CON.3.M9 Establishing conditions for remote data backup [IT department]

a. When an external storage site is used for online backup, a service level agreement (SLA) is concluded and the physical location of the data is agreed to ensure service quality.
b. Access to backups is possible only with a secure authentication.

c. The data contained in the backup is encrypted in the backup location and when transferring the data.
d. The quality of the network connection enables to back up and recover data within the allowed backup and recovery times.

3.4 Advanced measures

CON.3.M13 Application of cryptography in data backup (C-I) [IT department]

a. The backed-up data is encrypted to ensure data confidentiality and integrity.
b. The choice of cryptographic mechanism is made with a view to ensuring that the data can be recovered after a longer period of time.
c. The protection and retention of cryptographic keys is ensured by secure key management procedures (see CON.1.M2 Data backup when using a cryptographic device).

CON.6 Data erasure and destruction

1 Description

1.1 Purpose

To provide measures for the secure erasure of data and guidance on the regulations for data destruction.

1.2 Responsibility

The information security manager is responsible for the implementation of the data erasure and destruction measures.
Additional responsible persons: The data protection specialist, the responsible specialist, the IT department, the employee, the administrative department.

1.3 Limitations

The module covers only the general organisational requirements for data erasure and destruction. The modules CON.3 Data backup concept, OPS 1.2.2 Archiving, CON.9 Exchange of information also concern erasure and destruction.

2 Threats

2.1 Absence of or inadequate documentation of regulations on data erasure and destruction

Unless employees are instructed to securely erase data, data may remain on the data media in a readable form. Retired data media and IT systems may no longer be under the control of the organisation, in which case the risk of data leakage is even higher. Sensitive data on the data media may fall into the hands of third parties. Negligent leakage of personal data can result in significant reputational damage and fines for the organisation.

2.2 Loss of confidentiality due to residual information on the data media

In most file systems, the use of a simple delete function does not destroy files marked for erasure by the user. Only file references are erased from the file system management information and the data space associated with the file is marked as free. However, the actual contents of the data space on the data medium will be preserved and can be restored with the appropriate means.

2.3 Use of an unreliable disposal service

When the secure erasure or destruction of data media (including the destruction of paper documents) is entrusted to an external service provider, negligence on the part of the service provider may lead to the theft of data media either directly from the service provider's premises or from pre-destruction collection points.

2.4 Mishandling of defective data media

The fact that a normal user can no longer retrieve data from a data medium does not mean that the data on the data medium has been permanently destroyed. If such defective data media are thrown away in the regular trash, they may fall into the hands of an attacker, who can use special tools to recover some or all of the data.

3 Measures

3.1 Life cycle

Planning

CON.6.M1	Procedures for data erasure and destruction
CON.6.M2	Safe disposal of work tools and data media requiring protection
CON.6.M11	Outsourcing the destruction of data media to an external service provider
CON.6.M4	Procedures for the secure destruction of data media

Implementation

CON.6.M12	Procedures for the secure erasure of data
CON.6.M8	Guidelines for employees on data erasure
CON.6.M13	Guidelines for the destruction of defective data media

Additional advanced measures

CON.6.M14	Additional guidelines for the secure destruction of data media

3.2 Key measures

CON.6.M1 Procedures for data erasure and destruction [administrative department, responsible specialist, data protection specialist, IT department]

a. The organisation puts in place procedures for the erasure and destruction of data.
b. Each sub-unit determines which operational data is deleted or retired and under what conditions.
c. Minimum and maximum retention periods for data are determined in accordance with the requirements arising from legislation. Procedures for the retention and erasure of personal data are agreed with the data protection specialist.
d. The responsible person for data erasure and destruction is designated and, where necessary, a dedicated external service is used.

CON.6.M2 Safe disposal of work tools and data media requiring protection

a. Data contained in data media and work tools is securely erased or destroyed before disposal.
b. When data media are retired, the established regulations and guidelines are followed (see CON.6.M12 Procedures for the secure erasure of data).
c. Collection points are established on the organisation's premises for the disposal of data media and work tools, protected from unauthorised access.

CON.6.M11 Outsourcing the destruction of data media to an external service provider [procurement department]

a. The procedure for the disposal and destruction of data media involving external service providers is secure and understandable. Appropriate and secure means of destruction or erasure are used.
b. When outsourcing the destruction service, the data media to be destroyed are stored on the organisation's premises, protected from unauthorised access, until removal.
c. The removal of data media is secured on the basis of the data protection requirements.
d. The external companies responsible for the disposal and destruction are regularly audited for compliance with the prescribed requirements.
e. The key actions described in OPS.2.1 Outsourcing are adapted to the service provider and its personnel.

CON.6.M12 Procedures for the secure erasure of data

a. Depending on the type of data medium and the data protection requirements, the following procedures are applied when erasing data, such as
- if the data on the data media to be overwritten is not encrypted, the data media are overwritten multiple times and in full using a random data generator (for example, PRNG Stream).
- if the data on the data media is encrypted, the cryptographic keys are destroyed. The destruction of the cryptographic keys is performed according to the rules of procedure described in the cryptography concept.

b. For the erasure of data from smart phones and other smart devices, the devices are reset to factory default settings and an initial boot and initial set up is performed.
c. IoT devices are reset to factory default settings, and all access data stored on the device is overwritten or erased.
d. The contents of the data media embedded in the IoT devices is erased, using the appropriate functionality of the device.

3.3 Standard measures

CON.6.M4 Procedures for the secure destruction of data media

a. Before data media are destroyed, it is verified that the data can be effectively and securely erased from the data media (see CON.6.M12 Procedures for the secure erasure of data).

b. Appropriate procedures are in place for the destruction of the data media in use. Appropriate means are used to destroy different types of data media.
c. Responsible employees are aware of the procedures and means to be used for the destruction of data media.
d. The destruction procedures and means are regularly verified to ensure that they are up to date and still sufficiently secure.

CON.6.M8 Guidelines for employees on data erasure [employee, IT department, data protection specialist]

a. Written guidelines on data erasure and destruction are in place, covering all data media, applications, IT systems, and other work tools that may contain information (for example, smart devices).
b. Guidelines on data erasure and destruction are communicated to all employees. Regular and random inspections are made to ensure that employees are complying with the guidelines.
c. Guidelines for the erasure and destruction of information are updated as necessary.

CON.6.M13 Guidelines for the destruction of defective data media

a. If the data cannot be securely erased from the data medium due to a defect in the data medium itself, the data medium is physically destroyed.
b. By special agreement with the service provider (that is, the repairer of the data medium), the destruction of the data medium may also be performed by the service provider. In such a case, the service provider must comply with all the requirements for the secure destruction of data media.

3.4 Advanced measures

CON.6.M14 Additional guidelines for the secure destruction of data media (C)

a. Data media are demonstrated to be destroyed in accordance with recognised industry norms or standards (such as ISO/IEC 21964).

CON.7 Information security for business trips

1 Description

1.1 Purpose

To set out measures to ensure the security of digital data and paper-based information when employees are on business trips and to assist the responsible persons in putting in place security measures for business trips.
The module specifically addresses the procedural, technical, and organisational measures necessary for the performance of professional duties when travelling abroad.

1.2 Responsibility

The information security manager is responsible for the implementation of information security measures for business trips.
Additional responsible persons: The user, the IT department, the human resources department.

1.3 Limitations

The module does not cover local IT systems whose security measures are described in the module groups NET Networks and Communication, SYS IT Systems, and APP Applications. More general topics on client computer security are covered in the modules SYS.2.1 C_lient computer in general_, NET.3.3 Virtual Private Network (VPN), and SYS.3.2.2 Mobile device management (MDM).

2 Threats

2.1 Interception of information and spying / Economic espionage

Conversations, telephone calls, or data transmissions may be intercepted in unfamiliar premises and IT environments.

2.2 Disclosure and misuse of information in need of protection (electronic and physical)

When on a business trip, it can easily happen that a traveller leaves confidential paper or digital documents in a public room or in their hotel room.

2.3 Identity spoofing

An attacker may impersonate another person, both in physical and digital communication (through spoofing, forgery, hijacking, proxy attacks, etc.). Foreign business partners are often not personally

known to the employee. As a result, an employee may blindly trust a person who, knowing the background information, poses as another person.

2.4 Lack of security awareness and careless handling of information

Data media may be temporarily left unattended, for example in a meeting room during a meeting break or in a passenger compartment.

2.5 Breach of local legislation or regulations

Legislation and regulation in the country of destination (for example, data protection, notification obligations, responsibility, third party access) are often not known to the employee travelling abroad and therefore, the requirements imposed by the country are not complied with.

2.6 Coercion, extortion, kidnapping, and corruption

The physical security of travellers may be compromised when travelling abroad through coercion, extortion, or kidnapping. Senior management is often targeted.

2.7 Information from an unauthorised source / fabrication

While working abroad, it is possible to provide false and manipulated information to a traveller to deceive them. This can affect business decisions and the operation of business processes.

2.8 Theft or loss of equipment, data media, and documents

Mobile devices or documents can be lost or stolen, putting the sensitive information they contain at risk.

3 Measures

3.1 Life cycle

Planning

CON.7.M1 Information security regulations for business trips

CON.7.M3 Identification of country-specific legislation, travel, and environmental conditions

Implementation

CON.7.M2	Raising awareness among employees
CON.7.M10	Encryption of mobile IT devices and data media
CON.7.M11	Anti-theft devices
CON.7.M14	Email security

Operation

CON.7.M4	Use of screen filters
CON.7.M5	Use of a screen lock
CON.7.M7	Secure remote access
CON.7.M8	Secure use of a wireless local area network
CON.7.M9	Secure handling of data media
CON.7.M12	Secure disposal of materials and documents requiring protection
CON.7.M13	Secure carrying of data and data media

Emergency response

CON.7.M6	Timely incident reporting

Additional advanced measures

CON.7.M15	Emission security of mobile IT devices
CON.7.M16	Methods and tools for protecting integrity
CON.7.M17	Specialised travel equipment
CON.7.M18	Restriction of access rights when travelling abroad

3.2 Key measures

CON.7.M1 Information security regulations for business trips

a. Information security requirements for stays abroad are established in the information security regulations for business trips.

b. At a minimum, the regulations on information security for business trips cover:

- the nature of information security when travelling abroad, the objectives and scope of security;
- the responsibilities of the management, the information security manager, and the travelling employee;
- dealing with IT system loss, theft, or information leakage;
- increasing employees' awareness and training;
- protection of IT equipment (for example, encryption, anti-virus, automatic locking);
- data and data media protection;

- secure erasure of data and data media or documents;
- security of communications and data exchange;
- rights to take and collect data;
- 24/7 help desk support for questions and incident resolution.

c. An information sheet on information security aspects is prepared for employees using mobile IT devices on business trips.

CON.7.M2 Raising awareness among employees

a. Employees are briefed on the regulations on information security for business trips.
b. Employees are aware of and follow the rules for responsible use of information technology when travelling abroad, including:

- prohibition of the use of unapproved hardware and software;
- communication with their organisation and business partners;
- caution when accepting gifts offered to them;
- prohibition of the use of gifts containing digital memory;
- use of passwords and access restrictions;
- prohibition of the use of unsafe networks.

c. Employees are made aware of the destination's legislation and environmental conditions, including:

- country-specific legislation;
- country-specific travel and environmental conditions;
- advice on safe behaviour.

CON.7.M3 Identification of country-specific legislation, travel, and environmental conditions [human resources department]

a. Country-specific legislation and climate conditions are identified prior to travel, and relevant information material is prepared for employees.
b. The organisation assesses the level of risk and security and environmental conditions at the destination and decides on the need for additional protective measures (for example, the vaccination of employees).
c. The organisation develops and implements measures to protect equipment under difficult travel and environmental conditions.

CON.7.M4 Use of screen filters [user]

a. A full-screen filter is used to protect the information displayed on the screen of a mobile IT device.

CON.7.M5 Use of a screen lock [user]

a. Devices use a secure passcode- or password-protected screen lock.
b. The screen lock is automatically activated after a short break in use. Adequate locking delays for laptops and smart devices are specified in the information security regulations for business trips.

CON.7.M6 Timely incident reporting [user]

a. Employees notify the organisation of the loss or theft of an IT device or data medium as soon as possible, through agreed notification channels and contact persons.
b. The impact of the loss of the IT device or data medium is assessed and appropriate measures are implemented:

- the device's access setting is changed;
- the persons potentially at risk of the loss of confidential information are informed;
- affected user accounts and VPN connections are blocked;
- if the functionality is available, the device is remotely blocked and/or reset;
- in the event of a lost item being found, it is checked whether it has been tampered with.

CON.7.M7 Secure remote access [IT department, user]

a. Remote access with a preconfigured VPN and secure authentication mechanism is provided to connect to the organisation's network for employees travelling abroad.
b. IT equipment with remote access is used only by authorised persons.
c. Remote access devices have up-to-date and securely configured software, in particular web applications.
d. Mobile IT devices are equipped with a restrictively configured personal firewall.

CON.7.M8 Secure use of a wireless local area network [user]

a. A public wireless local area network uses a virtual private network (VPN) or comparable security mechanisms (see NET.3.3 Virtual private network (VPN), CON.7.M7 Secure remote access).

b. When using public wireless local area networks, the rules for the secure use of access points to the WLAN network are followed (see NET.2.2 Use of wireless local area network. INF.9 Mobile workplace).

CON.7.M9 Secure handling of data media [user]

a. Mobile data media are checked before use to ensure that they are not infected with malware.
b. Transportable data media are checked to ensure that they do not contain sensitive information.
c. When a data medium is disposed of, the data on the data medium is erased, taking the following into consideration:

- the data medium is completely erased, unlike normal erasure - not only the data references, but also the referenced data is erased;
- in the case of encrypted data erasure, the cryptographic keys are also securely erased;
- the data on the memory stick or other semiconductor data media is erased by at least two overwritings.

CON.7.M10 Encryption of mobile IT devices and data media [user, IT department]

a. Mobile IT devices and data media are encrypted in accordance with the established procedures within the organisation to protect sensitive information.
b. Encryption keys are stored separately from the encrypted device.
c. Data encryption is carried out in accordance with foreign regulations.

CON.7.M12 Secure disposal of materials and documents requiring protection [user]

a. Employees are required to securely destroy unnecessary data media or documents while abroad, rather than dispose of them.
b. If there are no facilities for secure destruction while travelling, or in the case of documents or data media containing particularly sensitive information, they are retained until return and then destroyed in a secure manner.
c. Where third-party data destruction equipment (paper shredder) is used, successful disposal is ensured.

3.3 Standard measures

CON.7.M11 Anti-theft devices [user]

a. Anti-theft devices (for example, mechanical or electronic locking) are implemented to protect mobile IT devices.
b. The purchase and use of anti-theft devices is in line with the organisation's security policies and is economically justified.

CON.7.M13 Secure carrying of data and data media [user]

a. Before the start of the business trip, unnecessary data is erased or removed from the IT equipment to be carried (see CON.7.M9 Secure handling of data media).
b. The employee is aware of which data media may be taken on international travel and what security measures must be taken.
c. Depending on the data protection requirements, additional requirements may be imposed for taking data abroad (see CON.7.M10 Encryption of mobile IT devices and data media).
d. The following measures are applied when transporting IT equipment:

- equipment is transported in the carry-on luggage rather than in the regular luggage;
- leaving the property unattended or forgetting it is avoided;
- devices are protected by passwords, data with protection requirements is encrypted;
- an overview of the current location of the equipment is kept.

CON.7.M14 Email security [user, IT department]

a. End-to-end encryption is used to ensure the security of the email solution.
b. Use of the organisation's email on public computers (for example, in hotels or internet caf's) is avoided.

3.4 Advanced measures

CON.7.M15 Emission security of mobile IT devices (C)

a. In the case of very high protection requirements, wired peripherals are used.
b. Equipment certified for emission security is used.

CON.7.M16 Methods and tools for protecting integrity (I) [user]

a. Data integrity is ensured by the use of check code comparison (for example, CRC) during data transmission.
b. Digital signatures and timestamps are used to maintain the integrity of sensitive information.

CON.7.M17 Specialised travel equipment (C-I-A) [IT department]

a. Equipment that has been pre-configured for this purpose is used for business trips.
b. In equipment prepared for travel, only the necessary functions can be used, in accordance with the principle of minimum requirements.

CON.7.M18 Restriction of access rights when travelling abroad (C-I) [IT department]

a. Access rights necessary for day-to-day work are granted to employees on international assignments. Excessive access rights are suspended for the duration of the trip, temporarily restricting the employee's access to the intranet if necessary.
b. During a stay abroad, the user environment is restricted from using features and performing actions that are not necessary to perform the user's tasks (for example, running scripts).

CON.8 Software development

1 Description

1.1 Purpose

To provide measures to manage the information security of the software solution commissioned by the organisation or developed within the organisation and to ensure the security of the software. The measures in this module can be used for the creation of a specific project-based software solution as well as for the continuous adaptation of legacy software that has been in use for many years.

1.2 Responsibility

The responsible specialist is responsible for the software development measures.
Additional responsible persons: The developer, the IT department, the tester, the administrative department.

1.3 Limitations

This module deals with information security in software development from the point of view of the contracting authority-developer relationship and does not provide a comprehensive overview of the whole software development process. The measures are complementary to the contracting authority's view of information security requirements and mitigation of security risks of software development presented in APP.7 Custom software development. Legal requirements for software development are described in module ORP.5 Compliance management (requirements management). The management of software changes is addressed in module OPS.1.1.3 Patch and change management. The acceptance and the installation of software in the operational environment is covered in OPS.1.1.6 S_oftware testing and onboarding_. If the planned software contains data encryption, additional measures from the module CON.1 Cryptography concept are taken into account.

2 Threats

2.1 Inappropriate software development methodology

The software development methodology sets out the activities to be carried out during the development process, including the formulation of the stages of the development project, their sequence, and the conditions to be fulfilled to proceed to the next stage. An inappropriate software development methodology will affect the functioning of the whole development process if important aspects of the project's information security are not adequately addressed and, conversely, too much valuable project time is spent on unimportant details. As a result, project efficiency and overall quality suffers. If important information security functionality is left out of the software product or is not adequately tested, the software under development may not meet the stated information security requirements.

2.2 Choosing an unsuitable software development environment

If the selection of the software development environment does not take into account the required functionality and the required extension capabilities, serious problems will arise during the development phase if the required functionality is not available in the development environment or does not meet the specified requirements.

2.3 Insufficient quality assurance

Insufficient quality assurance can lead to a development project being stretched beyond its deadline or, in the worst case, to the entire project failing. If software development lacks continuous monitoring of unauthorised manipulation of the software or of the integrity and adequacy of the security of the development process, significant security weaknesses may remain in the software product. It is often the case that quality assurance can be applied to in-house software development projects, but the development work carried out by an external service provider is not assessed to the same standard.

2.4 Missing or inadequate documentation

If the work documentation used in software development is at the level of design plans and does not contain the necessary level of detail, software errors will not be detected in time. Inadequate documentation significantly hinders the planning and execution of subsequent software modifications or enhancements. Lack of documentation complicates software maintenance and management procedures after software deployment. During the management process, an administrator may unknowingly make a mistake that could, in the worst case, lead to data loss or an interruption of the business process associated with the software.

2.5 Insufficient security of the development environment

An unsafe development environment without access restrictions allows software manipulation. Unauthorised software modifications made by the developer or by external unauthorised persons are difficult to detect later. Unless it is possible to identify afterwards who changed something in the software code and when, the attacker cannot be caught.

2.6 Software design errors

The more functionality a software contains, the more complex the management of the software source code becomes. If the software is not based on a well-thought-out software architecture, it will be difficult to modify the software product later. There is a risk that not all known security weaknesses can be fixed quickly enough.

2.7 Inadequate software testing and acceptance procedures

If the software is not adequately tested prior to deployment in the operating environment, or if there are no proper procedures for acceptance and validation of the software, the software received may

contain security weaknesses and errors in the software functionality. Such errors may also affect the operation of other IT systems in the operating environment to which the software product is interfaced.

2.8 Use of production environment data for software testing

When real data taken from the production environment is used in development or test environments, it is possible that confidential data can be accessed by unauthorised persons. Significant harm may result from the use of anonymised personal data in a test environment.

3 Measures

3.1 Life cycle

Planning

CON.8.M2	Selection of the appropriate software development methodology
CON.8.M3	Selection of the appropriate software development environment
CON.8.M1	Definition of software development roles and responsibilities
CON.8.M11	Preparation of procedures for the conduct of software development

Operation

CON.8.M5	Secure system design
CON.8.M6	Use of software libraries from trusted sources
CON.8.M7	Testing software during software development
CON.8.M8	Securely installing software changes, patches, and updates
CON.8.M10	Source code version control
CON.8.M20	Inspection of external software components
CON.8.M12	Detailed software documentation
CON.8.M16	Software development supervision

Implementation

CON.8.M14	Information security training for software developers
CON.8.M21	Consideration of software risks
CON.8.M22	Secure software architecture

Additional advanced measures

CON.8.M17	Selection of trusted development tools

CON.8.M18 Regular security audits of the development environment

CON.8.M19 Integrity inspections of the development environment

3.2 Key measures

CON.8.M2 Selection of the appropriate software development methodology

a. A suitable software development methodology and a process model appropriate to the methodology is selected for the software development.
b. The selected software development methodology is followed in the design and implementation of the project plan.
c. The software development process model includes information security requirements. Information security requirements are taken into account during the development process.
d. Employees are trained in the application of the software development methodology.

CON.8.M3 Selection of the appropriate software development environment

a. Prior to the selection of the software development environment, the requirements to be met by the software development environment and the tools are documented, and the criteria for the selection of the tools are defined. The requirements are validated by the employee responsible for software development.
b. The deployed software development environment meets the established requirements.

CON.8.M5 Secure system design

a. The following rules for secure system design are taken into account for the software under development:

- data are verified and validated upon entry before further processing in the IT system;
- for client-server applications, the final validation and confirmation of the data is always performed on the server;
- the standard software setting and the default values of the parameters allow the software to be used securely;
- in the event of an error or failure of a software component, the data to be protected will not be made available;
- the software requires as few system privileges as possible;
- cryptographic processes and products conforming to the cryptography concept (see CON.1

Cryptography concept) are used for the transmission and storage of data requiring protection;

• secure and trusted user authentication and authorisation mechanisms appropriate to the protection requirements are used;

• of the passwords used for authentication, only secure password hashes are stored in the software;

• information security events are logged in the software with an audit trail and in a format that allows for a retrospective analysis of the events as necessary;

• information that is not necessary for the operation in the operating environment (for example, redundant comments) is removed from the software programme code and configuration files.

b. System design rules are documented. Software developers are aware of the established system design rules.

c. Adherence to the system design rules is verified during the software development process and before the software is approved for use.

CON.8.M6 Use of software libraries from trusted sources

a. The reliability of the sources used and the integrity of the libraries is verified before external software libraries are used in the development process.

CON.8.M7 Testing software during software development [tester, developer]

a. Software testing and code review is carried out prior to the acceptance test and approval for use by the contracting authority.

b. The contracting authority or the contracting authority's representative is involved in the software testing and code review process.

c. During the development process, the software is tested against functional requirements (requirements that the software must fulfil) and non-functional requirements (requirements that the software must meet).

d. During the development process, the behaviour of the software is tested for input values and data types that are incorrect and different from the permitted input values (negative testing).

e. The test data set used for testing is carefully selected and protected against unauthorised modifications.

f. Wherever possible, automated work tools (for example, code analysers) are used to test the software.

g. Software testing is carried out in development and test environments that are separated from the production environment.

h. During software development, it is tested whether the requirements specified for the software are appropriate and correctly dimensioned.

CON.8.M8 Securely installing software changes, patches, and updates [developer]

a. Security-critical patches and updates to the software are developed by the developer and delivered to the contracting authority without delay.
b. After security-critical changes have been made to external software libraries, the developer makes the necessary changes to the software and provides the appropriate patches to the contracting authority.
c. Software modifications, patches, and updates are protected against unauthorised changes by an installation package checksum or digital signature.

CON.8.M10 Source code version control

a. Suitable version control tools are implemented to ensure the security of the software's source code and to manage code changes.
b. Changes made to the code are saved as a separate version during version control. If necessary, it is possible to undo the changes made (revert to the pre-modified version of the source code).
c. The concept of data backup takes into account software version changes. Before and after the installation of a new software version, the data used in the software is backed up.

CON.8.M20 Inspection of external software components

a. All external software components (including libraries), for which security cannot be fully guaranteed, are security tested before deployment.
b. All external software components are tested prior to their initial implementation to prevent potential software conflicts.
c. To ensure the integrity of the external software components, the control codes and/or digital certificates of the components are verified.
d. The latest approved versions of external software components are used in the development of the software and obsolete software components are not used.

3.3 Standard measures

CON.8.M1 Definition of software development roles and responsibilities [administrative department]

a. A general person responsible for managing the software development process is appointed within the organisation.
b. The following software development activities are assigned within the organisation:
- requirements development, requirements management, and change management;
- software design and software architecture;
- information security in software development;
- specific software development activities (for example, testing).

c. A person responsible for the information security of the development project is designated within each software development project.

CON.8.M11 Preparation of procedures for the conduct of software development

a. The organisation establishes procedures for the conduct of software development. The procedures include the measures covered in this module, which are specific to the organisation.
b. Software development procedures are implemented for all instances of software development.
c. For external developers, compliance with the software development procedures is a contractual obligation.
d. Software development procedures are updated as necessary.

CON.8.M12 Detailed software documentation

a. Detailed and comprehensive documentation is available for the software product.
b. The software documentation includes at least the following:
a description of the functionality of the software;
- user manuals for the users of the software;

a description and drawings of the software architecture;
- specifications of the software interfaces;
- documentation of the software library;
- specifications of the cryptographic mechanisms used;
- software installation, configuration, and administration guidelines for software administrators.

c. The level of detail of the software documentation is sufficient to enable a technical expert of the required level to take over the management and development of the software product on the basis of

the documentation.
d. The chosen software development methodology and process model include the creation and continuous updating of the software documentation.

CON.8.M14 Information security training for software developers

a. Software developers have a basic knowledge of information security and are up to date with general trends in information security.
b. Software developers have received training that is specific to the organisation, covering at least the following:

- analysis of software requirements (including information security requirements);
- project management in general, particularly in software development;
- risk management and threat modelling in software development;
- quality management and quality assurance in software development;
- software development methodologies and process models;
- software architecture;
- software testing;
- software change management;
- information security requirements in the organisation and sectoral security aspects.

CON.8.M16 Software development supervision

a. A project management model appropriate to the chosen software development methodology is developed for the management of software development. The project management model includes a development project monitoring function.
b. The software development supervisors are adequately qualified to assess all stages of the software life cycle.
c. The project management model for software development is consistent with the organisation-wide risk management system.
d. Quality objectives are set for development projects.

CON.8.M21 Consideration of software risks

a. A software risk assessment is carried out during the first phase of the software product development.

b. The software risk assessment is based on the protection requirements of the organisation using the software, the software requirements directory, and the context in which the software will operate.
c. The software risk assessment includes the development of potential risk scenarios, the identification of associated risks, the assessment of the likelihood of the risks materialising, and their potential impact.

CON.8.M22 Secure software architecture

a. The choice of software architecture is made taking into account the software requirements directory and the results of the risk assessment.
b. The software architecture allows the application of the principles of secure system design (see CON.8.M5 Secure system design) when creating the software.
c. Wherever possible, the design of the software takes into account the software's compliance with future standards and its resilience to new possible attack methods.
d. The chosen software architecture allows for easy future maintenance and further development of the software.

3.4 Advanced measures

CON.8.M17 Selection of trusted development tools (C-I-A)

a. Only development work tools with necessary and proven security features are used for software development.
b. The hardware and software manufacturers used in development are verified to be compliant with the information security requirements.

CON.8.M18 Regular security audits of the development environment (C-I-A)

a. Regular security audits are conducted to assess the implementation of security measures in the software development and test environment.

CON.8.M19 Integrity inspections of the development environment (I) [IT department]

a. Appropriate cryptographic processes (for example, file checksums) are used to ensure the integrity of the development environment and to prevent tampering.

b. The number of false positives is kept to a minimum to ensure the rapid detection of traffic incidents.

CON.9 Exchange of information

1 Description

1.1 Purpose

To provide measures for a secure exchange of information between IT systems and external parties.

1.2 Responsibility

The information security manager is responsible for the implementation of the measures for the exchange of information.
Additional responsible persons: The user, the responsible specialist, the administrative department.

1.3 Limitations

The security of network connections is dealt with in the NET module group. The use of removable data media for data transmission is covered by the module SYS.4.5 Removable data media.

2 Threats

2.1 Failure to provide information at the scheduled time

Failure to provide information at the scheduled time can seriously undermine business processes or lead to wrong management decisions. Failure to process or prepare data in a timely manner for making decisions will result in failure to meet business objectives.

2.2 Unauthorised disclosure of information

During the exchange of information, data and thus confidential information may fall into the wrong hands or not reach the intended recipient. The recipient's ability to prevent unauthorised disclosure of information is limited. The risk of misuse of information is higher if the parties to the exchange of information have not signed a confidentiality agreement.

2.3 Transmission of incorrect or inside information

If users are not adequately trained or are not sufficiently vigilant in passing on information, sensitive information may become available to unauthorised persons. If a data medium is transferred without securely erasing data previously stored on the data medium, such apparently erased data will be accessible to the recipient.

2.4 Unauthorised copying or modification of data

If unsafe channels are used to transmit data or data media, it is possible for data to be copied during its transmission without being detected. An attacker may also be able to eavesdrop on communications over the communication network used to exchange the data. If the attacker has access, they can also modify, manipulate, or add malware to the data during the transmission.

2.5 Use of insufficient cryptographic tools

If an easily intercepted key is chosen for encryption, or if secure channels are not used to send the cryptographic key to the communication partner, confidential data may leak.

3 Measures

3.1 Life cycle

Planning

CON.9.M1	Designation of authorised partners for the exchange of information
CON.9.M2	Procedure for the exchange of information

Implementation

CON.9.M3	Training on the exchange of information for employees
CON.9.M4	External agreements for the exchange of information

Operation

CON.9.M5	Removal of residual information from files prior to transmission
CON.9.M6	Compatibility check between the sender's and the recipient's IT systems
CON.9.M7	Backup of data to be transmitted
CON.9.M8	Encryption and digital signatures

Additional advanced measures

CON.9.M9 Conclusion of confidentiality agreements

3.2 Key measures

CON.9.M1 Designation of authorised partners for the exchange of information [administrative department, user]

a. The organisation defines what information is allowed to be transferred, to which partners, and through which data exchange channels.
b. The rights of the recipient to receive and further process the information are verified before it is transmitted to an external partner.
c. The recipient of the information is informed of the purposes for which and the manner in which the information may be used.

CON.9.M2 Procedure for the exchange of information [administrative department, user]

a. The organisation establishes procedures for the exchange of information, covering all forms of oral and electronic exchange of information.
b. The organisation establishes guidelines for determining the protection requirements of the information and the appropriate measures to protect the information.
c. Prior to the transmission of confidential information, the communication partner is informed that the information is intended to be used only for the purpose for which it is transmitted.
d. The organisation specifies which data exchange channels and environments are not permitted.

CON.9.M3 Training on the exchange of information for employees [responsible specialist]

a. Employees are familiar with the regulations applicable to the exchange of information and know how to handle confidential and internal-use information.
b. Employees are aware of what information can be communicated, when, where, and how.
c. Employees are trained in the use of IT tools to protect data (for example, encryption or the use of checksums).

3.3 Standard measures

CON.9.M4 External agreements for the exchange of information [administrative department]

a. The following conditions are agreed for the regular exchange of information with external partners:

- whether and what information must be protected;
- what the means of communication are;
- confidentiality requirements (see also CON.9.M9 Conclusion of confidentiality agreements);
- the level of security required and how this is demonstrated;
- how to deal with security incidents;
- dispute resolution procedures;
- legal framework conditions.

b. Arrangements are made for the exchange of information in the event of disruption in normal communications.

CON.9.M5 Removal of residual information from files prior to transmission [user]

a. Users are informed of the needs and means of disposal of residual information. Users are trained accordingly.
b. Prior to transmission, files are checked to ensure that they do not contain residual information that should not be published, such as comments, revision history, or redundant metadata.
c. Any residual information found is deleted, by changing the file format if necessary.
d. The absence of residual information in the submitted files is checked on a random basis.

CON.9.M6 Compatibility check between the sender's and the recipient's IT systems

a. The compatibility of the sender's and the recipient's IT systems and products is verified as follows before the data media are sent:

- physical compatibility of the equipment;
- the character code used (for example, ASCII);
- operating system and file system formats;
- application software;
- security software and security parameters.

b. Discrepancies are resolved by data conversion and/or data media replacement.

CON.9.M7 Backup of data to be transmitted [user]

a. If the data to be transferred is located only on the data medium and cannot be restored from other data sources, a temporary backup of the data medium is made.

CON.9.M8 Encryption and digital signatures [user]

a. Whenever possible, confidential information is encrypted before transmission.
b. High-integrity information is protected by a digital signature.
c. To encrypt the data, a cryptographic mechanism suitable for both the sender and the recipient is selected according to the protection requirements.

3.4 Advanced measures

CON.9.M9 Conclusion of confidentiality agreements (C) [administrative department, user]

a. The transmission of confidential information is subject to a contract with the recipient that specifies:

- what information is confidential and for how long;
- who is authorised to have access to the confidential information;
- how the confidential information is to be kept;
- the ownership of the information and the rights of the recipient to use the information;
- the consequences for breaching the confidentiality agreement.

CON.10 Web applications development

1 Description

1.1 Purpose

To provide measures for the development of secure dynamic (content-changing) web applications and for the protection of data processed in web applications.

1.2 Responsibility

The developer is responsible for the implementation of the web application development measures.
Additional responsible persons: There are no additional responsible persons in this module.

1.3 Limitations

Measures related to the secure use of web applications are described in module APP.3.1 Web applications. General measures for secure software development are described in module CON.8 Software development.

2 Threats

2.1 Inadequate authentication and access rights

If an attacker manages to bypass the authentication of a web application, they will be able to use the web application without authorisation. If the web application contains sensitive data, this could result in extensive financial and reputational damage to the organisation. If an attacker manages to log in to the web application as a user with elevated privileges, this opens up even more opportunities to steal, manipulate, or delete data. If the granting of web application user rights, authorisation, and resource sharing are non-securely designed and poorly implemented, the web application user (and the attacker impersonating the user) may gain unauthorised access to security-critical data.

2.2 Inadequate validation of inputs and outputs

Manipulated input data processed in a web application may not be detected in time. An attacker may be able to bypass the web application's protection mechanisms by manipulating input data and execute commands directly at the system or database level. If the data is not checked before it is issued, malicious code (for example malicious JavaScript commands) contained in the data could propagate to the related IT systems.

2.3 Missing or inadequate error management of a web application

Minor anomalies in the operation of a web application often go unrecorded and unaddressed. Failure to detect and address failures and errors in the web application in a timely manner can lead to a growing problem that may affect the operation of the application or make it inaccessible to users. An error in the web application could lead to large-scale data loss. An error in cached data could affect data integrity. A faulty security mechanism could lead to unauthorised access to data.

2.4 Inadequate logging of security events

Insufficient logging of security events in a web application makes it impossible to identify security events later and to find out why they occurred. Failure to identify the cause of the incident makes it difficult to implement measures to prevent similar incidents in the future.

2.5 Disclosure of sensitive background information in the web application

The data returned by the web server and the web application in response to certain queries may contain information about the version and configuration of the web server, the operating system, and the software that an attacker needs. Known weaknesses in IT components can be exploited by an attacker to plan a targeted attack on the web application.

2.6 Use of automated attack devices

An attacker may automatically generate a large number of repetitive queries that the web application must be able to process, to prevent the web application from working or to gain access to data. A denial-of-service attack against a web application can overload the web application and make it inaccessible to users. Repeated login attempts generated by the attack device can be used to try to guess combinations of user names (if the application provides feedback on this) and passwords of the application, that is, to conduct a brute-force attack or to compile lists of valid usernames.

2.7 Inadequate session management

In case of inadequate session management, an attacker without access rights can hijack a session initiated by another user. If the attacker manages to identify the session ID of a privileged user with extensive privileges in the application, they are able to act as an authorised user. In the case of session fixation, the attacker first allows the web application to set the session ID and then this is passed to an authorised user (for example, via an email link). If an authorised user uses this link and authenticates to the web application with the session identifier provided by the attacker, the attacker can use the web application with the session identifier known to them for the session and with the privileges of the authorised user.

3 Measures

3.1 Life cycle

Implementation

CON.10.M1	Secure authentication in the web application
CON.10.M2	Regulating access to the web application
CON.10.M4	Restricting the use of web application content
CON.10.M5	Restricting data uploads
CON.10.M6	Protection against the unauthorised automatic use of the web application
CON.10.M14	Secure HTTP configuration of web applications
CON.10.M16	Use of multi-factor authentication

Operation

CON.10.M3	Secure session management
CON.10.M7	Protection of confidential data
CON.10.M8	Input validation and output encoding
CON.10.M10	Restriction on the disclosure of sensitive background information
CON.10.M12	Approval of significant changes
CON.10.M13	Web application failure handling
CON.10.M15	Preventing query forgery

Planning

CON.10.M9	Protection against SQL injection
CON.10.M11	Secure software architecture for a web application

Additional advanced measures

CON.10.M17	Preventing resource blocking
CON.10.M18	Cryptographic security of sensitive data

3.2 Key measures

CON.10.M1 Secure authentication in the web application

a. Access to the content of the web application is granted only through user authentication and is governed by secure and appropriate authentication methods.
b. The chosen authentication methods are appropriate and secure and their choice is documented.
c. Wherever possible, centrally managed authentication components (for example, TARA, the Estonian authentication service) are used for authentication.
d. User authentication data is only allowed to be stored in the web application after the risks involved have been weighed and acknowledged. The user will be required to familiarise themselves with the risks and to give their unambiguous ('opt-in') consent before storing their authentication data.

e. The number of allowed unsuccessful login attempts is set in the web application. Once this number is exceeded, additional security measures (for example, blocking user access for a specified period of time) apply.

CON.10.M2 Regulating access to the web application

a. User access rights are limited as necessary.
b. The rights mechanism ensures that users can only perform actions allowed by their rights.
c. User access rights are managed in a central and trusted IT system.
d. In the event of a failure of the access rights system, access to the web application is denied.
e. Access control includes URL calls and object references, in addition to application resources and functions.

CON.10.M3 Secure session management

a. Session ID security is ensured during the creation, transmission, and storage of session IDs on the client computer.
b. Session IDs are generated randomly and with sufficient entropy. The session ID generation function of the web application infrastructure is used whenever possible. To this end, the web application infrastructure is securely configured.
c. The web application allows users to terminate an ongoing session in a controlled and unambiguous manner. After the user logs in again, the session ID is replaced by a new one.
d. The session duration is capped. Inactive sessions are automatically terminated after the specified idle time.
e. After the session is terminated, all session data is deleted on both the server and the client side.

CON.10.M4 Restricting the use of web application content

a. The web application only delivers data and content to users as intended and permitted.
b. Web application forwarding destinations are in a trusted domain.
c. The redirection functionality for users is limited in the web application.
d. When a user leaves a trusted domain, the user is informed.

CON.10.M5 Restricting data uploads

a. The user is only able to save files in a predefined way.
b. The user is not able to change the location of the data storage configured in the web application.
c. The uploading function of the web application is restricted.

CON.10.M6 Protection against the unauthorised automatic use of the web application

a. The web application is protected against automated access.
b. Security mechanisms are implemented in such a way as to ensure that they do not unduly restrict the actions of authorised users.
c. Where RSS feeds or other automated functions are available on the web application, they are taken into account when setting up the security mechanisms.

CON.10.M7 Protection of confidential data

a. From the client's computer to the server, data is transferred only using the HTTP PO ST method.
b. No sensitive data is stored or temporarily buffered on the client's computer.
c. Confidential data on the forms is not stored in the browser in the form of cleartext.
d. The web application's access data is protected on the server by sufficiently strong encryption. Of the authentication credentials, only the 'salted' hash of the password is stored on the server.
e. The source code of the web application is protected against unauthorised access.

CON.10.M8 Input validation and output encoding

a. Input data transferred to the web application is considered potentially dangerous data and must be filtered and validated before further processing.
b. All input data, including secondary data (for example, session identifiers), is validated in a trusted IT system hosted on the server.
c. Incorrect inputs are not automatically processed, where possible. If this cannot be avoided, the input data is made secure.
d. Dangerous symbols are shielded in such a way that they cannot be further interpreted or triggered by the target system.

CON.10.M9 Protection against SQL injection

a. To prevent SQL injection, data is transferred from the web application to the database management system (DBMS) using stored procedures or SQL statements.

b. If neither stored procedures nor SQL statements can be used, SQL queries are protected by other means.

CON.10.M10 Restriction on the disclosure of sensitive background information

a. Webpages and web application responses do not contain information that would help an attacker bypass security mechanism. To this end, it is ensured that:

- only neutral error messages are transmitted;
- no security-related comments or product or version data are disclosed;
- only limited access to security documentation is possible;
- unnecessary files are regularly deleted;
- external search engines use the web application as intended;
- the sharing of information on storage paths is avoided;
- web application configuration files are not located in the root directory of the website.

3.3 Standard measures

CON.10.M11 Secure software architecture for a web application

a. The software architecture of the web application, with all components and dependencies, is documented. The software architecture documentation is updated and adapted as necessary.
b. The development of the web application is based on the approved software architecture documentation. The level of detail of the documentation is sufficient to address issues that developers may have.
c. The software architecture documentation also identifies the non-application components that are necessary for the application to work.
d. The design of the software architecture takes into account which security mechanisms are implemented for which components, how the web application is integrated into the existing infrastructure, and which encryption functions and procedures are used.

CON.10.M12 Approval of significant changes

a. Before making a major change to the web application, user confirmation is required, implemented by re-entering the user password. In the case of multi-factor authentication, it is sufficient to enter an additional authentication factor.
b. If password re-entry cannot be used to authenticate an action, another authentication method is

used.
c. Users are notified of changes via an external communication channel.

CON.10.M13 Web application failure handling

a. The integrity of the web application is preserved when resolving failures that occur during the operation of the web application.
b. The web application logs all error messages generated.
c. The operation that is in progress due to the failure is aborted and access to resources is blocked.
d. The previously reserved web application resources are released during failure handling.
e. If possible, the web application performs the failure handling itself.

CON.10.M14 Secure HTTP configuration of web applications

a. To protect against clickjacking and cross-site scripting, the web application is configured with appropriate HTTP response options (for example, X-FRAME-OPTIONS: deny).
b. The web application uses at least the following HTTP headers:
- Content-Security-Policy (CSP);
- Strict-Transport-Security (HSTS);
- Content-Type;
- X-Content-Type-Options;
- Cache-Control.

c. The web application is configured to be as request-restrictive as possible with HTTP headers.
d. Cookies are assigned the attributes secure, SameSite, and httponly.

CON.10.M15 Preventing query forgery

a. The web application supports cross-site request forgery prevention security mechanisms that distinguish between intended and legitimate website requests from unsolicited requests or unauthorised commands.
b. It is verified whether any additional credential, in addition to the session identifier, is required to access protected resources and functions.
c. The authenticity of the HTTP query is further verified to prove the user's intended query.

CON.10.M16 Use of multi-factor authentication

a. Whenever possible, multi-factor authentication is used to authenticate users of the web application.

3.4 Advanced measures

CON.10.M17 Preventing resource blocking (A)

a. Resource-intensive type operations are avoided to prevent denial-of-service attacks.
b. If resource-intensive type operations cannot be excluded, special security measures are implemented to protect them.
c. The web application logs are monitored and prepared for possible overflow.

CON.10.M18 Cryptographic security of sensitive data (C-I)

a. Sensitive data in the web application is protected by cryptographic mechanisms that provide adequate protection.

OPS: OPERATIONS

OPS.1 Own operations

OPS.1.1 Main IT operations

OPS.1.1.1 IT management in general

1 Description

1.1 Purpose

To establish information security measures as integral to all main aspects of IT management (management of IT assets, IT procurements, running the IT, change management, monitoring, incident management, and decommissioning in IT).

1.2 Responsibility

The IT department is responsible for the implementation of IT management measures.
Additional responsible persons: No additional responsible persons.

1.3 Limitations

The module discusses information security aspects relevant to the entire field of IT management. In addition to focusing on information technology, IT management also handles its secure integration into the business processes of an organisation. The module does not replace the best practice frameworks of IT management, such as ITIL (Information Technology Infrastructure Library) or standards (EVS-ISO/IEC 20000 standards series). The sectoral security measures of IT management are described primarily in the following modules of module group OPS.1.1 Main IT operations: OPS.1.1.2 IT management, OPS.1.1.3 Patch and change management, and OPS.1.1.7 System management. Network management measures are described in module NET.1.2 Network management. The management of access rights is discussed in module ORP.4 Administration of identity and rights and remote management in module OPS.1.2.5: Remote maintenance. Data backups and archiving processes are addressed in modules CON.3 Data backup concept and OPS.1.2.2 Archiving. Modules DER.1 Detection of security incidents, DER.2.1 Handling of security incidents, and DER.2.3 Resolution of large-scale security incidents focus on IT management aspects for handling unusual situations. Fulfilling the management tasks of third parties is covered in modules OPS.2.3: Outsourcing and OPS.3.2 Information security of a service provider. This module does not discuss the special aspects of DevOps methodology or the implementation of information security measures when conducting IT projects.

2 Threats

2.1 Lack of qualified staff

The functioning the business processes of an organisation depends on the smooth operation of IT management. The lack of qualified staff could interrupt the continuity of IT management processes, prolong wait times, and increase the frequency of human errors made by IT personnel. Staff shortages damage the information security aspects of IT management significantly. For example, sufficient monitoring activities and analysis of activity logs cannot be arranged due to the lack of employees. The necessary know-how concentrating only into the hands of a few employees creates dependence on single individuals. A key staff member leaving will create problems with ensuring the availability of IT systems.

2.2 Insufficient documentation of IT management

Conducting IT management processes based on an insufficient or outdated process manual or one containing unauthorised changes could cause interruptions in the work of the IT systems, data leaks, or loss of integrity. Even fixing the consequences of events that have occurred would require a lot more time because there are no detailed instructions for restoring the IT systems and recovering the related data. When external parties are involved in IT management, poor management of activities could cause leaks of sensitive information.

2.3 Limited resources in IT management

When there are no necessary tools for conducting and automating IT management processes, the quality and efficiency of IT management will suffer and so will the functioning of the business processes of the organisation. The time required for eliminating failures increases and the staff is 'putting out fires' instead of improving business processes. In the case of a lack of resources, creating an infrastructure for testing changes in the operational environment and improving IT management processes is not possible.

2.4 Abuses of privileges or confidential information

It is possible to access confidential information and manipulate business-critical data through the abuse of a user account with IT administrator privileges. Unauthorised persons can access a privileged account through phishing or social engineering attacks against an administrator. If the IT management accounts are not closed and the log-in data is not changed when an IT administrator leaves the organisation, they can continue to log into the IT systems, thereby jeopardising the security of the IT systems. A leak of confidential information may be caused by a human error made by an IT administrator - for example, by the latter leaving an access card or a printout of the configuration data of an IT system unattended.

2.5 Unauthorised access to IT devices

When unauthorised persons have access to computers or IT devices used for IT management (for example, equipment is kept in an unlocked room), there is a risk of these devices being used for launching attacks against various IT systems. The risk is greater when the user accounts and data communication interfaces necessary for IT management are weakly protected, for example, by only requiring a password.

2.6 Repudiation or falsification of IT management activities

If an IT administrator submits misinformation about management activities (for example, denies that an important procedure was not carried out), then it could put the availability of an IT system and the security of data in the IT system at risk. When false information is forwarded to an IT administrator (such as manipulated data in an email) about the status of a system or consequent activities, then the administrator might misjudge the existing situation and launch procedures that make the IT systems unavailable to users or threaten the security of IT systems in other ways.

2.7 Neglecting to conduct management activities

When IT management activities are not conducted in accordance with established requirements and process manuals, it could damage the availability and integrity of IT systems. Often, the subsequent maintenance and management requirements of IT components are not taken into consideration when acquiring them. The IT components could be located in places with difficult access or places where the management interfaces necessary for management have not been adopted. In addition, the security of IT systems could be jeopardised when IT management activities are conducted carelessly or incorrectly.

3 Measures

3.1 Life cycle

Planning

OPS.1.1.1.M1 Determining the duties and responsibilities in IT management
OPS.1.1.1.M2 Assigning roles and user privileges in IT management
OPS.1.1.1.M3 Preparing IT management guidelines
OPS.1.1.1.M4 Ensuring the necessary resources for IT management

Operation

OPS.1.1.1.M5 Determining secure standard configurations
OPS.1.1.1.M6 Central management of IT assets
OPS.1.1.1.M7 Secure IT management procedures
OPS.1.1.1.M8 Regular inspection of IT management
OPS.1.1.1.M9 Regular monitoring of IT management
OPS.1.1.1.M10 List of vulnerabilities of IT components

OPS.1.1.1.M13 Security of IT management tools and documentation

OPS.1.1.1.M16 Training of IT management staff

OPS.1.1.1.M18 Relying on external service providers in IT management

OPS.1.1.1.M19 Regular maintenance of IT components

OPS.1.1.1.M20 Monitoring vulnerabilities of IT components

Implementation

OPS.1.1.1.M11 Concluding service level agreements

OPS.1.1.1.M12 Defining IT management processes

OPS.1.1.1.M14 Planning IT management during the acquisition of IT components

OPS.1.1.1.M15 Secure acquisition and use of IT management tools

Emergency response

OPS.1.1.1.M17 Arranging IT management in an emergency

Additional advanced measures

OPS.1.1.1.M21 Monitoring the use of IT management tools

OPS.1.1.1.M22 Automated security testing

OPS.1.1.1.M23 Penetration testing of IT components

OPS.1.1.1.M24 Detailed logs of IT management procedures

OPS.1.1.1.M25 Ensuring the autonomy of IT management tools

OPS.1.1.1.M26 Preventive maintenance of IT components

3.2 Key measures

OPS.1.1.1.M1 Determining the duties and responsibilities in IT management

a. The required IT management activities have been determined for all IT components.
b. IT administrators responsible for the management of IT components have been assigned.
c. The organisation has decided the communication channels for IT management and approved reporting between organisational units, including communication channels for the escalation of incidents.

OPS.1.1.1.M2 Assigning roles and user privileges in IT management

a. Roles for the management of a component and rights and authorisations necessary for the management are assigned to IT components.
b. A role concept for IT management has been prepared, separating roles for IT management from

the roles of everyday IT users.
c. User account with IT management privileges is not used for everyday IT activities.
d. Shared user accounts are allowed to be created and used only in exceptional cases with justification.
e. The aptness of roles and the access rights of administrator accounts are checked regularly. Roles, accounts, and access rights in IT management are updated as required.
f. User accounts of former employees are removed from the IT components at the first opportunity.
g. When decommissioning an IT component, its associated roles and administrator accounts are also deleted.

3.3 Standard measures

OPS.1.1.1.M3 Preparing IT management guidelines

a. Management activities of IT components in use are described in the IT management guidelines.
b. As a minimum, the IT management guidelines cover the following:
- details of the managed IT component;
- necessary management means and tools;
- configuration of IT components;
- adjustments to security settings in the configuration;
- IT management roles and accounts;
- testing of IT components;
- monitoring, logging, and automatic notifications;
- data backups and recovery plans;
- procedure for handling IT incidents;
- planned and unplanned management activities.

c. IT management guidelines are available to authorised persons at all times.
d. IT management guidelines are regularly reviewed to make sure that they are up to date and relevant. The guidelines are updated as required.

OPS.1.1.1.M4 Ensuring the necessary resources for IT management

a. The volume, necessary resources, labour, and know-how for IT management have been analysed for finding sufficient resources.
b. There is a sufficient number of employees with the required know-how for IT management. When

planning human resources, a reserve has been considered, necessary for compensating for short-term absences from work and temporary periods with increased need for personnel.
c. Sufficient material resources are ensured for IT management.
d. Resource requirements are assessed regularly. IT management resources are adjusted according to business needs and valid requirements.

OPS.1.1.1.M5 Determining secure standard configurations

a. Standard configurations offering better security for typical IT components have been created and documented in IT management guidelines.
b. Suitable security settings for all IT components have been developed and implemented on virtualised IT platforms where other IT components run.
c. Configurations of IT components comply with the security requirements of the organisation and take into consideration the manufacturer's recommendations for secure settings for components.
d. Standard configurations are tested before being implemented in the operational environment.
e. Standard configurations are checked regularly to make sure that they are up to date and appropriate. Standard configurations are adjusted according to changes in the technological environment and risk assessments.
f. Standard configurations include version numbers and change histories describing the adjustments that have been made.

OPS.1.1.1.M6 Central management of IT assets

a. IT management procedures include reviewing the existing IT assets and conducting regular inventories of the assets.
b. All IT components that have been installed in the operational environment, are used for testing, or are spares are registered in an asset management system that enables the central management of assets.
c. The asset management system also contains information on existing but decommissioned IT assets.

OPS.1.1.1.M7 Secure IT management procedures

a. Quality requirements have been established for IT management procedures and criteria for measuring the compliance of IT management activities have been determined.

b. IT components are tested before installing them in the operational environment and after making any significant changes. The necessary tests and relevant procedures are described in the IT management guidelines.
c. The IT department is prepared to replace the IT components in use with spare components. They have the necessary resources and procurement contracts.
d. Any work conducted during IT management is documented appropriately and clearly. We recommend using special software, such as the IT Helpdesk application.
e. The quality of IT management procedures and user satisfaction is monitored systematically.
f. Compliance with service level agreements (SLA) and operational level agreements (OLA) is verified systematically.

OPS.1.1.1.M8 Regular inspection of IT management

a. The following is inspected regularly:
- whether IT management procedures are applied to all IT components in the operational environment;
- whether the configurations of IT components comply with the required standard configurations;
- whether the IT management process is integrated into all business processes of the organisation.

OPS.1.1.1.M9 Regular monitoring of IT management

a. IT components are monitored based on a central monitoring plan approved by the management of the IT department.
b. Thresholds have been set for the essential parameters of IT components, deviation from which triggers an automatic notification to IT administrators.
c. The IT department has assigned communication channels for reporting the results of monitoring IT management and has prepared an emergency notification procedure.
d. Based on the monitoring data, it is possible to observe the current status of IT components and changes to the essential parameters over time. The results of monitoring activities are part of the input for planning changes in IT systems.
e. Monitoring information is only sent via secure communication channels.
f. The inclusion of IT systems in the monitoring plan for the IT management is checked periodically. The monitoring plan for the IT management is updated as required.

OPS.1.1.1.M10 List of vulnerabilities of IT components

a. Any known vulnerabilities of IT components are registered in a central list of vulnerabilities.
b. Maintaining a list of vulnerabilities and handling the vulnerabilities are a part of the IT management process.
c. When addressing vulnerabilities, the following is documented:

- any existing security update for fixing known vulnerabilities in an IT component;
- the deadline for installing a security patch in an IT component;
- the need to decommission and/or replace an IT component due to a vulnerability;
- the process of separating an IT component when updating or replacing the component is not possible.

OPS.1.1.1.M11 Concluding service level agreements

a. The IT department has concluded service level agreements (SLA) or operational level agreements (OLA) with its clients, considering the protection requirements of IT components.
b. When deciding the terms and conditions of SLAs, the dependence of organisational units and business processes on the functioning of IT components as well as the protection requirements of business processes have been taken into account.
c. Roles and the corresponding responsibilities established by SLAs are fulfilled.

OPS.1.1.1.M12 Defining IT management processes

a. The IT department has decided and approved IT management processes.
b. The descriptions of each IT management process contain the following information:

- the party initiating the process and participants in the process;
- IT management activities included in the process;
- interfaces (including input and output) with other IT management processes or business processes.

c. The staff of the IT department are familiar with IT management processes and comply with work procedures.
d. Evidence about completing an IT management process is documented. Completing individual process stages is logged as required.
e. Guidelines for situations outside typical IT management processes have been prepared. As a minimum, the following is documented:

- guidelines for instances when an IT management process cannot be carried out;
- guidelines for action in case of errors and deliberate manipulation of the process.

OPS.1.1.1.M13 Security of IT management tools and documentation

a. Only authorised employees of the IT department have access to equipment, tools, and guidelines used in IT management.
b. Authorised persons have access to resources and documentation necessary for IT management when required.
c. When IT management activities are conducted in an operational environment, any sensitive data is only transferred through secure protocols.
d. The use of IT management tools is monitored and patch management is applied to them (see OPS.1.1.3 Patch and change management).

OPS.1.1.1.M14 Planning IT management during the acquisition of IT components

a. When planning IT systems and acquiring IT components, the volume of IT management activities needed to keep them operational as well as requirements related to the IT management processes of the organisation are taken into consideration.
b. An analysis of IT management needs takes into consideration the complexity of the planned IT systems.

OPS.1.1.1.M15 Secure acquisition and use of IT management tools

a. Planning IT management resources and acquiring and using management tools is based on the actual needs of IT component management.
b. IT management processes and the necessary resources have been approved by all business units of the organisation.
c. As a minimum, the IT management network is logically separated from other networks of the organisation (see NET.1.1 Network architecture and solution). Any additional segmentation of resources is decided based on functional interdependencies between IT management tools, the information security policy, and the protection requirements of the information.

OPS.1.1.1.M16 Training of IT management staff

a. Training plans for staff involved in IT management make provisions for several staff members having the necessary skills and qualifications to manage an IT component.
b. As a minimum, training covers the following topics:

- standard configurations and hardening of information security;

• security settings specific to IT components and management tools in use;
• typical errors in management tools and fixing them;
• links and interfaces between IT management processes.

c. When acquiring new IT components, trainings are planned to learn relevant IT management procedures.

OPS.1.1.1.M17 Arranging IT management in an emergency

a. Conditions have been defined for the implementation of emergency procedures in IT management.
b. In the case of long-term disruptions or emergencies in IT systems, a disaster recovery manual for IT management has been prepared.
c. The disaster recovery manual for IT management lists which IT components are essential for the organisation to continue operating at a minimum acceptable level and which IT components are ensured support as a priority.
d. As a minimum, disaster recovery guidelines include the following:
• disaster recovery plans for resuming normal operation after an emergency;
• guidelines for restoring IT components;
• instructions for alleviating the impact of a long-term interruption in critical business processes.

OPS.1.1.1.M18 Relying on external service providers in IT management

a. The activities of external service providers involved in IT management are regulated through agreements and SLAs.
b. Communication channels and detailed contents of the service have been agreed with the service provider. This is particularly important when several service providers are used in a narrow service sector.
c. Service providers are documented. The compliance of activities of service providers is inspected regularly.

OPS.1.1.1.M19 Regular maintenance of IT components

a. IT components receive regular maintenance. Completed maintenance operations and upgrades are documented.
b. Individuals responsible for the maintenance of IT components are assigned.
c. Valid information security requirements are complied with during maintenance.

d. The work of external maintenance specialists has been approved by relevant parties ahead of time. A contact person has been appointed to coordinate the maintenance activities of the third parties and, if necessary, to inspect and approve the execution of work.

OPS.1.1.1.M20 Monitoring vulnerabilities of IT components

a. IT administrators regularly monitor and analyse information about known vulnerabilities and releases of security patches for the IT components in use.
b. IT components are tested to identify any vulnerabilities. The suitable scope, depth, and methodology of testing have been decided for each IT component. Any vulnerabilities found during testing are registered.
c. Known vulnerabilities of hardware, operating systems, and applications are eliminated at the earliest opportunity. If a manufacturer has not released a security patch for a vulnerability, additional security measures are used for the protection of the IT system.
d. Hardware, operating systems, applications, and services that have no manufacturer support and have known security vulnerabilities are decommissioned.

3.4 Advanced measures

OPS.1.1.1.M21 Monitoring the use of IT management tools (C-I-A)

a. The use of the management tools of IT components is monitored with security monitoring tools covering the entire organisation.
b. IT management tools have been integrated with the monitoring data from an automated intrusion detection system (IDS) for the central identification of security events in real time.

OPS.1.1.1.M22 Automated security testing (C-I-A)

a. IT components are tested regularly with automated testing tools to identify vulnerabilities.
b. The results of vulnerability scanning are logged automatically and made available to other relevant tools.
c. Upon the discovery of a critical vulnerability, an automatic notification is sent to authorised employees.

OPS.1.1.1.M23 Penetration testing of IT components (C-I-A)

a. Regular penetration testing of IT components is carried out based on the concept of organisational security testing.

OPS.1.1.1.M24 Detailed logs of IT management procedures (C-I-A)

a. All IT management procedures are logged in a traceable and verifiable manner.

OPS.1.1.1.M25 Ensuring the autonomy of IT management tools (C-I-A)

a. IT management tools can be used in the case of interruptions of the network connection or other external influence.
b. Interdependency between IT management tools has been minimised as much as possible. When configuring the tools, situations where the failure of one tool would interrupt the operation of another tool are avoided.

OPS.1.1.1.M26 Preventive maintenance of IT components (I-A)

a. The maintenance of IT components is planned and conducted at reduced intervals to prevent potential failures.

OPS.1.1.2 IT management

1 Description

1.1 Purpose

Presenting measures for the safe management of IT systems and networks.

1.2 Responsibility

The IT department is responsible for the implementation of the IT management measures.
Additional responsible persons: Human resources department.

1.3 Limitations

The module presents the general measures for IT management. Access rights are discussed in the module ORP.4 Administration of identity and rights; the management of changes is discussed in OPS.1.1.3 Patch and change management. Remote management of IT systems is described in the module OPS.1.2.5: Remote maintenance.
Fulfilling the management tasks of third parties is covered in the modules OPS.2.1 Outsourcing and OPS.3.1 Information security of the service provider. IT management in case of an error is described in the module group DER.2 Management of security incidents.

2 Threats

2.1 Problems due to unregulated duties

If the IT management tasks (for example, regarding planning, installation, documentation, patch management, or supervision) are not clearly defined or the employees are not familiar with or do not understand the procedure for IT management, important security activities might be left unrealised.

2.2 Lack of competent staff

Often, only one IT administrator has the skills and necessary knowledge for managing a complex IT system. If they have no replacement with the necessary training, problems might arise with ensuring the compliant and secure functioning of the IT system, should the IT administrator leave.

2.3 Abuse of administrative privileges

Persons who have access to documents and data in a database might abuse their greater rights in their own interests or the interests of outsiders. An IT administrator can be pressured or otherwise influenced to grant access to data.

2.4 Facilitating attacks

Attacks on an IT system are facilitated by errors of the IT administrator caused by negligence while configuring the IT system. The security controls meant for the protection of the IT system are not always implemented (e.g. due to convenience or some other reason). A lack of security awareness, the administrators not having sufficient time, and the absence of procedures create vulnerabilities which an attacker can easily exploit.

2.5 Disturbance of work

Conducting administrative work usually affects the functioning of IT systems. If the effect of administrating IT systems on the simultaneous use of IT systems is not taken into consideration and the administrative work is not planned for non-working hours, it might cause significant disruptions in the business process.

2.6 No option for incident analysis

In case of a security incident, it is difficult to determine the nature and the extent of the attack. If the IT incident or the planned change to the system caused by an unauthorised alteration is not identified quickly, the attacker can operate freely in the network.

2.7 Errors in IT System Management

When performing IT system management operations, human error by the IT administrator cannot be ruled out. For example, the IT administrator might confuse open console windows and enter an incorrect command line. Faulty management operations can have significant negative consequences.

2.8 Disruption of IT Systems Operations

Performing management operations usually affects the functioning of IT systems. If the impact of these operations on the simultaneous use of IT systems is not considered and the operations are not scheduled outside of business hours, it can significantly disrupt the business process.

3 Measures

3.1 Life cycle

Planning

OPS.1.1.2.M2	Procedure for the replacement of IT administrators
OPS.1.1.2.M21	Determining the roles in the management of IT systems
OPS.1.1.2.M7	Determining the duties of an IT administrator
OPS.1.1.2.M23	Principles for assigning roles in the management of IT systems and user privileges
OPS.1.1.2.M27	Alternative solution to a central IT management tool

Operation

OPS.1.1.2.M4	Termination of employment of an IT administrator
OPS.1.1.2.M6	Administrative account security

OPS.1.1.2.M22 Separation of the management of IT systems from regular work tools

OPS.1.1.2.M8 Application management

OPS.1.1.2.M11 Documenting administrative activity

OPS.1.1.2.M20 Regular commissioning of equipment

OPS.1.1.2.M24 Inspecting the management activities of IT systems

OPS.1.1.2.M25 Timing the conduct of IT management activities

OPS.1.1.2.M26 Backup of the configuration of IT components

OPS.1.1.2.M28 Logging the management activities of IT systems

Implementation

OPS.1.1.2.M5 Demonstrating operations in the management of IT systems

OPS.1.1.2.M16 Technical allocation of administrative access

Additional advanced measures

OPS.1.1.2.M18 Full logging of administrative operations

OPS.1.1.2.M17 Four eyes principle for IT administrators

OPS.1.1.2.M19 Guaranteeing high availability

OPS.1.1.2.M29 Monitoring the functioning of the management tools of IT systems

OPS.1.1.2.M30 Integrating IT systems management with a security information management system

3.2 Key measures

OPS.1.1.2.M2 Procedure for the replacement of IT administrators

a. IT system administrators have substitutes with suitable qualifications for IT systems management who are familiar with the specific systems or have completed the relevant training.
b. The names and contact details of substitutes have been documented.
c. A procedure for granting access rights to the substitutes is in place.
d. Access to the administrative accounts of IT systems in an emergency situation is only granted to authorised persons. The necessary access information is stored in a safe location that is accessible to the authorised individuals.

OPS.1.1.2.M4 Termination of employment of an IT administrator [human resources department]

a. When terminating the employment of an IT administrator, all personalised administrative accounts related to that person are blocked and their access rights are removed immediately (incl. access to

external services).
b. All passwords, access codes, and secret cryptographic keys known to the IT administrator who has left work are changed.
c. If the IT administrator who has left employment was an appointed contact person for third parties (e.g. by an agreement or as an administrative contact person), the relevant parties are informed about the termination of employment and a new contact person is appointed.
d. The measures are applied even if the IT administrator's duties were assigned to an individual not employed by the company.

OPS.1.1.2.M5 Demonstrating operations in the management of IT systems

a. Every IT system administrator and every substitute IT system administrator has a personal privileged account which is used only for administrative operations.
b. Only personal administrative accounts are used for administrative operations.
c. All administrative operations (including what was done, when, and by whom) can be proven after the fact.

OPS.1.1.2.M6 Administrative account security

a. The administrative accounts are protected with suitable authentication mechanisms. If passwords are used, then the same passwords are not used in other administrative zones. In case of a higher protection requirement, multi-factor authentication is implemented.
b. An IT administrator has a user account with regular rights for daily tasks; the privileged account is not used for performing daily duties.
c. Only the IT administrators have access to the administrative interface and the administrative functions of the IT system.
d. If the local console is not used for system management, then the use of administrative accounts is protected with secure network protocols (e.g. SSH, TLS) and with sufficiently strong encryption.

OPS.1.1.2.M21 Determining the roles in the management of IT systems

a. Roles in the management of IT systems have been determined. When determining the roles, the needs of the IT systems and the principle of minimality of user privileges have been taken into account.

b. When determining the roles, the protection requirement of the IT system has been considered; e.g. the separation of roles of managing the operating system and applications should be considered.

OPS.1.1.2.M22 Separation of the management of IT systems from regular work tools

a. The tools for IT management are clearly distinguishable from tools for regular work.
b. Applications for IT management are not used for other work tasks aside from IT management operations.
c. User accounts and passwords for logging in, used for IT management, are kept separate from other accounts and passwords.

3.3 Standard measures

OPS.1.1.2.M7 Determining the duties of an IT administrator

a. When duties are divided between several IT administrators, all tasks are covered and areas of responsibility clearly defined.
b. A responsible manager has been appointed for each IT system and application.
c. When allocating the duties of the IT administrator, the principle of separation of duties has been taken into consideration. Certain roles are not compatible with the role of an administrator (such as an IT auditor).
d. The rights and obligations of an IT administrator are updated regularly through the job description for IT administrators.

OPS.1.1.2.M8 Application management

a. The division of tasks between the application and system managers has been defined and documented.
b. Potential points of contact between the division of tasks of persons responsible for the management of application and IT systems have been coordinated (e.g. when employees are replaced).
c. If an IT administrator has to intervene in the running of an application (e.g. when changing the version), it is first coordinated with the users of the application while considering the needs of the users.

OPS.1.1.2.M11 Documenting administrative activity

a. All changes in the IT system made in the course of administrative activities are documented. Documentation demonstrates clearly which changes have been made at which time by whom and for what reason.
b. Information on the changes must also be available to the substitutes when an IT administrator is away.

OPS.1.1.2.M16 Technical allocation of administrative access (C-I-A)

a. Access to administrative interfaces is restricted by technical measures (e.g. only allowed from a specific network segment).
b. Persons who do not belong in the administrative team do not have access to administrative interfaces.
c. Administrative access for IT systems in other security zones has been created through the jump server of the respective security zone. Other access routes from other systems or network segments have been blocked.
d. Administrative interfaces should not be directly accessible from an external network.

OPS.1.1.2.M20 Regular commissioning of equipment

a. The organisation has an overview of all devices that may impact the information security situation. The register of devices corresponds to the actual situation.
b. In addition to IT systems and industrial automation components, the register includes the internet of things (IoT) devices.
c. Compatibility and security are taken into account when procuring devices. Wherever possible, new equipment is tested before it is purchased.
d. Before the introduction, devices pass a coordination procedure, during which the devices are labelled and registered (in the asset register, for example).

OPS.1.1.2.M23 Principles for assigning roles in the management of IT systems and user privileges

a. The organisation has established principles for assigning roles and user privileges in the management of IT systems.
b. The principles for assigning roles and user privileges in the management of IT systems stipulate how a role:

- is requested;
- is created;
- receives rights associated with it;
- is linked to a specific person.

OPS.1.1.2.M24 Inspecting the management activities of IT systems

a. Before starting the management activities of IT systems, the organisation makes sure that the planned activities correspond to the terms of reference.
b. Before starting the management activities of IT systems, the organisation makes sure that the planned activities will not have a negative impact on the use of IT management tools.
c. After completing the management activities of IT systems, the organisation makes sure that the configuration of the managed IT component corresponds to the desired target state.
d. Management activities of an IT system with an increased need for security are inspected by a person who is not the one conducting the activities.

OPS.1.1.2.M25 Timing the conduct of IT management activities

a. Before conducting any IT management activities, users of the IT system are informed in advance and/or the activities are conducted during a predetermined period for planned maintenance.

OPS.1.1.2.M26 Backup of the configuration of IT components

a. Before starting any management activities of an IT component, the party conducting it makes sure that a backup of the current configuration of the IT component has been made.
b. Prior to a management activity that might have negative consequences, the configuration of an IT component is copied right before starting the activity.

OPS.1.1.2.M27 Alternative solution to a central IT management tool

a. If necessary, a central IT management tool can be replaced by ensuring access to relevant management networks through a secure jump server.
b. Where a jump server is not used, direct physical access to the IT component is ensured for management activities.

OPS.1.1.2.M28 Logging the management activities of IT systems

a. All activities and access attempts related to an administrative account are logged. The integrity of the logged data is protected.
b. The management activity logs of IT systems are stored for a sufficiently long period.

3.4 Advanced measures

OPS.1.1.2.M18 Full logging of administrative operations (C-I)

a. In security-critical systems, all commands and functions executed by the system administrator are logged in addition to system logins.
b. IT system administrators do not have the rights to change or delete log files.
c. Log files are stored intact for the period that corresponds to the protection requirement.

OPS.1.1.2.M17 Four eyes principle for IT administrators (C-I)

a. Access to security-critical systems has been regulated to always require two employees (e.g. by dividing the password of the administrative account into two parts, of which each part is only known to one of the IT administrators).
b. When conducting administrative procedures, one IT administrator performs the required administrative duties and the other monitor their activity.

OPS.1.1.2.M19 Guaranteeing high availability (A)

a. The redundancy of the administrative tools of IT systems has been ensured.
b. In the case of a failure of an administrative tool of an IT system, administrative operations of the IT systems can still be carried out without any significant hindrances.

OPS.1.1.2.M29 Monitoring the functioning of the management tools of IT systems (A)

a. Availability requirements have been established for IT management tools.
b. The availability parameters of IT management tools are regularly monitored and the IT administrator responsible is informed of any deviations.

OPS.1.1.2.M30 Integrating IT systems management with a security information management system (C-I-A)

a. Logging the management activities of IT systems is interfaced with a security information and event management (SIEM) system.

OPS.1.1.3 Patch and change management

1 Description

1.1 Purpose

To present measures for applying, managing, and optimising the patch and change management of an organisation.

1.2 Responsibility

The IT department is responsible for the application of the patch and change management measures.
Additional responsible persons: Responsible specialist.

1.3 Limitations

The module discusses the installation of software updates and the information security aspects of change management. Module groups SYS and APP describe updating specific IT systems. Module OPS.1.1.6 Software testing and onboarding covers the testing of patches and changes as well as their installation in an operational environment. Changes made in the course of a software update are described in module CON.8 Software development.

2 Threats

2.1 Inadequately established obligations

Unclear, undetermined, or overlapping work duties in patch and change management decelerate the process and cause errors. Premature approval of patches and changes without testing and taking into account all aspects could significantly affect the security of the IT systems. If the security patches are not installed or are installed too late, then it could affect the confidentiality and integrity of IT systems.

2.2 Inadequate exchange of information when managing changes

If the patch and change management is unregulated in an organisation and the relevant persons fail to communicate sufficiently, it could lead to wrong decisions or being late with the installation of changes. In case of insufficient exchange of information, IT management becomes inefficient and security vulnerabilities are created. A change that has not been previously announced could create a work stoppage because the user does not know how to act in the new situation.

2.3 Lack of consideration for business processes

Uncontrolled changes could endanger the functioning of business processes and cause extensive malfunctions in the affected IT systems. Unless the changes have been planned and tested with relevant main units, the effect, the level of priority, and the expected security level of the changes could be misjudged. The result might not correspond to the actual business requirements.

2.4 Limited resources for patch and change management

If patch and change management lacks suitable employees, the cooperation between the IT department and business departments could suffer. In case of a lack of resources, it is impossible to create a compliant infrastructure for the test and operational environment. Staff shortages are particularly important when immediate action is necessary; for example, when applying emergency patches.

2.5 Problems with the automatic installation of patches and changes

When using patch management software centrally, faulty updates could be issued for the entire IT system, causing extensive security problems. If the IT devices are not permanently available in the local area network, a system that installs security patches at certain intervals might not update some of the devices.

2.6 Limited recovery options in patch and change management

When patches or changes are installed without making provisions for recovery, repairing an IT system quickly in case of an error becomes impossible. The same applies when the software recovery procedures are not efficient or do not function in all instances.

2.7 Incorrect assessment of the priority of patches and changes

When making a mistake in assessing the level of priority of a change, some significant patches could be installed last, and therefore, the related security risk lasts longer. The tool for patch and change management might be faulty, causing it to submit incomplete or erroneous data about the patch or change.

2.8 Manipulation of data and tools when managing changes

If an attacker can take over central tools for patch and change management, then they can spread manipulated software to many IT systems simultaneously. When an external partner manages these tools, then the attack can be initiated from the partner's network.

3 Measures

3.1 Life cycle

Planning

OPS.1.1.3.M1 Procedure for patch and change management
OPS.1.1.3.M2 Assigning responsibility
OPS.1.1.3.M5 Handling requests for changes
OPS.1.1.3.M8 Secure application of patch and change management tools

Operation

OPS.1.1.3.M3 Secure configuration of automatic updates
OPS.1.1.3.M15 Regular updates of IT systems
OPS.1.1.3.M6 Approval of changes
OPS.1.1.3.M7 Reconciliation of change management with business processes
OPS.1.1.3.M10 Ensuring the integrity and authenticity of software products

Implementation

OPS.1.1.3.M9 Procedures for testing and implementing new hardware
OPS.1.1.3.M11 Continuous documentation of information processing

Additional advanced measures

OPS.1.1.3.M12 Using change management tools
OPS.1.1.3.M13 Assessing the efficiency of changes
OPS.1.1.3.M14 Synchronisation of changes

3.2 Key measures

OPS.1.1.3.M1 Procedure for patch and change management [responsible specialist]

a. A patch and change management procedure has been established for making changes to the IT components, software, and configuration data.
b. The patch and change management procedure regulates the planning, approval, and documentation of the installation of software patches and updates.
c. Patches and updates are tested before implementation (see also OPS.1.1.6 Software testing and onboarding).
d. If the installation of patches and updates fails, a procedure for undoing the changes has been prepared.
e. In the case of bigger changes, the information security manager is included in the planning of changes. The required level of security is maintained both during and after implementing the change.

OPS.1.1.3.M2 Assigning responsibility

a. All business processes have assigned persons who are responsible for patch and change management.
b. The person responsible for patch and change management classifies and accepts change requests and coordinates the implementation of changes.
c. In an organisation with a complex IT infrastructure, a change advisory board, which meets at set intervals, supports the person responsible; the board includes the representatives of the main units of the organisation in addition to the individuals involved in the technical application of changes.

OPS.1.1.3.M3 Secure configuration of automatic updates

a. When implementing new products, their upgrade mechanisms are checked along with their configuration. Automatic updates are configured according to the organisational requirements for patch management.
b. If necessary, the update requests are blocked from the public update server, as is the automatic initiation of installing updates.
c. If possible, an internal update server is implemented (e.g. Windows Server Update Services, WSUS). In this case, the update server communicates directly with the servers of the manufacturer and downloads the desired updates for installation at a suitable time.
d. Security patches are downloaded to mobile devices which might often be outside the company

network straight from the update server of the manufacturer and as quickly as possible after the update is published.

OPS.1.1.3.M15 Regular updates of IT systems

a. Firmware, operating systems, and applications are updated regularly. Updates are done as quickly as possible after the publication and testing of a security update.
b. Patches and changes are installed according to their level of priority and the urgency of installation.
c. After updates are installed, all necessary devices and applications are checked to make sure that they have been updated.
d. If it is decided that a security update is not going to be installed, then the decision to that effect and the reason for not installing it are documented.
e. Upon the end of the manufacturer's support, an analysis will be conducted to determine how the absence of further security patches impacts the secure use of devices or applications. Insecure devices or applications will be removed from use.

3.3 Standard measures

OPS.1.1.3.M5 Handling requests for changes [responsible specialist]

a. Requests for changes are submitted, registered, and documented according to the procedure for patch and change management.
b. When planning changes, the effect of the change on the functioning of the organisation is assessed and technical and human resources as well as deadlines for implementation are decided.
c. The person responsible for implementing the change checks whether the aspects related to information security have been sufficiently taken into account with the request for change.

OPS.1.1.3.M6 Approval of changes

a. The coordination process of changes includes all relevant target groups, including information security.
b. Target groups involved with changes can express their opinion on the changes to avoid unwanted changes from the point of view of the target group.
c. Time-critical changes can be approved through a simplified process.

OPS.1.1.3.M7 Reconciliation of change management with business processes

a. When planning changes, the needs related to the main activity of the organisation and their effect on the business processes are primarily taken into account, incl. from the point of view of information security.
b. All entities affected by changes are informed in a timely manner about the upcoming changes.
c. The selected time for the implementation of changes should disturb business processes as little as possible. When the disruption of business process is unavoidable, the possible effects of the disruption are taken into account when making the decision.
d. The management of the organisation can change the priorities and planned execution deadlines for hardware and software if necessary.

OPS.1.1.3.M8 Secure application of patch and change management tools

a. When selecting tools for patch and change management, support for various software platforms, the frequency of releasing updates and verifying them, the flexibility of the configuration, and the possibility to reverse the changes are considered.
b. Security requirements for patch and change management have been established, which pertain to the secure management of the tools and the requirements for logging, data backup, and emergency response.

OPS.1.1.3.M9 Procedures for testing and implementing new hardware

a. Before implementation, new hardware is tested in a test environment that is separated from the operational environment and has been created specifically for this reason.
b. The functionality, compatibility, and absence of unwanted side effects of the product are checked during testing. Testing objectives are chosen depending on the nature of the hardware.
c. Test results of the hardware and results for the approval for commissioning are documented.
d. If any faults are discovered in the hardware despite completing the testing and approval process, an error correction process is initiated.

OPS.1.1.3.M10 Ensuring the integrity and authenticity of software products

a. Software and its updates are acquired only from known trustworthy suppliers.
b. Before installing a package, its authenticity is verified based on a checksum or a signature, for example.

c. The organisation has the necessary tools for verification that are needed for checking integrity and authenticity.

OPS.1.1.3.M11 Continuous documentation of information processing

a. The organisation has an established procedure for documenting changes made to the IT systems.
b. It has an up-to-date documentation on the configuration of IT applications and IT components, added components, users, data backup, malfunctions and errors that have been detected and rectified, and the completed maintenance operations.

3.4 Advanced measures

OPS.1.1.3.M12 Using change management tools (A)

a. When selecting change management tools, the performance of the installation of changes and the capability to restore the situation prior to the change in case of an error in many work stations or servers simultaneously are taken into account.
b. The tool for patch or change management allows for deliberate interruption of the installation if necessary. Interruption of the update installation has been tested beforehand.

OPS.1.1.3.M13 Assessing the efficiency of changes [responsible specialist] (I-A)

a. In order to assess the effectiveness of a change, follow-up testing is conducted to compare the post-change situation with the situation before the change.
b. Follow-up testing is conducted by users who are familiar with the business processes of the organisation as well as the valid quality and security requirements, and who can identify and assess potential errors.
c. The results of the follow-up tests are documented.

OPS.1.1.3.M14 Synchronisation of changes (C-I-A)

a. Patches and changes are installed in all IT systems as quickly as possible at the same time.
b. There is a procedure and tools which allow checking whether the change has been installed in all targets.
c. Changes which are unavoidably late (in mobile IT systems, for example) are implemented at the earliest opportunity.

OPS.1.1.4 Protection against malware

1 Description

1.1 Purpose

To present measures for organising protection against malicious programs.

1.2 Responsibility

The IT department is responsible for implementing the measures of the module Protection from malicious programs.
Additional responsible persons: User.

1.3 Limitations

Specific requirements for the protection of specific IT systems of an organisation from malicious programs have been listed in the relevant SYS modules (e.g. SYS.2.2.3 Windows 10 client).
The removal of identified malicious programs and restoring IT systems is discussed in the modules DER.2.1 Handling of security incidents and DER.2.3 Resolution of large-scale security incidents.
The user training is covered in the module ORP.3 Raising awareness and providing training on information security.

2 Threats

2.1 Software vulnerabilities and downloading malicious code

When the IT systems are not sufficiently protected from malicious programs (e.g. by the timely installation of patches and secure configuration of applications), an attacker can take advantage of the vulnerabilities of the software to install malicious code. Even visiting a malicious website is enough to make it possible to abuse the vulnerabilities of a browser or some installed plugin (such as Java or Adobe Flash) and infect the IT system. IT systems that are not regularly updated are particularly at risk (many smart phones, for example).

2.2 Extortion with ransomware

Ransomware is a widespread type of malware, which encrypts the data in the infected IT system. To achieve this, attackers use encryption methods which allow decryption only with a key known to the attacker. The key is published only after a large sum has been transferred to the attackers. If there is no efficient protection from malware and additional measures have not been implemented (such as data backup), then a ransomware attack could cause great financial and reputational damage.

2.3 Targeted and social engineering attacks

Often, adapted malicious programs which virus protection programs cannot identify yet are used for attacking organisations. For example, managerial staff is enticed to open malicious email attachments via social engineering during an attack. If an attacker has managed to infect one computer in this manner, then they can widen their activity in the organisation through that.

2.4 Botnets

Malicious programs can also spread botnets in the IT systems of an organisation. An attacker who controls thousands of computers in the botnet can use the botnet for various purposes, such as sending spam or initiating a denial-of-service attack. Even if there is no direct negative effect on the availability and integrity of the services and IT systems of an organisation, it is a violation of law that causes reputational damage.

2.5 Infecting production systems and devices in the Internet of Things

In addition to normal IT systems, malicious programs are increasingly used to attack devices which, at first glance, do not seem like usual targets. For example, an attacker could infect a surveillance camera, which can be accessed through the internet, for espionage or use smart lighting which has been connected to a network as a part of a botnet if such devices are not sufficiently protected from malware. When manipulating industrial control systems through malicious programs, an attacker can damage property or cause long-lasting work stoppages.

3 Measures

3.1 Life cycle

Planning

OPS.1.1.4.M1 The concept of anti-malware

OPS.1.1.4.M7	Increasing the awareness of users

Implementation

OPS.1.1.4.M2	Using system-specific security mechanisms
OPS.1.1.4.M5	Application of anti-malware

Acquisition

OPS.1.1.4.M3	Selecting anti-malware for endpoints

Operation

OPS.1.1.4.M6	Updating virus protection programs and virus signature data
OPS.1.1.4.M9	Informing about an infection with a malicious program

Additional advanced measures

OPS.1.1.4.M10	Using a special environment for analysis
OPS.1.1.4.M11	Application of several scanning engines
OPS.1.1.4.M12	Application of data carrier analyses
OPS.1.1.4.M13	Handling untrusted files
OPS.1.1.4.M14	Selecting and implementing information security products for protection against targeted attacks

3.2 Key measures

OPS.1.1.4.M1 The concept of anti-malware

a. A concept has been prepared which determines the IT systems that are protected from malware and the manner of protection.
b. The use of IT systems is avoided until they can be reliably protected from malware.
c. The concept of anti-malware is regularly reviewed and, if necessary, updated.

OPS.1.1.4.M2 Using system-specific security mechanisms

a. The types of security mechanisms that are added to the IT systems in use are known.
b. All IT system security mechanisms have been implemented, except when at least an equivalent replacement mechanism exists or when there are compelling reasons for the non-application of a security mechanism.
c. The instances of conscious non-application of security mechanisms are documented with the relevant justification.

OPS.1.1.4.M3 Selecting anti-malware for endpoints

a. The selection of anti-malware is based on the used platforms, other existing security mechanisms, and the presumed efficiency and detection capability of the anti-malware.
b. Products that have been adjusted for business uses and have valid maintenance and support services are used at endpoints.
c. When selecting anti-malware, the data protection and confidentiality requirements are taken into consideration.

OPS.1.1.4.M5 Application of anti-malware

a. Anti-malware has been tested before being approved for implementation.
b. Anti-malware is configured according to the use environment.
c. If some of the security functions of the product have been deactivated, then it must have a documented reason.
d. The rights of users for changing the security settings of anti-malware are restricted.

OPS.1.1.4.M6 Updating virus protection programs and virus signature data

a. The virus protection program and virus signature data are updated regularly according to the recommendations of the creator of the software.
b. In the case of virus protection program updates, the documentation of changes is consulted and the configuration of software is changed if necessary.

OPS.1.1.4.M7 Increasing the awareness of users [user]

a. Potential threats related to malware are regularly explained to users.
b. Instructions for avoiding dangers related to malware have been shared with the users.
c. The users know that files from untrusted sources should not be opened.
d. The users are obligated to inform the contact person appointed by an organisation about an infection or a suspicion of infection with malware.

3.3 Standard measures

OPS.1.1.4.M9 Informing about an infection with a malicious program

a. When malware is detected, the anti-malware application notifies the central handling point and blocks the infected program.
b. The responsible employee makes a decision on whether the malware notification could mean a security incident as well as on the subsequent steps.
c. A procedure has been established for handling the incident notification and warnings of the anti-malware application.
d. An action plan for the removal of malware and for restoring the situation before the infection has been documented and tested.

3.4 Advanced measures

OPS.1.1.4.M10 Using a special environment for analysis (C-I-A)

a. Well-known web-based virus scanning tools are used for the automated analysis of files with a suspected infection.
b. The users of the communication network of the Estonian state authorities and entities and partners from the private sector use the web-based tool at irma.cert.ee to check suspicious attachments sent via email and other files with an uncertain origin.

OPS.1.1.4.M11 Application of several scanning engines (C-I-A)

a. Various anti-malware tools with scan engines have been applied in systems with a higher protection requirement to increase their detection capacity.

OPS.1.1.4.M12 Application of data carrier analyses (C-I-A)

a. Before a data carrier that has been received from an external party is connected to the IT systems of an organisation, a specially configured computer is used for checking the data carrier.

OPS.1.1.4.M13 Handling untrusted files (C-I-A)

a. Untrusted files can only be opened in specially configured computers that are isolated from the rest of the IT system.
b. The contents of dubious files are converted into a safe format for further processing or they are printed out.

OPS.1.1.4.M14 Selecting and implementing information security products for protection against targeted attacks (C-I-A)

a. Products that offer more security than conventional products and have additional protective functions are selected in the case of a higher protection requirement.
b. The security effect and compatibility of the selected product is tested in the prepared test environment before granting approval for implementation.

OPS.1.1.5 Logging

1 Description

1.1 Purpose

To present measures for the safe collection, storage, analysis, and appropriate disposal of logging data.

1.2 Responsibility

The IT department is responsible for implementing the logging measures.
Additional responsible persons: Responsible specialist.

1.3 Limitations

The logging of specific IT systems and applications and their protection is additionally discussed in thematic modules (e.g. the logging of operating system events is discussed in the modules SYS.1.1 Server in general and SYS.2.1 Client computer in general). Archiving of log data is covered in the module OPS.1.2.2 Archiving. Measures for personal data processing are presented in the module CON.2 Personal data protection. Using IT system logs for the detection and treatment of security incidents is described in the modules DER.1 Detection of security incidents and DER.2 Management of security incidents.

2 Threats

2.1 Missing or insufficient logging

If logging is not activated when configuring IT systems or if logging is impossible, security incidents remain unregistered and attacks unidentified. An attack is also not identified when logging is applied but log data is not analysed. In addition, an attack remains undiscovered when the log data does not include necessary and relevant information.

2.2 Inadequate selection of relevant log data

Analysing a large amount of log messages in real time requires a lot of computer and human resources. If only a small part of the collected data is informative, analysing log data becomes even more time-consuming due to the abundance of information. If the working memory of the IT system of log infrastructure is insufficient, it might cause the log data that contains important information to be overwritten or deleted prematurely.

2.3 Unsynchronised time during logging

If the clocks of all IT systems of an organisation are not synchronised, then the log data of various IT systems does not correlate and can cause erroneous event messages. Analysing log data that is collected in this manner is complicated and it might be impossible to use these logs as evidence in IT forensics.

2.4 Bad planning of logging

If logging is not planned in detail, the IT systems might be unmonitored and security incidents pertaining to these IT systems may remain unidentified. If the use of personal data is not logged, then the violations of data protection might remain unidentified.

2.5 Loss of confidentiality and integrity of log data

Certain IT systems create log data that can be linked to natural persons. If log data which includes user names, IP addresses, email addresses, and computer names is not forwarded in an encrypted manner or stored safely, then this data can be copied and intercepted. An attacker may gain access to confidential information or use the collected personal data for learning about the organisational structure and organising more targeted attacks.

2.6 Incorrectly configured logging

If the logging rules of an IT system are configured incorrectly, the system might fail to log important data. If excessive data is logged (e.g. in case of personal data when it is not necessary), the organisation might be in violation of legislative requirements. If log data cannot be linked to other information, then analysing logs becomes more complicated and security incidents might remain undetected.

2.7 Failure of data sources

If the IT systems do not forward the required log data, then detecting security incidents based on log data becomes impossible. The reasons for the failure of data sources could be malfunctions in hardware and software, but also poorly managed IT systems. If the failure of data sources remains undetected, it leaves a misleading impression of the security of an organisation. An attacker who has infiltrated the systems might be undetected for a long time.

2.8 Log infrastructure that is too small

In case of complex information systems, the requirements for logging also become more stringent. If the log infrastructure does not enable storing and there is a lot of log data to be analysed. If the log infrastructure does not allow it, then the security events cannot be analysed or are analysed insufficiently.

3 Measures

3.1 Life cycle

Planning

OPS.1.1.5.M1	Logging rules
OPS.1.1.5.M3	Configuring the logging of events
OPS.1.1.5.M6	Establishing a central log infrastructure

Operation

OPS.1.1.5.M4	Synchronisation of time
OPS.1.1.5.M5	Compliance with the legal framework conditions
OPS.1.1.5.M8	Archiving log data
OPS.1.1.5.M9	Provision of log data for analysis
OPS.1.1.5.M10	Protection of log data from unauthorised access

Additional advanced measures

OPS.1.1.5.M11 Increasing logging capacity

OPS.1.1.5.M12 Encryption of log data

OPS.1.1.5.M13 Logging system with high availability

OPS.1.1.5.ME1 Log hash chaining

3.2 Key measures

OPS.1.1.5.M1 Logging rules [responsible specialist]

a. The organisation has established logging rules which comply with the valid information security policy and which stipulate the manner of safe planning, organisation, and implementation of logging.
b. Based on the protection requirement, the logging rules determine the extent of logging IT systems and applications and which ones are logged.
c. Any deviations from the logging rules need a permission from the information security manager and are documented.
d. Compliance with the rules is checked regularly and the results are documented.

OPS.1.1.5.M3 Configuring the logging of events

a. All security events of IT systems and applications are logged.
b. Internal log functions of IT systems and applications which are included in the logging rules have been implemented.
c. The operation and correctness of logging is regularly checked at intervals established in the logging rules.
d. If security incidents cannot be internally logged by an IT system or application, compensating measures have been implemented (e.g. logging network-level events) according to the recommendations of the manufacturer of the IT system or application.

OPS.1.1.5.M4 Synchronisation of time

a. The system times of IT systems and applications that are logged are always synchronised.
b. Logs use a unified time format; see also NET.1.2 Network management.

OPS.1.1.5.M5 Compliance with the legal framework conditions [information security manager]

a. When logging, the requirements of data protection and other relevant legislation are complied with (see also CON.2 Data protection).
b. Log data is deleted according to the established procedure.
c. Unauthorised deleting or changing of log data is prevented with technical measures.

3.3 Standard measures

OPS.1.1.5.M6 Establishing a central log infrastructure

a. Important log data that is essential for the protection of business-critical IT systems is stored entirely in central log servers or an infrastructure of log servers.
b. In order to save the logs, access to the network segment of log servers is only granted to the designated clients of the log server (see also NET.1.1 Network architecture and solution).
c. In addition to security events (see also OPS.1.1.5.M3 Configuration of logging), the central log infrastructure also logs events that point to possible errors (e.g. overloading the system or initiating unusual operations).
d. In case of increasing the extent of logging, additional resources can be added to the log infrastructure.
e. When establishing a log infrastructure outside the organisation, the services of a trustworthy and specialised service provider are used.

OPS.1.1.5.M8 Archiving log data

a. Log data is archived in accordance with the logging rules (see also OPS.1.1.5.M1 Logging rules). When archiving, the requirements of relevant legislation are also taken into account (see also OPS.1.2.2 Archiving).

OPS.1.1.5.M9 Provision of log data for analysis

a. The used logging application enables analysing the processed log data.
b. The processing and analysis of log data takes place in compliance with the logging rules (see also OPS.1.1.5.M1 Logging rules).
c. When analysing log data, the information security policy of the organisation and the legal basis for data processing is taken into account.
d. Log data is stored in its original form.

OPS.1.1.5.M10 Protection of log data from unauthorised access

a. All log data is stored and protected from unauthorised access and the access rights to log data are documented.
b. The managers of IT systems and applications cannot change or delete log data.

3.4 Advanced measures

OPS.1.1.5.M11 Increasing logging capacity (C-I-A)

a. Logging capacity is sufficient for analysing the log data in a central location as much in real time as possible. For this purpose, the log data is saved at the shortest possible intervals.
b. In case of a high protection requirement, the list of types and the quantity of logged events is extended.
c. In case of a high protection requirement, IT systems and applications that cannot be logged into a central location are not used.

OPS.1.1.5.M12 Encryption of log data (C-I)

a. The log data is only forwarded in an encrypted format.
b. The saved log data is signed digitally.
c. The log data that has been archived and is kept outside log infrastructure is always encrypted (see also CON.1 Encryption concept).

OPS.1.1.5.M13 Logging system with high availability [information security manager] (A)

a. The requirements for high availability have been taken into account when creating the log infrastructure.

OPS.1.1.5.ME1 Log hash chaining (I)

a. Blockchain technology is used for ensuring the integrity of logs, where local timestamps of log entries are linked in a chronological order into a cryptographic hash chain.
b. The log hash chain is reliably linked, preventing unauthorised changes to the log data.
c. An authorised employee checks the integrity of the log hash chain regularly.

OPS.1.1.6 Software testing and onboarding

1 Description

1.1 Purpose

To present recommended procedures for testing and commissioning software and the measures for ensuring the compliance with technical and regulatory security requirements of the commissioned software.

1.2 Responsibility

The IT department is responsible for implementing the measures of software testing and onboarding. **Additional responsible persons:** human resources department, data protection specialists, responsible specialist, tester.

1.3 Limitations

The measures of the module are implemented with the measures from the modules CON.8 Software development and APP.6 Software in general. Software testing after the implementation of changes is described in the module OPS.1.1.3 Patch and change management.

2 Threats

2.1 Testing software with working data

Although testing software with working data is convenient, persons who are involved in software testing can see confidential work or personal data. If the data from the operational environment and not the copy of such data is used for testing, then the data might be unintentionally changed or deleted. Although working data is used when testing the integration of IT systems, the processing of data used in testing might inadvertently affect operations with real data in other systems.

2.2 Missing or insufficient testing procedure

If the new software is not tested or is tested inadequately, then errors in software or the installation process might go unnoticed. If the changes or updates are not tested sufficiently, then it might create

serious availability and integrity problems. For example, downloading an update for a database system that has not been tested beforehand might cause data losses.

2.3 Missing or insufficient approval procedure

As a result of a missing or insufficient approval procedure, software with technical shortcomings might be adopted. The software might lack necessary functions or its source code might contain unnecessary components. In addition, unapproved software might not be compatible with other applications in use.

2.4 Inadequate documentation of tests and testing results

If the documentation of software testing is insufficient, then it will be impossible to identify at a later time which functionality was tested and which operations were conducted for testing. If the identified software errors or missing functions have been inadequately documented, then the errors will be transferred to the IT systems in the operational environment.

2.5 Insufficient documentation of approval criteria

If the approval criteria have not been unambiguously agreed and documented, then a software version with errors might be approved for installation. The errors might only become apparent in the operational environment and cause a late completion of the software project and financial losses.

3 Measures

3.1 Life cycle

Planning

OPS.1.1.6.M1 Planning software tests

OPS.1.1.6.M7 Selecting staff for software testing

OPS.1.1.6.M10 Procedure for the approval of testing

Operation

OPS.1.1.6.M2 Functional testing of software

OPS.1.1.6.M3 Analysing testing results

OPS.1.1.6.M4 Approval of software

OPS.1.1.6.M5 Conducting non-functional tests

OPS.1.1.6.M11 Anonymisation or pseudonymisation of test data

OPS.1.1.6.M12 Regression tests

OPS.1.1.6.M15 Compliance with the guidelines for installation and configuration

Implementation

OPS.1.1.6.M6 Supervision of software testers

OPS.1.1.6.M13 Separating the testing environment from the operational environment

Additional advanced measures

OPS.1.1.6.M14 Conducting penetration tests

OPS.1.1.6.M16 Background checks for testers

3.2 Key measures

OPS.1.1.6.M1 Planning software tests

a. Based on the protection requirements, technical possibilities, and the testing environment, the framework conditions for testing are established before testing the software.
b. The testing relies on the framework conditions for testing and the specifications of the software.
c. The test stories cover the entire functionality of the software.
d. The testing environment is as similar to the operational environment as possible.
e. The functioning of software is checked during testing in all planned user environments (e.g. in various devices) and in supported operating systems.

OPS.1.1.6.M2 Functional testing of software [tester]

a. All software functions are checked with the functional testing of software. Functional testing is used for verifying that the software functions as required.
b. Functional testing does not have any effect on the further operation of the software.

OPS.1.1.6.M3 Analysing testing results [tester]

a. During the analysis of testing results, the actual values measured during testing are compared against the expected results.
b. The results of the analysis of testing results are documented.

OPS.1.1.6.M4 Approval of software [responsible specialist]

a. The structural unit that provides the approval checks whether the software was tested according to requirements and whether the test results correspond to the previously established conditions.
b. After a successful software testing, the implementation of software is approved with a documented decision.

OPS.1.1.6.M5 Conducting non-functional tests [tester]

a. Non-functional testing is used for testing the capacity, quality indicators, and security of software.
b. In case of security-critical functions, conducting security tests is obligatory.
c. The chosen test stories and test results are documented.

OPS.1.1.6.M11 Anonymisation or pseudonymisation of test data [data protection specialist, tester]

a. Test data of software prepared based on sensitive data is sufficiently protected from disclosure in the test environment.
b. As a minimum, all test data related to natural persons has been pseudonymised. If the test data can be linked to a specific person, then the decision to use such data is made involving a data protection specialist.
c. If possible, all test data related to physical persons is anonymised.

3.3 Standard measures

OPS.1.1.6.M6 Supervision of software testers [responsible specialist]

a. The IT department informs the software tester in good time about the type of the upcoming testing and the details of objects to be tested.
b. The tester is informed about the uses of the software and possible additional requirements.

OPS.1.1.6.M7 Selecting staff for software testing [responsible specialist, human resources department]

a. When selecting a software tester, the necessary professional qualifications and knowledge of the programming languages, development environments, and testing methods currently in use are taken into consideration.

b. The testers who did not participate in the programming of the aforementioned software module review the source code.

OPS.1.1.6.M10 Procedure for the approval of testing

a. A procedure for the approval of testing has been established, which determines:
- the obligatory tests;
- the expected results;
- the criteria for the acceptance of testing.

b. A procedure for action in case of a refusal to approve the testing has been established.

OPS.1.1.6.M12 Regression tests [tester]

a. After changing the software, it is submitted to a comprehensive regression test to check the compatibility of the software and discover potential new errors.
b. The selected testing instances and testing results are documented. The exclusion of testing instances is substantiated in writing.

OPS.1.1.6.M13 Separating the testing environment from the operational environment

a. Software is tested only in the special testing and prelive environment.
b. The testing and prelive environment is separated from the operational environment and clearly distinguishable from the operational environment.
c. The architecture and technical parameters of the testing environment are documented.

OPS.1.1.6.M15 Compliance with the guidelines for installation and configuration [tester]

a. The guidelines for the installation and configuration of software have been complied with in preparing the testing environment (see also APP.6 Software in general).

3.4 Advanced measures

OPS.1.1.6.M14 Conducting penetration tests [tester] (C-I-A)

a. Guidelines for penetration testing have been prepared, which establish the testing methods and criteria for the results.
b. The completed penetration tests correspond to the guidelines for penetration tests.

c. Vulnerabilities identified during penetration tests are classified according to the risk level and documented.
d. Any significant vulnerabilities that are identified are eliminated before the implementation of the software.

OPS.1.1.6.M16 Background checks for testers [human resources department] (C)

a. In domains with a high protection requirement, additional background checks are conducted for the companies and the testers conducting the testing before a contract for testing is concluded.
b. The testers of an IT system or software that contains classified information have clearance for access to state secrets that complies with the valid legislation.

OPS.1.1.7 Systems management

1 Description

1.1 Purpose

To present measures for the secure configuration and monitoring of a systems management solution, the components thereof, and the IT systems managed, and for information exchange. Systems management is used for the central administration of integrated and managed systems. Systems management is an integrated whole consisting of a central management solution, IT systems that are managed, and data communication interfaces.

1.2 Responsibility

The IT department is responsible for compliance with the measures applicable to systems management.
Additional responsible persons: No additional responsible persons.

1.3 Limitations

General measures for the management of IT systems are described in module OPS.1.1.2: IT systems management.
Network management measures are discussed in module NET.1.2 Network management. Secure

interfacing of IT systems with systems management is discussed in the modules of SYS module group, focusing on systems. Measures for logging and backing up a systems management solution are presented in modules OPS.1.1.5 Logging and OPS.1.2.2 Archiving.
Management of the changes made to a systems management solution is described in module OPS.1.1.3 Patch and change management. Measures for the remote management of IT systems are presented in module OPS.1.2.5: Remote maintenance.

2 Threats

2.1 Unauthorised access to the systems management solution

The systems management solution is a priority target for attackers as the extensive access rights of the systems management solution allow the attacker to control and manipulate all IT systems managed. The attacker can gain access to delicate data or disturb the business processes which are supported by the systems managed.

2.2 Errors in the automation of systems management

Any errors in the automation of systems management processes (e.g. in scripts) may disable the systems managed or significantly reduce the security of the IT systems. Due to automation, an error may affect a higher number of IT systems within a very short period of time, incl. critical IT systems, the high availability of which is very important from the business perspective.

2.3 Disturbing the data communication of systems management components

A targeted attack or random interruption in the data communication between systems management components may damage the integrity of the IT systems managed and restrict the availability of IT services. Tapping and manipulation of the communication of systems management allows the attacker to influence the functioning of the IT systems managed and view the information sent between the IT systems.

2.4 Insufficient synchronisation of clocks

If the system times of systems management components are not synchronised, the management of security incidents is complicated. The log data used may not be mutually correlated, as a result of which a potential security incident may remain undetected.

2.5 IT systems which are incompatible with the systems management solution

Systems which are incompatible with the systems management solution cannot be managed centrally in the designed extent. A situation may arise in which the IT systems are unavailable or the failures occurring in them are not reported to the central management system. Those IT systems may also be deprived from centrally implemented system updates or changes in the configuration of administration interfaces.

2.6 Lack of access to the systems management solution

If an authorised user (administrator) us unable to access the systems management solution when needed, this may result in a failure of the IT systems managed.

2.7 Interruption of the connection between the systems management solution and the systems managed

An interruption of the connection with the systems managed may damage the availability of the IT services and/or the integrity of the IT systems. The extent of the damage depends on the extent of the communication interruption and the duration thereof. The failures arising from the lack of connection are difficult to analyse and the errors detected hard to fix.

2.8 Insufficient coordination of systems management and network management

If the changes planned in the network management are no longer coordinated with the parties responsible for systems management, the changes made in the network may be unexpected and have a negative impact on systems management. Conflicts between the configurations of the network and IT systems may make the IT systems managed unavailable for the systems management solution, and the resulting failures may generate a high number of error messages, as well as events with unpredictable consequences.

3 Measures

3.1 Life cycle

Planning

OPS.1.1.7.M1 Defining the requirements of systems management

OPS.1.1.7.M2 Designing the systems management solution

OPS.1.1.7.M7 Security rules of systems management

OPS.1.1.7.M8 Concept of systems management

Operation

OPS.1.1.7.M3 Synchronising clocks

OPS.1.1.7.M4 Protection of the data communication of systems management

OPS.1.1.7.M5 Mutual authentication of the systems management solution and the IT systems managed

OPS.1.1.7.M6 Security of the access of the systems management solution

OPS.1.1.7.M11 Regular compliance analysis of systems management

OPS.1.1.7.M12 Central activation of systems management operations

OPS.1.1.7.M14 Central management of the configurations of the IT systems managed

OPS.1.1.7.M15 Monitoring, logging, and notifications of the systems management solution

OPS.1.1.7.M17 Restricting the systems management information exchange

OPS.1.1.7.M18 Checking the condition of the systems management solution

OPS.1.1.7.M19 Security of the data communication of the systems management solution

Implementation

OPS.1.1.7.M9 Systems management implementation plan

OPS.1.1.7.M10 Instructions for the secure operation of systems management

OPS.1.1.7.M13 Allocating permitted administration interfaces

Emergency response

OPS.1.1.7.M16 Integration of systems management with emergency response

Additional advanced measures

OPS.1.1.7.M20 Highly available systems management solution

OPS.1.1.7.M21 Physical partitioning of the systems management network

OPS.1.1.7.M22 Integrating systems management with a security information management system

OPS.1.1.7.M23 Synchronising the clocks of different locations

OPS.1.1.7.M24 Inspecting the security configuration of the systems managed

OPS.1.1.7.M25 Logging the user sessions of the systems management solution

OPS.1.1.7.M26 Restricting access to the systems management solution

3.2 Key measures

OPS.1.1.7.M1 Defining the requirements of systems management

a. The organisation has defined the requirements of systems management, including the security requirements, taking all systems management processes into consideration.
b. Technical requirements for the infrastructure of systems management have been established.
c. The IT systems managed have been defined and the interfaces of the IT systems with the central systems management component have been documented.

OPS.1.1.7.M2 Designing the systems management solution

a. As a result of designing the systems management solution, the following have been documented:
- detailed analysis of the requirements for systems management;
- the general concept of the systems management solution;

a comprehensive project plan for the introduction of the systems management solution;
- the prerequisites for the completion of the stages of the project and the quality controls to be performed.

b. At least the following aspects have been taken into consideration is designing the security of the systems management solution:
- the network segments covered by the systems management solution;
- secure access to the systems management solution;
- authentication and authorisation in the IT systems managed;
- the network connections and network protocols for the data communication between the components of the systems management solution;
- logging of systems management events and integration of the logs with the central log management solution;
- the availability of support services from the producer or developer of the systems management solution for the duration of the intended service life;
- installation of systems management solution updates, incl. to the IT systems managed;
- the reporting provided by the systems management solution and interfacing with other IT systems;
- the security requirements for the IT systems managed.

OPS.1.1.7.M3 Synchronising clocks

a. The times of the main components of the systems management solution and the IT systems managed are synchronised.
b. A suitable network time protocol is used for synchronising clocks.

OPS.1.1.7.M4 Protection of the data communication of systems management

a. Secure network protocols are used to create the data communication between the systems management solution and the systems managed (e.g. SSH, TLS).
b. If secure network protocols cannot be used, the data communication of the systems management solution is organised in a special administration network separated from the regular network (see NET.1.1 Network architecture and solution). If there is no administration network, a virtual private network (VPN) or a data communication solution with an equivalent level of security is used.

OPS.1.1.7.M5 Mutual authentication of the systems management solution and the IT systems managed

a. The authentication between the systems management solution and the IT systems managed is mutual (bidirectional).
b. The mechanisms used for the authentication of the components of the systems management solution are compliant with the general authentication principles of the organisation.
c. Secure protocols are used for authentication.

OPS.1.1.7.M6 Security of the access of the systems management solution

a. The access of users to the systems management solution is secured by appropriate mechanisms for the authentication and authorisation of users.
b. The data sent for the authentication of users is encrypted.
c. The process of selecting the mechanism for the authentication of the users is documented.
d. The strength of the encryption mechanisms and encryption keys used is checked regularly.
e. The authorisation mechanism of the systems management solution enables users to perform only those operations which the users are authorised to perform.

3.3 Standard measures

OPS.1.1.7.M7 Security rules of systems management

a. The security rules of systems management have been drawn up to ensure the security of systems management.
b. The security rules of systems management include at least the following:

- the areas and IT systems which fall within the scope of the central systems management solution;

• automated systems management processes and operations;

• description of the configuration management included in the systems management solution (e.g. version management);

• the technical specifications for regulating access;

• the requirements for logging;

• the requirements for checking the quality of automated operations (e.g. the use of scripts);

• the requirements for ensuring the security of the data connection;

• the rules for network segmentation (if segmentation is used);

• technical specifications of the network of the systems management solution (IP addresses, DNS, etc.);

c. The systems management security regulation is accessible for authorised employees. The employees involved with systems management follow the security rules of systems management.

d. Compliance with the security rules of systems management is checked regularly. The results of the inspection are documented.

OPS.1.1.7.M8 Concept of systems management

a. The organisation has drawn up a concept of systems management which takes into consideration the security requirements for systems management (see OPS.1.1.7.M1 Defining the requirements of systems management and OPS.1.1.7.M7 Security rules of systems management).

b. The concept of systems management includes at least the following:

• the methods, techniques, and tools of systems management;

• regulation of access to the systems management solution;

• the data communication security measures;

• placement of the components of the systems management solution in the network segments;

• monitoring the components of the systems management solution and automatic notifications;

• logging of the systems management solution;

• technical specifications of automated operations (e.g. configuration management);

• development and testing of automated operations;

• the actions and communication channels used to respond to interruptions and security incidents;

• integration of systems management information with other processes of the organisation;

• integration of systems management with the organisation-wide emergency response concept;

• the resources required for implementing and operating the systems management solution, incl. the human resources required and the requirements for the capacity of the network.

OPS.1.1.7.M9 Systems management implementation plan

a. A detailed implementation plan has been drawn up for operating the systems management solution, which takes into consideration all the requirements included in the security regulation and the concept of systems management.

OPS.1.1.7.M10 Instructions for the secure operation of systems management

a. There are instructions for the secure operation of the systems management solution.
b. The instructions for the secure operation of systems management include all security requirements established for the systems management solution and the underlying infrastructure.

OPS.1.1.7.M11 Regular compliance analysis of systems management

a. The integrity of the information of the systems management solution and the IT systems managed is checked regularly.
b. The configurations of the IT systems managed with the systems management solution are compliant with the centrally designed configurations.
c. The accuracy of the scripts and other outcomes of automatic operations of the systems management solution is checked regularly.

OPS.1.1.7.M12 Central activation of systems management operations

a. Only the systems management solution can activate systems management operations in the IT systems managed.
b. Only the required administrative functions are activated in the IT systems managed by the systems management solution.

OPS.1.1.7.M13 Allocating permitted administration interfaces

a. Administrative access to the systems managed is only permitted through specific interfaces of the systems management solution.
b. In exceptional cases (e.g. in an emergency situation with the systems management solution not functioning), the IT systems managed can also be configured through direct access.
c. Any cases of using direct access and any configuration changes made outside of the systems

management solutions are documented. The changes made are later included in the systems management solution.

OPS.1.1.7.M14 Central management of the configurations of the IT systems managed

a. The configurations of the IT systems managed are managed as part of the systems management solution in the configuration management system described.
b. The data of the central configuration management system is always complete and updated. Any changes in the information are versioned, the changes made can be traced. The configuration management information is included in the regularly created back-up copy.
c. Only authorised users can access the configuration management information.
d. The functioning of the central configuration management and the accuracy of the information in the system are checked regularly.
e. All interfaces between the systems management solution and the IT systems managed are documented in the central configuration management system. Related parties coordinate functional changes in the interfaces before implementing the changes.
f. The configuration information of the systems managed can be shared over the network and activated automatically, without a delay and without interrupting the IT services.

OPS.1.1.7.M15 Monitoring, logging, and notifications of the systems management solution

a. The capacity and availability indicators of the systems management solution and the systems managed are monitored based on predetermined threshold values. Any exceeding of the threshold values is reported automatically to the responsible employees.
b. Systems management error analysis also includes the monitoring results and error messages from other systems (e.g. a systems management failure may be caused by a network interruption).
c. The details of all significant events in the managed systems and the systems management solution are sent automatically to the central log management system (see OPS.1.1.5 Logging).
d. The following aspects have been taken into consideration in defining a significant event:

- an error of the IT systems managed (e.g. through availability);
- an error of the systems management solution;

a malfunction of a hardware or IT infrastructure component;

- an unsuccessful login attempt to the systems management solution;
- an unsuccessful login attempt to an IT system managed;
- critical condition of a system managed (e.g. overburdening);

• critical condition of the systems management solution.

e. Automatic error messages of the systems management solution are sent without a delay.

OPS.1.1.7.M16 Integration of systems management with emergency response

a. The systems management solution is integrated with the emergency response concept of the organisation.

b. The configuration data of the systems management solution and all systems managed has been backed up and the recovery of the data has been included in the recovery plans.

OPS.1.1.7.M17 Restricting the systems management information exchange

a. The information exchange between the users of systems management, the components of the systems management solution, and the IT systems managed is restricted to the minimum extent required.

b. Suitable tools which enable the filtration of information are used to restrict the data connection.

OPS.1.1.7.M18 Checking the condition of the systems management solution

a. Compliance of the condition of the systems management solution with the defined normal situation is checked regularly.

b. In the case of identifying any discrepancies, the normal situation of the systems management solution is restored as soon as possible.

OPS.1.1.7.M19 Security of the data communication of the systems management solution

a. The data connection between the systems management solution and the systems managed is encrypted.

b. The strength of the encryption mechanisms and encryption keys used is checked regularly.

3.4 Advanced measures

OPS.1.1.7.M20 Highly available systems management solution (A)

a. A computer network designed with double system components and redundancy is used to increase the availability of the systems management solution.

OPS.1.1.7.M21 Physical partitioning of the systems management network (C-I)

a. The systems management network is physically partitioned from the network used for performing other tasks.

OPS.1.1.7.M22 Integrating systems management with a security information management system (C-I-A)

a. Logging the security events of the systems management solution is interfaced with a security information and event management (SIEM) system.
b. Possibilities for interfacing with an SIEM system and the information interfaces and formats supported are taken into consideration in the selection of the systems management solution.
c. The systems management solution is covered with automatic monitoring to identify potential security vulnerabilities.

OPS.1.1.7.M23 Synchronising the clocks of different locations (C-I-A)

a. The clocks of the systems management solution components and the IT systems managed are synchronised with the agreed source of reference time in all locations of the organisation.

OPS.1.1.7.M24 Inspecting the security configuration of the systems managed (C-I-A)

a. The security configurations of the systems management solution and the systems managed are checked regularly.
b. Appropriate identification systems are used to detect departures from the defined normal state and potential security vulnerabilities.

OPS.1.1.7.M25 Logging the user sessions of the systems management solution (C-I)

a. The entire data exchange of the systems management solution (incl. all system commands) is logged.
b. All system commands of the systems management solutions pass an automatic check and an automatic message is sent in the case of identifying any abnormalities or unusual behavioural patterns.

OPS.1.1.7.M26 Restricting access to the systems management solution (C-I)

a. Administrative access to the systems management solution is only possible through the jump server created for this purpose.

OPS.1.2 Supporting operations

OPS.1.2.2 Archiving

1 Description

1.1 Purpose

To present measures for the long-term, safe, and recoverable storage of documents in unaltered forms. The module contains measures for the safe planning, establishing, and running of an archival system.

1.2 Responsibility

The responsible specialist is responsible for the compliance with the measures for archiving.
Additional responsible persons: The user, the IT department

1.3 Limitations

Measures related to operative data backup are presented in the module CON.3 Data backup concept. The measures for the safe use of data backup solutions are described in the modules APP.4.3 Relational database systems, SYS.1.1 Server in general, and SYS.1.8 Storage solutions.

2 Threats

2.1 Unsuitability of data carriers for long-term storage

In time, data carriers can become physically and technologically out of date and therefore unsuitable for use. If the migration of data has not been organised appropriately, then this might create problems with the compatibility of used data formats over time.

2.2 Insufficient classification criteria of the archiving system

In case of unsuitable classification criteria or insufficient indexing, searching for archived documents or consolidating based on a characteristic might be very complicated. The purpose of the documents is not as clearly discernible over time. There is also the danger that the classification criteria for documents does not correspond to the purposes of data storage.

2.3 Insufficient documentation of archive access

In case of insufficient logging, unauthorised access attempts to the archive might remain undetected. An attacker can inconspicuously gain access to the archival information and copy or change the data.

2.4 Insufficient transfer of hard copy data to an electronic archive

When scanning documents, the look and contents of the data to be stored can become distorted. Documents might also be lost. If important parts of documents are not scanned, then they might be misinterpreted.

2.5 Inadequate updating of encryption procedures during archiving

If the encryption procedures for archiving are not updated regularly, the encryption protection loses its reliability. Outdated and unsafe signatures may call into question the integrity of the document and the encrypted data is no longer usable in court. If the encryption algorithm does not meet the current requirements, then the confidentiality of the encrypted document might also be compromised. When changing certificates (e.g. due to changing a certificate of the Estonian ID-card), the later decryption of data might become impossible.

2.6 Inadequate supervision of archiving

When the archiving process is left unsupervised or the supervision is too general, the process might fail to meet the security requirements in effect. The corruption of the integrity or confidentiality of documents might bring legal and economic consequences to the organisation.

2.7 Violation of legal framework conditions in archiving

When the legal framework conditions are not considered when archiving electronic documents, it might lead to sanctions based on civil or criminal law (e.g. when the retention dates established for tax, budgetary, or other legal reasons are ignored).

3 Measures

3.1 Life cycle

Planning

OPS.1.2.2.M1 Determining the electronic archiving factors

OPS.1.2.2.M2 Developing the concept of archiving

Implementation

OPS.1.2.2.M3 Suitable organisation of an archiving system and archiving media

OPS.1.2.2.M11 Training for the managers of the archiving system

OPS.1.2.2.M17 Selection of a suitable archiving system

Operation

OPS.1.2.2.M4 Uniform indexing of data in archiving

OPS.1.2.2.M5 Suitable preparation of data to be archived

OPS.1.2.2.M6 Protection of the integrity of the index database of the archiving system

OPS.1.2.2.M8 Logging archival access

OPS.1.2.2.M10 Rules for the use of the archiving system

OPS.1.2.2.M12 Monitoring the storage resources of an archiving medium

OPS.1.2.2.M13 Regular review of archiving processes

OPS.1.2.2.M19 Regular checks of archiving and recovery

Emergency response

OPS.1.2.2.M7 Regular backup of system and archival data

Migration

OPS.1.2.2.M9 Selecting suitable data formats for archiving

OPS.1.2.2.M14 Regular monitoring of the archiving systems market

OPS.1.2.2.M15 Updating encryption mechanisms in archiving

OPS.1.2.2.M16 Updating the technical components of the archiving system

Acquisition

OPS.1.2.2.M18 Suitable media for archiving

Additional advanced measures

OPS.1.2.2.M20 Duplication of encryption procedures

OPS.1.2.2.M21 Safe transfer of documents to an electronic archive

3.2 Key measures

OPS.1.2.2.M1 Determining the electronic archiving factors

a. Before preparing a concept for archiving, possible technical factors have been determined, among all else:

- the IT environment;
- security mechanisms;
- expected data volumes and reaction times;
- file formats;
- volumes of changes and the number of generations;
- resource requirements.

b. The legal and organisational factors related to electronic archiving have been ascertained, among all else:

- the legal basis for archiving;
- minimum and maximum storage times;
- access rights;
- frequency of access;
- interfacing,
- ergonomics.

c. The confidentiality, integrity, availability, and authenticity requirements of electronic archiving have been prepared and approved.

OPS.1.2.2.M2 Developing the concept of archiving

a. An archiving concept has been developed which describes the rules that must be complied with, the persons responsible, the type of data to be archived and its format, and the required security measures.

b. When documenting the archiving concept, the factors described in module OPS.1.2.2.M1 Determining the electronic archiving factors have been taken into account.

c. The archiving concept has been approved by the management of the organisation.

d. The archiving concept is regularly reviewed. If necessary, the archiving concept is adapted to the new circumstances.

OPS.1.2.2.M3 Suitable organisation of an archiving system and archiving media [IT department]

a. Archiving systems and related IT components have been housed in guarded premises. Depending on the type and size of storage or archiving system, measures from the modules INF.1 The building in general, INF.2 Server room and data centre, and INF.6 Media archive have been applied.
b. Only authorised persons have access to archiving systems, including the right of entry to premises.
c. Physical security and suitable environmental conditions of the archiving system are guaranteed for the long-term storage of archiving media.

OPS.1.2.2.M4 Uniform indexing of data in archiving [IT department, user]

a. All data, documents, and data entries that are stored in the archive are indexed so they would be quickly locatable in later search requests.
b. A uniform structure for the archival indexing information is determined when developing the concept.
c. The functionality of the indexing system is checked with random searches.

OPS.1.2.2.M5 Suitable preparation of data to be archived [IT department]

a. During the entire archiving period, the support and usability of the file systems of used data formats and storage carriers is guaranteed.
b. The archived data is readable without technical difficulties, reproducible, and has evidential value.
c. The encryption mechanisms used for encryption and maintaining the evidential value comply with the current requirements.
d. If necessary, the saved data can be converted into a valid data format or migrated to a new storage carrier, IT hardware, or IT software.

OPS.1.2.2.M6 Protection of the integrity of the index database of the archiving system [IT department]

a. The integrity of the index database is checked regularly. Any loss of integrity is rectified immediately and information about the incident is documented.
b. The index database is backed up regularly and the recoverability of the backup is checked after each backup is created.
c. In case of large archival databases, the index databases are duplicated.

OPS.1.2.2.M7 Regular backup of system and archival data [IT department]

a. All archival data, index databases, and relevant system data is backed up at intervals decided in the backup concept (see also CON.3 Data backup concept).

OPS.1.2.2.M8 Logging archival access [IT department]

a. In case of all instances of accessing the archive, the date, time, user, reason for accessing the archive, the client system, the operations that were conducted, and error messages (if there are any) are logged.
b. The log data of archival access is analysed regularly to identify possible deviations. When a deviation is identified, the process for incident handling is initiated.
c. Critical events such as deleting data or removing data carriers from the archiving system are checked immediately after a respective log entry is created.
d. The log data of archival access is stored for the storage period determined in the archiving concept.

OPS.1.2.2.M9 Selecting suitable data formats for archiving [IT department]

a. When archiving log data, standard data formats that can be processed electronically are used, the syntax and semantics of which are disclosed more broadly.
b. The selected solution guarantees that the data is stored for as long as possible.
c. The selected data formats enable to reproduce the archived material in its faithful original format.
d. The suitable format for maintaining the evidential value of documents and ensuring manipulation-proof archiving is PDF (ver A-2a or /A-2u) which allow for the uniform presentation of a document in computers with different hardware and software configurations.
e. In order to maintain the evidential value of images and ensure their manipulation-proof archiving, formats that enable reproduction without losses and image compression procedures are used; the suitable formats for this are TIFF (ver 6) or PNG (ver 1.2.).
f. WAV, FLAC (ver 1.21), AVI (unpacked), MOV (unpacked), and MPEG-4 (H.264) formats are suitable as archival formats for audio and video files.
g. The ASICE data format is used for archiving digitally signed document containers.

3.3 Standard measures

OPS.1.2.2.M10 Rules for the use of the archiving system [IT department]

a. The organisation has established rules for using the archiving system, which entail the following:
- separation of operational and administrative roles and responsibilities;
- agreed level of service;
- managing access rights;
- procedures for handling data and data carriers;
- monitoring the archiving system and environment;
- procedures for data backup;
- logging archival operations;
- managing changes in the archiving system.

b. The managers of the archiving system comply with the rules for the use of the archiving system.

OPS.1.2.2.M11 Training for the managers of the archiving system [IT department]

a. The managers of the archiving system are trained in the following subjects (as a minimum):
- the architecture and security mechanisms of the implemented archiving system and its operating system;
- installation and maintenance of the archiving system;
- procedure for handling data and data carriers;
- documenting administrative operations;
- procedures for configuration, updates, and disposal;
- handling deviations from the rules.

b. Training and participation in the training is documented.

c. The managers receive additional training in case of any changes to the archiving system.

OPS.1.2.2.M12 Monitoring the storage resources of an archiving medium [IT department]

a. The free storage of an archiving medium is checked before saving the data.

b. If the free storage volume decreases below the required limit, the system administrator is notified.

c. Additional resources exist for increasing the storage capacity and a procedure has been prepared for its implementation.

OPS.1.2.2.M13 Regular review of archiving processes

a. The correctness and compliance of the archiving process is checked regularly.

b. A checklist of control questions is prepared for the review based on the archiving concept (see

also OPS.1.2.2.M2 Developing the concept of archiving) and the rules for using the archiving system (see also OPS.1.2.2.M10 Rules for using the archiving system).
c. Any deviations and vulnerabilities discovered during the review are handled at the earliest opportunity.

OPS.1.2.2.M14 Regular monitoring of the archiving systems market [IT department]

a. When monitoring the market and the developments of the archiving systems, attention is paid to the following aspects:

- changing or new standards;
- changes in the products of the manufacturer of the system that is in current use;
- notifications of any vulnerabilities that are discovered, e.g. in encryption algorithms;
- notifications of the danger of a loss of the protective capacity of the encryption algorithms;
- changes in current data formats and release of new formats.

b. At least one employee has been appointed to regularly monitor the information listed above, assess its significance, and recommend improvements if necessary.

OPS.1.2.2.M15 Updating encryption mechanisms in archiving [IT department]

a. The algorithms, keys, cryptographic products, and procedures are checked for being up to date and compliant with the standards in effect (see also CON.1.M1 Procedure for selecting encryption tools).
b. Security procedure in case the encryption mechanism weakens has been established (e.g. the archival data with weakened encryption mechanisms is encrypted again by using a safer encryption algorithm).

OPS.1.2.2.M16 Updating the technical components of the archiving system [IT department]

a. The technical up-to-dateness of the archiving system is checked regularly (see also OPS.1.2.2.M14 Regular monitoring of the archiving systems market).
b. The suitability of new components is tested before they are implemented.
c. A procedure for migration has been established for switching to new formats or tools.
d. All changes, conversions, testing, and replacement plans of the components of the archiving system are documented.

OPS.1.2.2.M17 Selection of a suitable archiving system [IT department]

a. When selecting an archiving system, the concept of archiving that has been prepared is complied with (see also OPS.1.2.2.M2 Developing the concept of archiving).
b. The following is taken into account when selecting an archiving system:

- version control support for documents and data;
- compliance of functions and processes with the ISO 14721 standard;
- mechanism for regulating access with a system of multilevel rights;
- logging, see also OPS.1.2.2.M8 Logging archival access;
- organising access for supervision;
- expandability of the system;
- access time;
- sufficient storage capacity;
- possibility to conduct operations manually;
- automatic checks of free storage capacity and storage limit alarm;
- compatibility with other components and systems;
- encryption mechanisms or their support.

OPS.1.2.2.M18 Suitable media for archiving [IT department]

a. When selecting archiving media, the compliance of the archiving medium with the data volumes, the maximum allowed access time, and the number of simultaneous access requests is taken into account.
b. The presumed service life of the archiving medium enables archiving for the required storage period.

OPS.1.2.2.M19 Regular checks of archiving and recovery [IT department]

a. The functioning of the archiving process is checked by reviewing the log data or archiving media regularly.
b. The readability and integrity of the archiving medium is tested at least once a year.
c. The operational capacity of the hardware components of the archiving system (particularly the mechanical parts of the archive) is checked regularly.
d. When errors and predetermined events (such as data copying) become evident, the appointed employees are informed automatically of the event.
e. A procedure has been established for handling errors and malfunctions that have been discovered.

3.4 Advanced measures

OPS.1.2.2.M20 Duplication of encryption procedures [IT department] (C-I)

a. Only encryption procedures compliant with the valid standards and norms are used for the long-term storage of archival data.
b. The data to be archived is processed with at least two different encryption procedures simultaneously.

OPS.1.2.2.M21 Safe transfer of documents to an electronic archive (C-I)

a. Roles and obligations have been assigned for scanning paper documents.
b. When ordering scanning from outside the organisation, the service agreement stipulates obligatory security requirements.
c. A procedure for preparing documents for scanning has been created.
d. The electronic format of the paper document corresponds to the original in its content and presentation.

OPS.1.2.4 Remote work

1 Description

1.1 Purpose

To present measures for the protection of information that is stored, processed, and forwarded in the course of remote work.

1.2 Responsibility

The information security manager is responsible for compliance with remote work measures.
Additional responsible persons: IT department, employees, human resources department, manager.

1.3 Limitations

The measures for the protection of the remote work infrastructure are explained in the module INF.8 Home workplace. Additional measures are presented in the module INF.9 Mobile workplace.

2 Threats

2.1 Absence or inadequacy of rules for remote workplaces

In the absence of rules for remote workplaces, employees might be unaware of their exact obligations. If an employee cannot recognise an information security incident at their remote workplace or does not know who should be notified, confidential information might fall into the wrong hands.

2.2 Unauthorised private use of a remote work computer

Software of unknown origin can be installed on a computer that is not under the direct control of the employer. Due to the carelessness of the user, malware might infect the computer. In addition to the person working remotely, their family members and guests could gain access to the computer.

2.3 Delays due to the unavailability of the remote worker

Unless definite times have been agreed with the person working remotely when the employee must be available, they might be unavailable at a time when they are needed. This might cause delays in the work process. Depending on an organisation, this might affect the entire business process significantly.

2.4 Danger of information not reaching employees

A person working remotely has less opportunities to participate in professional information exchange. This decreases their involvement in the business processes of the organisation and reduces the productivity of the remote worker. Unless the movement of information is guaranteed, important information security notification will also fail to reach the employee.

2.7 Ignoring security measures

Due to limited options for monitoring a remote workplace, the employee might fail to apply the recommended or obligatory security measures or do so to their full extent. A failure to implement security measures in a remote workplace could cause losses which could have been avoided under normal circumstances. Confidential information might end up in the hands of unauthorised persons.

3 Measures

3.1 Life cycle

Planning

OPS.1.2.4.M1	Rules for remote work
OPS.1.2.4.M6	Security concept for remote work
OPS.1.2.4.M7	Procedure for using communication devices
OPS.1.2.4.M9	User support and maintenance of a remote workplace
OPS.1.2.4.M10	Analysis of requirements for a remote workplace

Implementation

OPS.1.2.4.M2	Security of the remote work computer

Operation

OPS.1.2.4.M5	Raising awareness and training of remote workers
OPS.1.2.4.M8	Regular exchange of information with the organisation

3.2 Key measures

OPS.1.2.4.M1 Rules for remote work [manager, human resources department]

a. Rules governing remote work have been prepared and made available for the employees.

b. The remote work rules take into consideration the following security aspects:

- handling confidential information;
- data protection requirements;
- data backup and data synchronisation;
- using data communication;
- remote access rights;
- transport and storage of documents and data carriers;
- procedure for notifying of security events.

c. Agreements between the employer and the employee regarding remote work have been prepared, which take into account the legal aspects of occupational health and safety and which define the following (as a minimum):

- the voluntary nature of remote work;
- working equipment;
- working time and availability;
- reaction times, for example, the frequency of reading emails;

• overtime, additional remuneration, and covering additional costs;
• proprietary liability;
• terminating remote work.

d. The remote work rules are reviewed and updated regularly.

OPS.1.2.4.M2 Security of the remote work computer

a. A remote work computer is used only for its intended purposes (e.g. the user cannot install unapproved software onto a remote work computer).
b. The remote work computer is used only by an authorised person. The authorised persons are the remote worker and the administrator of remote work computers.
c. The security controls for the remote work computer depend on the protection requirement of the processed data. As a minimum, the following measures are applied:
• secure identification and authentication mechanisms which react to faulty entry with a temporary denial of access;
• an automatic screen lock, which can only be opened after another identification and authentication;
• minimum requirements for security-critical parameters (e.g. password requirements) ensure sufficient security;
• regular data backups are created for the computer;
• the content and volume of logging is sufficient for discovering malfunctions and security events;
• the hard drive of the computer is encrypted;
• the computer has tools for the encryption of files;
• the system configuration of the computer is set to the maximum level of security.

OPS.1.2.4.M5 Raising awareness and training of remote workers

a. The remote workers have completed the training on security measures for remote work.
b. The following aspects have been covered during the training for remote workers:
• the dangers of remote work;
• secure storage of work documents;
• physical security measures of a remote workplace;
• network security;
• secure use of data carriers;
• easier maintenance operations and problem solving.

c. The measures for training remote workers from the module ORP.3 Increasing awareness of information security and training are implemented.
d. Trainings for remote workers are organised at regular intervals.

3.3 Standard measures

OPS.1.2.4.M6 Security concept for remote work

a. A security concept for remote work has been prepared, which describes the protection requirement, security objectives, and security requirements of the remote workplace.
b. As a minimum, the following is documented in the security concept for remote work:
- the procedure for handling data, documents, and data carriers;
- organising communication between the organisation and remote workplace;
- authentication mechanisms;
- the procedure for using network connections;
- the procedure for data exchange;
- the procedure for data backups.

c. The security concept for remote work complies with the general security concept of the organisation.
d. The concept is updated regularly.

OPS.1.2.4.M7 Procedure for using communication devices [IT department, employee]

a. The framework conditions for using communication devices is established in the security concept for remote work.
b. As a minimum, the procedure for using communication devices establishes:
- communication options for information exchange (incl. message exchange, phone, email);
- services used for forwarding information;
- the use of video conference services;
- security controls for information exchange;
- the use of digital signatures;
- instructions for using public internet services for professional and personal purposes.

OPS.1.2.4.M8 Regular exchange of information with the organisation [manager, employee]

a. Regular information exchange between the remote worker, organisation, and colleagues has been organised.
b. Work-related announcements and information about changes in information security reach remote workers operatively without delay.
c. All colleagues know how to contact the remote worker.

OPS.1.2.4.M9 User support and maintenance of a remote workplace [IT department, employee]

a. A user support function has been created for solving software and hardware problems in remote work computers and contact persons have been appointed.
b. The user support knows the configuration of the hardware and software in the remote work computer.
c. Remote maintenance is conducted at a previously agreed time. Remote access to the computer is granted only for the time of the remote maintenance and only to the authorised employee.
d. The manner of transporting IT devices for maintenance has been decided.

OPS.1.2.4.M10 Analysis of requirements for a remote workplace [IT department]

a. Before the creation of remote workplaces, an analysis of the requirements containing at least the following has been conducted:
- confidentiality requirements for information processed in a remote workplace;
- goals for gaining access to the organisation;
- volume of data traffic between the remote workplace and the organisation;
- need to use intranet services;
- need to use the internet;
- requirements for the transportation of documents and data carriers;
- need and selection of hardware and software components for a remote workplace (coordinated with the IT management).

b. The requirements of each specific remote workplace are documented and approved by the Head of IT.
- This module does not contain any advanced measures.

3.4 Advanced measures

There are no advanced measures in this module.

OPS.1.2.5 Remote maintenance

1 Description

1.1 Purpose

To present measures for the protection of information that is saved, processed, and forwarded in the course of active and passive remote maintenance as well as of maintenance interfaces.

1.2 Responsibility

The IT department is responsible for complying with the measures of remote maintenance.
Additional responsible persons: User.

1.3 Limitations

The module does not handle all remote maintenance operations; therefore, measures from modules OPS.1.1.3 Patch and change management, ORP.3. Increasing awareness of information security and training, CON.1 Cryptography concept, and CON.3 Data backup concept should be taken into account.
Measures from modules OPS.2 Operations as a service and OPS.3 Operations of the service provider should also be applied. In the case of cloud services, module OPS.2.2 Using cloud services should be taken into consideration.
Modules OPS.1.1.2: IT systems management and OPS.1.1.7 Systems management discuss the central management of IT systems.
Module IND.3.2 Remote maintenance of operational technology components focuses on the remote maintenance of operational technology systems.

2 Threats

2.1 Inadequate compliance with remote maintenance rules

When the persons involved are not aware of or do not comply with the rules of remote maintenance, errors might occur during maintenance operations. The employees who conduct remote maintenance have greater rights than regular users, and therefore, an error caused by inattentiveness or convenience could cause significant losses. Ignoring security measures during remote maintenance is hard to identify and attacks caused by exploiting security vulnerabilities are difficult to detect and counter.

2.2 Absence or inadequacy of planning and regulating remote maintenance

When mistakes are made when planning remote maintenance and potential security vulnerabilities are not taken into consideration, this might affect the security of not only one IT system, but all IT systems of the organisation. Security vulnerabilities related to remote maintenance might occur in weak communication protocols, patch management processes, cryptographic and authentication mechanisms.

2.3 Incorrect authentication in remote maintenance

Due to the use of insecure authentication mechanisms, an unauthorised person might acquire administrative rights over a remote maintenance computer or tools. This might bring along unauthorised changes in the configuration of IT systems and applications, data deletion, or leaks of confidential information. The risk is even greater when an external partner is involved in remote maintenance.

2.4 Overdue or incorrect remote maintenance

If IT systems which need constant maintenance do not receive remote maintenance, then in the worst-case scenario, it might render the IT system unusable. The errors made during remote maintenance could cause malfunctions when using the IT systems. If the maintenance is overdue or incorrect, the known security vulnerabilities might go unrectified.

2.5 Use of insecure protocols in remote maintenance

If the data connection of remote maintenance is not encrypted or insecure protocols are used for tunnelling between two endpoints or networks, such as outdated versions of IPSec, SSH, or SSL/TLS, the security of the data connection is not ensured to a sufficient degree.

2.6 Uncontrolled use of remote maintenance functions

When the tasks of persons conducting remote maintenance operations have not been regulated or documented by an agreement, the staff conducting remote maintenance might exceed their authorisation and damage the IT systems.

2.7 Unauthorised use of an online remote maintenance service

If access for the remote maintenance of IT systems is enabled through an online service in a web server of third parties through a web browser, the system administrators have no control over who, when, and for which purpose uses this connection. The data connection channel between the IT system and the server is constantly open. In case of unencrypted data connection, the forwarded information can be manipulated.

2.8 Unauthorised use of remote maintenance components

If the function of integrated remote maintenance of the IT system is not taken into account when using the IT systems and its use is not limited, it might create unauthorised access to the systems and data. The functionality of remote maintenance components that are integrated into the IT systems is often not sufficiently documented, they can contain security vulnerabilities and enable bypassing security mechanisms that are implemented on the level of networks and operating systems.

3 Measures

3.1 Life cycle

Planning

OPS.1.2.5.M1 Implementation plan for remote maintenance

OPS.1.2.5.M6 Remote maintenance rules

OPS.1.2.5.M7 Remote maintenance documentation

Operation

OPS.1.2.5.M2 Establishing a secure connection for remote maintenance

OPS.1.2.5.M20 Secure implementation of remote maintenance

OPS.1.2.5.M24 Security of integrated remote maintenance functions

OPS.1.2.5.M25 Restricting remote maintenance that is conducted outside the management network

Implementation

OPS.1.2.5.M3 Data connection security during remote maintenance

OPS.1.2.5.M5 Secure implementation of online maintenance services

OPS.1.2.5.M8 Secure remote maintenance protocols

OPS.1.2.5.M10 Secure use of remote maintenance tools

OPS.1.2.5.M17 Authentication mechanisms for remote maintenance

OPS.1.2.5.M19 Remote maintenance from third parties

Acquisition

OPS.1.2.5.M9 Selecting suitable remote maintenance tools

Emergency response

OPS.1.2.5.M21 Emergency plan in case of a remote maintenance failure

Additional advanced measures

OPS.1.2.5.M14 Secure configuration of the remote maintenance client

OPS.1.2.5.M22 Redundancy of remote maintenance communication networks

3.2 Key measures

OPS.1.2.5.M1 Implementation plan for remote maintenance

a. When planning remote maintenance, the needs of the organisation as well as the technical and regulatory aspects of remote maintenance have been taken into consideration.

b. The implementation plan for remote maintenance establishes:

- the protection requirement and security objectives;
- responsibilities when conducting remote maintenance;
- legal and regulatory restrictions;
- remote maintenance channels;
- using a service provider;
- network separation requirements.

c. In case of a higher protection requirement, remote maintenance can only be conducted through a special management network.

OPS.1.2.5.M2 Establishing a secure connection for remote maintenance [user]

a. A remote maintenance connection can only be created by a user of the IT system, i.e. the party needing maintenance.
b. When remote maintenance is initiated, an external maintenance provider is authenticated in a safe manner. If the connection with the remote maintenance provider is lost for any reason, then new access can be created only by authenticating oneself again.

OPS.1.2.5.M3 Data connection security during remote maintenance

a. Access rights and possibilities for establishing data connection are limited based on the minimum principle.
b. Data connection between a remote maintenance server and client is encrypted.
c. After the remote access is no longer needed, all data connection channels in use are closed (deactivated).
d. Remote maintenance tools are installed in only those workstations that are used for remote maintenance.
e. Data connection is logged to ensure the traceability of the data transmission.

3.3 Standard measures

OPS.1.2.5.M5 Secure implementation of online maintenance services [user]

a. Remote maintenance through an online service is generally banned and blocked.
b. Online maintenance services are implemented only as justified exceptions, the potential instances of using those are regulated, and their use is registered and approved.
c. Automatic connection of client computers with online services is prohibited; technical measures are implemented to prevent a connection.

OPS.1.2.5.M6 Remote maintenance rules

a. The requirements for remote maintenance are documented in the information security policy. When separate remote maintenance rules exist, the information security policy makes a reference to those.
b. All parties who participate in the creation, implementation, use, and ending the use of the remote maintenance plan have read it.
c. Compliance with the remote maintenance rules is checked regularly.

OPS.1.2.5.M7 Remote maintenance documentation

a. Remote maintenance documentation is sufficient and up to date.
b. As a minimum, the remote maintenance documentation includes the following:
- the configurations of the IT systems that need maintenance;
- system users and their privilege profiles;
- added hardware and software components;
- procedures for data backup and handling data carriers;
- descriptions of discovered and eliminated failures.

c. Documentation is stored in a secure manner. Authorised persons can access the documentation quickly if necessary.

OPS.1.2.5.M8 Secure remote maintenance protocols

a. Communication protocols which are up to date and considered secure are used for remote maintenance.
b. Data exchange is encrypted. Encryption procedures that correspond to the protection requirement are used for tunnelling (at least SSH v2, TLS 1.2, SNMP v3, IPSec with IKEv2).
c. Communication protocols are used for remote maintenance, which allow the identifications of random disturbances in the forwarded data and their automatic elimination. The recipient confirms that the data has been received.
d. In order to guarantee that the protocols in use are up to date, information about the detected vulnerabilities is monitored regularly.

OPS.1.2.5.M9 Selecting suitable remote maintenance tools

a. When selecting remote maintenance tools, the measure OPS.2.4.M1 Implementation plan for remote maintenance is taken into consideration.
b. Remote maintenance tools are selected based on the analysis of the organisational handling, security, and data protection requirements and the accompanying risk assessment.
c. All decisions for the acquisition of remote maintenance tools are coordinated with the persons responsible for procurement, systems, and applications, and the security governance.

OPS.1.2.5.M10 Secure use of remote maintenance tools [user]

a. User guidelines along with the descriptions of sample procedures have been prepared for the use of remote maintenance tools.
b. The users have completed training on the use of remote maintenance tools.
c. A contact person has been appointed who is going to solve technical issues regarding the remote maintenance tools.

OPS.1.2.5.M17 Authentication mechanisms for remote maintenance

a. Multi-factor authentication is used for the initiation of a remote maintenance session.
b. The selection of an authentication method and the reasons for it are documented.

OPS.1.2.5.M19 Remote maintenance from third parties

a. All changes made by an external service provider during remote maintenance (for example, in the configuration settings, source code) are documented. The documentation on changes is delivered to the organisation receiving remote maintenance.
b. The staff of the external service provider undertakes to fulfil the contractually agreed requirements, including confidentiality agreements.
c. Maintenance operations that are conducted by the staff of an external service provider are monitored, and if possible, recorded. The organisation has appointed a person who is responsible for monitoring the remote maintenance.
d. Remote maintenance is initiated exclusively from the intranet and only for a predetermined period of time.
e. Remote maintenance access is given to an external service provider based on the principle of minimality.
f. The employees of the external service provider always authenticate themselves as personally identifiable users.
g. Remote maintenance can be terminated from the intranet at any time.
h. When remote maintenance is provided through third parties, the measures from the module OPS.2.1 Outsourcing are also implemented.

OPS.1.2.5.M20 Secure implementation of remote maintenance

a. Remote maintenance is conducted based on prior notification and confirmation.
b. Access for remote maintenance is only granted after successful authentication.

c. Full administrative rights are not granted for remote maintenance. The person providing remote maintenance does not have access to those IT systems which are not necessary for maintenance.
d. Data exchange between the remote maintenance server and client is controlled with a firewall. The measures of detecting and preventing denial-of-service attacks are in place.
e. All remote maintenance operations, the beginning and end of the remote maintenance, and the persons providing this maintenance are registered and logged.

OPS.1.2.5.M21 Emergency plan in case of a remote maintenance failure

a. An emergency plan has been developed to minimise the damage caused by failures, reverse maintenance operations, and quickly resume normal work.
b. When preparing and testing the emergency plan, measures from the module DER.4 Emergency management are implemented.

OPS.1.2.5.M24 Security of integrated remote maintenance functions

a. When acquiring IT systems, the options and security provided by their integrated remote maintenance functions are evaluated.
b. If the remote maintenance functions that are integrated into the IT systems are not used or if they could contain security vulnerabilities, the integrated remote maintenance functions are deactivated.
c. The components of the IT system, the remote maintenance of which is organised on the level of firmware, can be accessed only through a separate management network.

OPS.1.2.5.M25 Restricting remote maintenance that is conducted outside the management network

a. If possible, remote maintenance from devices outside the management network is avoided.
b. Conducting remote maintenance from a client device that is outside the management network is only allowed through the jump server in the management network.
c. Jump server access is only granted to trusted client devices that require it.

3.4 Advanced measures

OPS.1.2.5.M14 Secure configuration of the remote maintenance client (C)

a. Only client devices prepared for remote maintenance are used for remote maintenance.
b. All functions and components of remote maintenance tools that are installed in the remote maintenance client device and are not necessary for the maintenance are deactivated.
c. The remote maintenance tools and workstations in which they are used are configured and set in a secure manner.
d. Data communication in the client devices of remote maintenance is limited. Only data communication needed for maintenance operations is allowed.
e. A user account created specifically for this purpose is used for remote maintenance

OPS.1.2.5.M22 Redundancy of remote maintenance communication networks (A)

a. In case of remote maintenance in an emergency situation, the IT system can be accessed through a redundant connection (e.g. 4G mobile network).

OPS.1.2.6 Synchronising clocks with the NTP server

1 Description

1.1 Purpose

Presenting the measures for the secure synchronisation of the clocks of the Network Time Protocol (NTP) client equipment of the NTP server and for ensuring reliable and accurate time in all connected IT systems.

1.2 Responsibility

The IT department is responsible for the implementation of the measures of synchronising clocks.
Additional responsible persons: No additional responsible persons.

1.3 Limitations

The measures described in the module are applied to all IT systems which use NTP.
The general security measures established for servers are discussed in the module SYS.1.1 Server in general, and the measures applied to client computers in the module SYS.2.1 Client computer in general.

2 Threats

2.1 Error in deploying the NTP server

A situation may occur in which all IT systems are not connected to the NTP server to obtain accurate time information. For example, an error made in designing or segmenting the network may disrupt the connection between the NTP server and the clients. Different times of the clocks are often not detected before they have caused an IT incident, for example if automated operations are activated at incorrect times.

2.2 Incorrect time or no time

The NTP server may be temporarily unavailable or send inaccurate time information.

2.3 Conflicting time information

Time information originating from different sources may be conflicting. If an IT system uses several NTP servers for synchronising the clock, the times of the NTP servers may differ. If the times are significantly different, the IT system is unable to determine which time information provided is correct. Differences between the times may cause failures in the IT systems, misinterpretation of information, or interruptions in data exchange with other IT systems.

2.4 Manipulation of NTP data communication

In the event of a network attack, the attacker can manipulate NTP data communication, for example change the time information of network packages when the information is being sent or redirect NTP inquiries to a server selected by them. This will allow the attacker to change the system time of the NTP clients and use it to abuse time-restricted access rights or access rights which have expired by the time of the attack.

3 Measures

3.1 Life cycle

Planning

OPS.1.2.6.M1 Planning the deployment of NTP

OPS.1.2.6.M2 Secure use of external NTP servers

Implementation

OPS.1.2.6.M3 Secure configuration of an NTP server

OPS.1.2.6.M4 Prohibition of undesired sources of time information

OPS.1.2.6.M7 Secure configuration of NTP clients

Operation

OPS.1.2.6.M5 Operating NTP in the client-server mode

OPS.1.2.6.M6 Monitoring internal NTP servers

OPS.1.2.6.M8 Using secure protocols in synchronising clocks

Additional advanced measures

OPS.1.2.6.M9 Using different sources of accurate time information

OPS.1.2.6.M10 Only using internal NTP servers

OPS.1.2.6.M11 Ensuring the redundancy of NTP servers

OPS.1.2.6.M12 Ensuring the authenticity of NTP servers

3.2 Key measures

OPS.1.2.6.M1 Planning the deployment of NTP

a. The organisation has mapped the IT systems which require accurate time information and documented the requirements of the IT systems for the accuracy and availability of time information.
b. Upon the deployment of the NTP (Network Time Protocol), it is documented which NTP servers are used by which NTP clients.
c. It is defined whether the NTP servers operate in the client-server or in the broadcast mode.

OPS.1.2.6.M2 Secure use of external NTP servers

a. Before the deployment of an NTP server which is located outside of the local area network, the reliability of the service provider and the NTP server are analysed.
b. Only reliable NTP servers may be used for synchronising the clocks of an IT system outside of the local area network.
c. In the case of using an external NTP server, the terms and conditions of use established by the operator of the NTP server are observed.

OPS.1.2.6.M3 Secure configuration of an NTP server

a. Only authorised NTP clients can request the configuration details of the NTP server.
b. Only authorised users can change the configuration of the NTP server and only in clearly established cases.
c. If there is no accurate internal source of time, the internal NTP server is configured to receive regular and accurate time information from an external NTP server.

OPS.1.2.6.M4 Prohibition of undesired sources of time information

a. The settings of NTP clients only permit using permitted sources of time information for synchronising the clocks of IT systems; other sources of time information are blocked under the settings.

3.3 Standard measures

OPS.1.2.6.M5 Operating NTP in the client-server mode

a. NTP servers are configured for communication in the client-server mode. An NTP server only sends time information as a response to inquiries from active NTP clients.

OPS.1.2.6.M6 Monitoring internal NTP servers

a. The availability, resource use, and accuracy of the time of the NTP servers located in the computer network of the organisation are monitored regularly.
b. At least the following is logged in the case of an IT device functioning as an NTP server:
- unexpected reboots;
- unexpected reboots of the NTP service;
- failures of the NTP service;
- abnormal time information.

c. If an NTP server is operating in the broadcast mode, the accuracy of the time of the NTP clients is also monitored to detect discrepancies in the time information.

OPS.1.2.6.M7 Secure configuration of NTP clients

a. The sources which are used by the IT system to obtain time information upon activating and rebooting the IT system and after rebooting the NTP service are defined and configured unambiguously.

b. It is defined how the NTP clients respond to time information which is significantly different from the expected; any incorrect time information received is ignored.
c. Sufficient time information is ensured for the NTP clients even if the NTP server restricts responding to time inquiries or prohibits sending inquiries.

OPS.1.2.6.M8 Using secure protocols in synchronising clocks

a. Secure information exchange protocols are used in synchronising the clocks of IT systems.

3.4 Advanced measures

OPS.1.2.6.M9 Using different sources of accurate time information (A)

a. An organisation with a main process which requires highly accurate time uses more than one Stratum 1 NTP server in its computer network.
b. Each Stratum 1 NTP server is directly connected to an independent hardware-based (Stratum 0) source of time information, such as a GPS or radio clock, to obtain primary and accurate time information without a computer network.

OPS.1.2.6.M10 Only using internal NTP servers (I)

a. The IT systems which are connected to the intranet (NTP clients) only use internal NTP servers for synchronising clocks.

OPS.1.2.6.M11 Ensuring the redundancy of NTP servers (A)

a. The IT systems of an organisation with processes which require highly accurate time obtain the time information from at least four independent NTP servers.

OPS.1.2.6.M12 Ensuring the authenticity of NTP servers (I)

a. The NTP client verifies the authenticity of the NTP server before information exchange. The NTP client only accepts time information received from an authenticated NTP server.
b. The authentication requirement also applies to the NTP servers which share time information with lower-level NTP servers.

OPS.2 Operations as a service

OPS.2.2 Using cloud services

1 Description

1.1 Purpose

To present measures for the secure implementation and use of cloud services.

1.2 Responsibility

The IT department is responsible for complying with the measures for using cloud services.
Additional responsible persons: Data protection specialist, responsible specialist, management of the organisation, human resources department.

1.3 Limitations

The measures of the module complement outsourcing (see also OPS.2.1 Outsourcing) with the peculiarities of cloud services (the same infrastructure is used for servicing many clients). The measures of the service provider are described in the module OPS.3.1 Information security of the service provider. The module of using cloud services does not describe specific security measures of the respective application interfaces (APIs) of cloud services. The measures depend on the cloud service that is used; therefore, the selection of measures might differ between services.

2 Threats

2.1 Absence or inadequacy of the cloud service strategy

In case of an absent or inadequate cloud service strategy, the organisation might decide to choose an unsuitable cloud service or service provider. The selected cloud service might not be compatible with the information technology and business processes of the organisation or correspond to the required level of the protection requirement.

2.2 Dependency on the cloud service provider (loss of control)

When using an external cloud service, the organisation depends on the cloud service provider and does not have full control of the information regarding the business processes and their security. The

organisation does not know whether the cloud service provider implements the security measures according to requirements. The use of an external cloud service often causes the know-how of the information security and IT in the organisation to decrease.

2.3 Inadequate management of requirements when using cloud services

When an organisation decides to use a cloud service, it comes with great expectations of the users for better performance or functionality. However, the goal of the management of the organisation is often related to decreasing costs. If the opinion of all parties is not considered when establishing the requirements for the cloud service, then transferring to a cloud service might not provide the desired additional value.

2.4 Violation of legislative requirements

International providers of cloud services often comply with the legislative acts of third countries. The clients of the cloud service might fail to pay adequate attention to the legal framework conditions. Therefore, they might violate the requirements of the local legislative acts out of ignorance and jeopardise the security of information of the external service.

2.5 Lack of simultaneous operation capability of the cloud service provider

Various clients mostly use a shared infrastructure in case of cloud computing (such as IT systems, networks, and applications). If the resources of various clients have not been sufficiently securely separated, the client might gain unauthorised access to the data of another client.

2.6 Inadequacy of the contract concluded with the cloud service provider

If the contract with the cloud service provider does not describe areas of responsibility, tasks, performance indicators, or expenses adequately or clearly enough, then the cloud service provider might fail to implement all necessary security measures either inadvertently or due to a lack of resources. The client of the cloud service could be negatively affected by circumstances not covered by the contract. For example, when the dependence of the service provider on a third party is not known, it could negatively affect the information security and the service quality of the organisation.

2.7 Inadequate planning of the migration to cloud services

An inadequate plan for transferring to cloud services jeopardises data security. If the organisation discards testing the migration with test data and a small-scale pilot project, then there is a risk that the services will not work as required after full-scale migration.

2.8 Inadequate integration of cloud services with own IT systems

If the cloud services are not integrated into the IT infrastructure of the organisation in a suitable manner or if it is done insufficiently, then the users cannot use the cloud service to its full extent. The agreed functionality and productivity might not be achieved, disrupting the business processes. Insufficient integration with the information technology of the organisation might cause significant security vulnerabilities.

2.9 Inadequate regulation of terminating the use of cloud services

If the termination of the contract has been agreed insufficiently, it could cause significant losses for the company. Without sufficient internal preparedness, the organisation would find it difficult to transfer the cloud service to another service provider quickly or integrate it into the organisation's IT systems. If the transfer of the service stretches over time and the data cannot be transferred completely, it might cause downtime and data losses.

2.10 Inadequacy of the management framework of the cloud service

Adopting a cloud service often changes the distribution of roles related to the service (e.g. system administrators might become service administrators). Changes in the administration of a cloud service might temporarily affect the quality of the service. If the employees are not trained in their new tasks or the training is insufficient, it might lead to service disruptions and problems with service administration.

2.11 Inadequacy of the emergency response concept

In case of a partial or complete disruption of the cloud service, unexpected situations and shortcomings in the emergency response concept could prolong the downtime. If the buyer of the service and the service provider have not agreed on the steps to take in an emergency scenario (e.g. when the external connections are cut on a national level), the recovery time will be even longer.

2.12 Malfunctions in the system of the cloud service provider

If a malfunction occurs in the IT systems of the cloud service provider, it will also affect the client of the cloud service, and in the worst case, the service will be completely unavailable. Malfunctions in the interface between the cloud service provider and the client or a successful attack against the cloud computing platform would lead to a similar result.

3 Measures

3.1 Life cycle

Planning

OPS.2.2.M1	Cloud service strategy
OPS.2.2.M2	Cloud service security policy
OPS.2.2.M3	Preparing a list of cloud services
OPS.2.2.M4	Determining the areas of responsibility and interfacing
OPS.2.2.M5	Plan of migration to a cloud service
OPS.2.2.M6	Action plan for joining a cloud service
OPS.2.2.M7	Security programme for cloud services

Acquisition

OPS.2.2.M8	Criteria for selecting a cloud service provider

Implementation

OPS.2.2.M9	Cloud service contract that meets the customer's needs
OPS.2.2.M10	Safe migration to a cloud service

Emergency response

OPS.2.2.M11	Security programme for the emergency response of cloud services

Operation

OPS.2.2.M12	Information security when using cloud services
OPS.2.2.M13	Verification of the sufficiency of the cloud service security

Disposal

OPS.2.2.M14	Regular termination of a cloud service contract

Additional advanced measures

OPS.2.2.M15	Guaranteeing the transferability of a cloud service
OPS.2.2.M16	Additional backup of data
OPS.2.2.M17	Encryption when using cloud services

OPS.2.2.M18 Regular use of federation services

OPS.2.2.M19 Background checks for the staff of the cloud service provider

3.2 Key measures

OPS.2.2.M1 Cloud service strategy [responsible specialist, management of the organisation, data protection specialist]

a. A strategy for cloud services has been established which complies with the organisational objectives; it documents the following:

- the objectives, advantages, and risks of a cloud service;
- legal, regulatory, economic, and technical framework conditions related to the use of cloud services;
- expected cloud services and their use;
- conditions for terminating a cloud service.

b. An analysis of feasibility, profitability, and security is conducted for each planned cloud service.

c. A step-by-step plan for the implementation of a service is prepared for the implementation of a cloud service.

OPS.2.2.M2 Cloud service security policy [responsible specialist]

a. The cloud service security policy is prepared based on the cloud service strategy (see also OPS.2.2.M1 Cloud service strategy).

b. The security requirements are determined based on the protection requirements of the service and the regulatory, technical, and legal framework conditions.

c. In the case of international service providers, state-based specifics and regulatory requirements have been taken into account.

OPS.2.2.M3 Preparing a list of cloud services [responsible specialist]

a. All planned and used cloud services are documented on a uniform basis.

b. At least the following data is presented for every cloud service:

- name and designation of the service;
- purpose of the service;
- parameters of the service and/or the contractual service level;
- time frames of the service;

- billing information;
- access rights and authentication method;
- contact persons.

OPS.2.2.M4 Determining the areas of responsibility and interfacing [responsible specialist]

a. Areas of responsibility related to the use of the cloud service and the activities of the parties to the service are defined and documented.
b. The necessary IT components for the implementation of a cloud service (e.g. data backup system) and hardware and software interfacing are selected and documented.

3.3 Standard measures

OPS.2.2.M5 Plan of migration to a cloud service [responsible specialist]

a. In order to transfer to a cloud service, the plan for migration to a cloud service is prepared which determines:
- roles and obligations;
- preparations for the IT environment and operational procedures,
- testing and transfer procedures;
- compliance checks of the level of service and security;
- procedures for withdrawing from a cloud service.

b. When transferring to a cloud service, the effect of the cloud service on the existing IT environment and the organisational work processes is assessed, interfacing with the existing IT systems is designed, and additional trainings are planned.

OPS.2.2.M6 Action plan for joining a cloud service

a. An action plan for joining a service is prepared to adopt a cloud service which includes at least the following activities:
- preparations and launch of the interface;
- suitability and testing of network connections;
- organisation of the service administration;
- data management.

b. The action plan for joining a cloud service has been documented and the action plan is updated regularly.

OPS.2.2.M7 Security programme for cloud services

a. A security programme for cloud services is prepared based on the cloud service security policy (OPS.2.2.M2 Cloud service security policy), which describes risks specific to the cloud (e.g. dependency on the cloud service provider, simultaneous operations, fixed data formats, access to data).
b. The security programme for the cloud service complies with the agreements concluded between the cloud service provider and the network provider and the terms of use of the service.

OPS.2.2.M8 Criteria for selecting a cloud service provider [management of the organisation]

a. In order to select a cloud service provider, a specification of requirements that includes and completes the data from the list of cloud services (see also OPS.2.2.M3 Preparing a list of cloud services) is prepared.
b. The following aspects are taken into account when selecting a cloud service provider:

- the reputation of the service provider;
- the area of activity of the service provider and specialisation in cloud services;
- public market analyses and recommendations;
- location and jurisdiction of the service provider;
- efficiency and availability of the service;

a customer-friendly attitude;

- the use of subcontractors;
- the suitability of contractual terms and conditions;
- terminating the service;
- cost-effectiveness.

c. The correctness of the service description received from the cloud service provider and the validity of certificates is checked by asking for additional information from the service provider.

OPS.2.2.M9 Cloud service contract that meets the customer's needs [management of the organisation]

a. The contract between the organisation and the cloud service provider determines the following:

- legal framework conditions;
- type and volume of information related to the cloud service;
- the efficiency and quality of the service;

- security requirements;
- the location of receiving the service;
- subcontractors or other third parties;
- requirements for the staff of the cloud service provider;
- communication paths and contact persons;
- organisation of work, responsibilities, and access rights;
- procedure for changes;
- testing and monitoring of the service;
- handling malfunctions and incidents;
- termination of the contract, follow-up activities, data handling.

OPS.2.2.M10 Safe migration to a cloud service [responsible specialist]

a. A previously developed plan (see also OPS.2.2.M5 Plan of migration to a cloud service) and a security programme (see also OPS.2.2.M7 Security programme for cloud services) are taken into consideration when migrating to a cloud service.
b. Before the actual adoption, the migration is tested in a test environment.
c. After the IT systems are migrated to an operational environment, the compliance of the service with the contractual terms and conditions is verified.

OPS.2.2.M11 Security programme for the emergency response of cloud services

a. A programme for emergency preparations is prepared for the cloud services in use which establishes:
- the contact persons;
- the procedure for handling emergencies, responsibilities, operations, and documentation;
- backup of data, interfaces, means, and infrastructure;
- the necessary technical means;
- organising trainings for handling emergencies.

OPS.2.2.M12 Information security when using cloud services

a. The documentation and instructions for the use of a cloud service are updated regularly.
b. The compliance of the cloud service with the terms and conditions and security requirements agreed in the respective service agreement is checked regularly.

c. The organisation checks regularly whether the security programme for cloud services (see also OPS.2.2.M7 Security programme for cloud services) is compliant and up to date.
d. Cloud service administrators comply with the measures in modules ORP.3 Increasing awareness of information security and training and OPS.1.1.2: IT systems management.
e. The functioning of data backup is checked regularly.
f. Handling emergencies is practised regularly in cooperation with the service provider.

OPS.2.2.M13 Verification of the sufficiency of the cloud service security

a. The cloud service provider proves the compliance of the information security with the regulatory requirements and/or internationally recognised criteria by presenting the respective certificates, accreditation, or audit results.
b. The evaluation of the proof verifies that the scope of the certificates covers the used cloud service.
c. When using the services of subcontractors for cloud services, they are required to prove meeting the same criteria as well.

OPS.2.2.M14 Regular termination of a cloud service contract [responsible specialist, management of the organisation]

a. In the event of a termination of a cloud service contract, procedures have been established for switching to an internal service or another cloud service provider while fulfilling all existing service requirements.
b. When terminating the cloud service contract, it does not negatively affect the continuity of the organisational business processes.
c. In case of expiry of the contract, the cloud service contract determines:
- right of ownership of the parties to the contract to the means of providing the service;
- delivering the service documentation and the necessary data to the client;
- secure removal of the client data from the service provider.

3.4 Advanced measures

OPS.2.2.M15 Guaranteeing the transferability of a cloud service [responsible specialist] (A)

a. Criteria have been established for switching the cloud service provider or switching to an internal service, which include portability requirements and the obligation to test the portability of a service.

b. The necessary portability is possible in accordance with the cloud service contract (see also OPS.2.2.M9 Cloud service contract that meets the customer's needs).

OPS.2.2.M16 Additional backup of data [responsible specialist] (I-A)

a. The cloud service contract presents detailed requirements for data backup to the service provider.
b. The cloud service contract determines the rights of the client to make additional data backup copies.
c. It has been decided whether, in addition to the data backup of the cloud service provider, the organisation will conduct additional data backup on its own.

OPS.2.2.M17 Encryption when using cloud services (I-A)

a. All processed data is exchanged in an encrypted manner between the cloud service provider and the organisation.
b. In order to encrypt the data in their storage or processing location, an agreement has been reached on whether the organisation that uses the cloud service encrypts the data (before sending it to the cloud service provider) or the forwarded data is encrypted in the IT systems of the cloud service provider.
c. If the cloud service provider encrypts the data, the allowed encryption mechanisms, key lengths, and requirements for secure key management are determined in the cloud service contract.
d. If the organisation encrypts the data, the process is coordinated with the service provider ahead of time. When implementing the measures, the module CON.1 Cryptography concept is also taken into consideration.

OPS.2.2.M18 Regular use of federation services [responsible specialist] (C-I-A)

a. When federation services are used for cloud services, only the necessary information with the identity token from the central directory service (SAML - Security Assertion Markup Language) is forwarded to the cloud service provider.
b. User rights are controlled regularly and only authorised users receive an identity token.

OPS.2.2.M19 Background checks for the staff of the cloud service provider [human resources department] (C-I-A)

a. The requirements and criteria for verifying the qualifications and trustworthiness of the staff have been agreed with the cloud service provider.
b. The cloud service provider proves the trustworthiness and compliance with the client's criteria of its staff.

OPS.2.3 Outsourcing

1 Description

1.1 Purpose

To present measures for achieving security objectives in outsourcing and improving information security during the entire life cycle of outsourcing.

1.2 Responsibility

IT department is responsible for the compliance with outsourcing measures.
Additional responsible persons: Procurement department, responsible specialist, the management of the organisation, head of emergencies, human resources department, administrative department.

1.3 Limitations

The module discusses security risks of outsourcing from the point of view of the outsourcer. Service provider's point of view is presented in module OPS.3.2 Information security of a service provider. In this module, outsourcing is IT outsourcing. Additional security analysis is needed in the case of procurements that only partly entail information technology. The module does not discuss the security of data exchange channels that are used for communication with a service provider. Cloud services are discussed in module OPS.2.2 Using cloud services. Requirements for the staff and physical security of a service provider are listed in module groups ORP. Organisation and personnel and INF. Infrastructure.

2 Threats

2.1 No outsourcing strategy

If a service provider is not presented with information security requirements or the security needs of the object of a procurement during the entire life cycle of the object when outsourcing, then the actual status of information security of the service provider might prove to be insufficient for the business processes of the client. There is a threat of damage to the business processes of the client and leaks of sensitive information.

2.2 Insufficient control over critical business processes

If some of the necessary knowledge and skills transfer to the service provider, the organisation will not have complete control over key business processes. The processes cannot be managed quickly and adequately. When a business process is interrupted, there may be problems with restoring the business process to the required state in a timely manner.

2.3 Dependency on a service provider

The decision to use outsourcing could lead to a complete dependence of the organisation on a service provider, leading to a loss of know-how and control over the business process. The security controls that are implemented might not correspond to the actual protection requirement. The client might not notice shortcomings in the information security of a service provider. A service provider might take advantage of the situation (e.g. increase the service fees significantly).

2.4 Inadequate level of information security of a service provider

If information security requirements are not explained to a service provider when outsourcing, the IT systems of the service provider or the service itself might contain vulnerabilities which an attacker can use for an attack against the IT systems of the organisation. An incident caused by a service provider might have direct financial consequences for the organisation as well as lead to reputational damage.

2.5 Insufficient control over an outsourced service

When outsourced services or processes are inadequately managed, the transparency and manageability of the processes decreases. The outsourcer has no control over the processes and activities of a service provider. The organisation cannot guarantee that a service provider of an outsourced process applies the necessary level of care to ensure the quality and the required security level of the service.

2.6 Insufficient agreements regulating the service

Agreements concluded with a service provider might not include all of the obligations of the service provider and all security measures that are to be applied. Neglecting to document security requirements might later hinder the submission of claims against a service provider. For example, if an agreement does not specifically establish a notification obligation, the service provider might fail to comply with it. Unimplemented security controls might cause the requirements of legislative acts to be ignored. Insufficient security controls in an agreement concluded with a service provider present a risk to the availability of a business process and the confidentiality of data.

2.7 Inadequacy of the management of access rights

Depending on the object of a procurement, the staff of a service provider might need access rights to the IT systems, data, or premises of the organisation. If granting, managing, and monitoring access rights has been poorly organised by the service provider, the data of clients might be jeopardised. Granting unmonitored access rights to the staff of a service provider facilitates the abuse of the aforementioned rights to copy or manipulate data.

2.8 Uncontrollability of the outsourced services of a service provider

A service provider might, in turn, acquire the necessary resources for the provision of a service from its own subcontractors. The entire process becomes more complex and less transparent due to additional parties. Control over the service provider lessens. The employees of the additional partners might not be aware of or comply with the security requirements that were originally agreed on.

2.9 Lack of key performance indicators (KPIs)

The organisation must be able to verify whether an outsourced service has been carried out and managed by a service provider as required. When no qualitative or quantitative KPIs for measuring the level of service have been established or if they fail to provide material results about the quality of the service or compliance with security requirements, then the service quality might deteriorate over time. Moreover, it will not be possible to verify and determine whether the service provider complies with the agreed security requirements.

2.10 Insufficient stipulations regarding the termination of an outsourcing relationship

If service agreements do not establish specific conditions for terminating a service, the client of the service might fail to terminate the contract without bearing remarkable expenses. If a service provider wants to set a term of cancellation that is too short, then this might force the client to quickly choose a new and unsuitable service provider. In addition, terminating a service might cause various security problems. Insufficient rules for deleting data (incl. backup data) could cause leaks of confidential information.

2.11 Insufficient disaster recovery of outsourced services

In case of an emergency or a crisis, outsourced services might be interrupted. Restoring processes that work well under normal circumstances might not be successful in an emergency situation. Interferences and emergencies are usually unexpected and cannot be entirely controlled. The concurrent service disruption leads to direct negative business consequences. All related companies are going to suffer damage - both the service providers and the clients. This type of cascade effect has a significant impact in the context of subcontracting.

3 Measures

3.1 Life cycle

Planning

OPS.2.3.M1	Security requirements for outsourced services
OPS.2.3.M2	Risk-based approach to holding procurements
OPS.2.3.M8	Preparing an outsourcing strategy
OPS.2.3.M9	Establishment of a procurement policy

Implementation

OPS.2.3.M3	Criteria for selecting a service provider
OPS.2.3.M4	Compliance of a service agreement with the requirements of the client
OPS.2.3.M5	Evaluating the multi-tenancy capabilities of a service provider
OPS.2.3.M6	Security principles for outsourced services
OPS.2.3.M10	Assigning contact persons responsible
OPS.2.3.M13	Avoiding a conflict of interest when concluding a service agreement
OPS.2.3.M14	Extended requirements for service agreements

Operation

OPS.2.3.M7 Regular termination of an external service agreement

OPS.2.3.M11 Register of outsourced services

OPS.2.3.M12 Reports on outsourced services

OPS.2.3.M15 Secure network connection between a service provider and a client

OPS.2.3.M16 Information security reviews of a service provider

OPS.2.3.M17 Rules for relying on the staff of a service provider

OPS.2.3.M18 Review of agreements concluded with a service provider

OPS.2.3.M19 Mapping alternative service providers

Emergency response

OPS.2.3.M20 Emergency response in the case of outsourcing

Additional advanced measures

OPS.2.3.M21 Concluding escrow agreements for software source code

OPS.2.3.M22 Conducting joint emergency drills

OPS.2.3.M23 Encryption of sensitive data

OPS.2.3.M24 Background checks for the staff of a service provider

OPS.2.3.M25 Sandboxing the data of a service provider

3.2 Key measures

OPS.2.3.M1 Security requirements for outsourced services [responsible specialist]

a. Security requirements based on a protection requirement and/or business impact assessments (BIAs) are established for all outsourced services.
b. When determining the security requirements for a service, the nature of the processed data and the type of security necessary for data exchange procedures and interfaces are taken into account.
c. When deciding the security requirements for an outsourced service, the interdependence between business processes and the input and output of processes has been taken into account.

OPS.2.3.M2 Risk-based approach to holding procurements

a. The possibility of outsourcing a service is decided based on risk and the previously determined protection requirement and risk profile.
b. The continued compliance of an outsourced service with the approved risk profile is verified regularly.

OPS.2.3.M3 Criteria for selecting a service provider [responsible specialist, procurement department]

a. A profile of specifications that contains security requirements has been prepared to select a service provider.
b. The following criteria for selecting and assessing a service provider have been established:
- suitability and transparency of services;
- compliance with the security requirements of the client;
- reputation and recommendations of the service provider;
- business culture of the service provider (in the case of a foreign service provider);
- qualifications of the staff of the service provider.

c. When selecting a service provider, the potential for a conflict of interest is evaluated.
d. The continued compliance of a service provider with the selection criteria for service providers is verified regularly.

OPS.2.3.M4 Compliance of a service agreement with the requirements of the client

a. All aspects of an outsourced service are agreed with a service provider in writing in the respective service agreement. A uniform agreement form has been prepared for service agreements.
b. Rights and obligations of contractual partners related to information security, established in the service agreements, are based on risks that have been previously mapped (see OPS.2.3.M1 Security requirements for outsourced services).
c. A service agreement stipulates details related to managing the provision of an outsourced service, such as the conditions of use of the infrastructure, authorising or not authorising subcontracting, requirements for staff, personal data protection, avoiding conflicts of interest, and handling malfunctions and incidents.
d. A service provider guarantees the availability and access rights to the information that is necessary for checking compliance, and if necessary, auditing options.
e. If necessary, a non-disclosure agreement (NDA) is concluded with a service provider to protect sensitive information.

OPS.2.3.M5 Evaluating the multi-tenancy capabilities of a service provider

a. The service provider guarantees the secure separation of client data when providing similar services to several clients, and submits a confirmation to that effect.

b. When requested by the client, the service provider presents technical specifications of the measures implemented to protect client data and to separate the data from public data as well as the information of other clients.

OPS.2.3.M6 Security principles for outsourced services

a. As a minimum, the service provider has implemented an information security management system (ISMS) to the extent of the outsourced service.
b. The organisation has determined and agreed with the service provider the modules and information security measures of the Estonian Information Security Standard (Estonian abbreviation 'E-ITS') that the service provider is obligated to implement.
c. The service provider has verifiably implemented E-ITS information security measures from all relevant E-ITS modules in the scope of the service. The E-ITS security measures selected by the service provider correspond to the protection requirements defined by the client.
d. The service provider proves the implementation of information security measures by submitting an auditor's report of an E-ITS audit or an ISO/IEC 27001 certificate issued by an accredited certification body. The scope of the audit presented in the auditor's report or the certificate covers all business processes and support services related to the outsourced service.
e. In the absence of an E-ITS auditor's report or a valid ISO/IEC 27001 certificate, the organisation makes sure (as a consumer of the service) that the requested information security measures which must be implemented are actually applied by the service provider.
f. The organisation has a contractual right to conduct information security inspections and audits in the organisation of the service provider or to commission them from an independent third party.

OPS.2.3.M7 Regular termination of an external service agreement [responsible specialist, management of the organisation]

a. A service agreement establishes the conditions for the regular termination of the agreement (for example, a notice period). The termination of the agreement according to the terms and conditions does not affect the continuity of the work processes of the client.
b. A service agreement establishes the terms and conditions for the extraordinary termination of the agreement.
c. A service agreement determines the rights and obligations of the parties at the termination of the agreement, including the obligation of the service provider to securely deliver or delete the client's data in their possession.

d. The parties have agreed on the manner of returning the data, software, and hardware. Legal requirements are followed when returning the aforementioned.
e. The parties have agreed on the manner of closing user accounts and removing access rights when the contractual relationship with the service provider ends.

3.3 Standard measures

OPS.2.3.M8 Preparing an outsourcing strategy [management of the organisation]

a. The organisation has established economic, technical, regulatory, and legal framework conditions and an outsourcing strategy that includes information security aspects.
b. The outsourcing strategy describes the goals, opportunities, and risks of outsourcing.
c. The client of the outsourced service has the necessary capabilities, competence, and resources for determining and verifying the information security requirements of the service.

OPS.2.3.M9 Establishment of a procurement policy [management of the organisation]

a. Based on the outsourcing strategy (see OPS.2.3.M8 Preparing an outsourcing strategy), the organisation has prepared and approved a procurement policy.
b. The procurement policy considers the information security needs of the organisation and contains typical requirements for contracts concluded with the service provider (see OPS.2.3.M4. Compliance of a service agreement with the requirements of the client).
c. The procurement policy establishes the testing methods and approval processes for using an outsourced service.
d. The procurement policy determines whether a service provider is allowed to rely on subcontractors when providing its services and under which conditions it is permitted.

OPS.2.3.M10 Assigning contact persons responsible [human resources department]

a. Internal and external communication partners with established rights and the contents of the forwarded information have been assigned for each outsourced service.
b. Both parties verify the existence and validity of the authorisation of their communication partner. The details of the communication partners are updated and documented.

OPS.2.3.M11 Register of outsourced services

a. The person responsible for outsourcing collates documents related to outsourcing into a register of outsourced services.
b. The register of outsourced services contains information about service providers, key process indicators (KPIs), the business-critical nature of processes, concluded agreements, and any changes in the services.

OPS.2.3.M12 Reports on outsourced services [responsible specialist]

a. The person responsible for outsourcing prepares regular reports on the current status of the services and potential issues for the management.
b. Reports on services include information on information security events and incidents which have taken place.

OPS.2.3.M13 Avoiding a conflict of interest when concluding a service agreement [management of the organisation]

a. When negotiating the terms and conditions of service agreements, representatives of various areas within the organisation participate in negotiations.
b. When preparing service agreements, potential conflicts of interest between a possible business partner and information security are avoided.

OPS.2.3.M14 Extended requirements for service agreements

a. A service agreement determines which objects and network services a service provider can access in the network of the client.
b. The key performance indicators (KPIs) of a service are documented as part of the service agreement. If the service does not comply with the agreed KPIs, sanctions may be applied against the service provider (such as a contractual penalty).
c. The service agreement contains various possibilities for terminating the outsourced service and includes related procedures for returning client data and assets.
d. The service agreement includes the obligations of the parties and guidelines for emergencies.

OPS.2.3.M15 Secure network connection between a service provider and a client

a. Before a service provider is allowed to access the network of a client, the following is agreed upon and documented:

- regulatory and technical conditions for using the connection;
- protection requirements and security controls of the connection;
- confidentiality obligations of the parties;
- special conditions for a foreign service provider.

b. The service provider and the client assign contact persons who will solve regulatory and technical issues related to the network connection.
c. The service provider and the client have agreed on the notification paths for network connection incidents and the procedure for handling the incidents.

OPS.2.3.M16 Information security reviews of a service provider

a. The implementation of security requirements by a service provider, stipulated in the respective service agreement, is verified regularly.
b. The results of the review of the information security of the service provider are documented.

OPS.2.3.M17 Rules for relying on the staff of a service provider

a. Before starting to provide a service, the valid requirements of the client are explained to the staff of the service provider. The staff of the service provider confirms by signature that they undertake to comply with the valid requirements of the client.
b. The service provider and the client have agreed on the procedures for replacing the employees of the service provider and for terminating employment.
c. External staff that visit the premises of the client for a short period or only once are treated similarly to regular visitors.

OPS.2.3.M18 Review of agreements concluded with a service provider

a. Security measures contained in the agreements concluded with a service provider are regularly inspected to check whether they are up to date and relevant. Whenever insufficient security measures are found, agreements concluded with the service provider are updated.
b. Agreements concluded with a service provider are reviewed and, if necessary, updated after an information security incident, a significant change in the nature of relevant risks, and any amendments to the law.

OPS.2.3.M19 Mapping alternative service providers

a. Action plans have been prepared for instances of ordinary or extraordinary termination of outsourced services to migrate services to an alternative service provider.
b. Potential service providers have been mapped who have a suitable company profile and sufficient level of information security for transferring the services.

OPS.2.3.M20 Emergency response in the case of outsourcing [head of emergency]

a. An emergency response plan is developed for outsourced services, which includes the recovery of IT components, interfaces, and communication channels of the provider and the recipient of a service.
b. The responsibility, contact persons, and procedures of the provider and the recipient of a service are documented in the emergency response plan for outsourced services.
c. The organisation checks the implementation of emergency measures by a service provider; for this purpose, the provider and the recipient of the service organise joint incident handling drills.

3.4 Advanced measures

OPS.2.3.M21 Concluding escrow agreements for software source code (I-A)

a. The escrow of software source code and other essential materials has been considered when ordering software from a service provider.
b. As a minimum, the escrow agreement regulates the following:

- user and modification rights of the software;
- instances of disclosing the source code;
- suitable storage and protection of the source code;
- procedure and frequency of depositing the source code.

OPS.2.3.M22 Conducting joint emergency drills [head of emergency] (A)

a. The organisation conducts joint emergency drills with service providers.
b. The results of the emergency management drills are used for improving the concept of emergency management and cooperation between the parties.
c. Joint emergency drills with service providers are conducted regularly.

OPS.2.3.M23 Encryption of sensitive data (C)

a. In the course of data communication between a service provider and a client, sensitive data is transferred in an encrypted format.
b. Data that is stored on a data carrier is protected from unauthorised access by encrypting the data or the data carrier.
c. If possible, state-approved and certified encryption software is used.

OPS.2.3.M24 Background checks for the staff of a service provider [human resources department] (C-I-A)

a. The provider and the recipient of a service establish the criteria for conducting the security checks of the service provider's employees in the service agreement.
b. The provider and the recipient of a service agree on which security checks are conducted and which party carries out the background checks.

OPS.2.3.M25 Sandboxing the data of a service provider (C-I-A)

a. Data received from a service provider is sandboxed.
b. Attachments of incoming emails are first opened in the sandbox.
c. The applications and updates of a service provider that is developing software is first tested in a sandbox.

OPS.3 Operations of the service provider

OPS.3.2 Information security of the service provider

1 Description

1.1 Purpose

To present measures for planning, implementing, managing, and controlling the information security of a service provider and for maintaining the required level of security from the point of view of the service provider. Risks related to the provision of a service must not endanger the users of the service. The general responsibility for the security of a service remains with the user of the service.

1.2 Responsibility

The IT department is responsible for implementing the information security measures of the service provider.
Additional responsible persons: Head of emergency, human resources department.

1.3 Limitations

This module defines services as IT services. The module contains security measures that apply to service providers. The point of view of a service recipient is discussed in module OPS.2.3: Outsourcing. It must also be taken into account in instances where a service provider itself relies on outsourcing. The module does not examine the security of communication channels between the service provider and the client of an outsourced service.

2 Threats

2.1 Inadequate information security management of a service provider

Inadequately established or non-compliant information security management of a service provider is expressed as the lack of accountability for information security, insufficient support from management, and non-transparent security processes. In case of inadequate information security management, a service provider is unable to meet the information security management requirements of the organisation that uses the service. The inadequacy of a service provider in information security matters is a threat to all organisations that use the service.

2.2 Inadequate emergency management of a service provider

The interruptions and disruptions in the IT systems of a service provider can affect the normal functioning of the processes of the service users. If a service provider has not sufficiently prepared for emergencies, restoring the services might take longer and the clients' business processes could be interrupted to a greater degree than agreed in the service agreement.

2.3 Incomplete service agreements with the recipients of a service

When the protection requirement and security requirements for data and systems based thereon have not been agreed on by a client and a service provider, the client's data might not have the necessary protection. If security requirements are not described in service agreements, a party would have no basis for submitting a financial claim against the other party in the case of security failures.

2.4 Weaknesses in interfacing with the IT systems of a service provider

If the IT interface between a client of an outsourced service and a service provider is not sufficiently protected, the services might be disrupted and data could be lost. An attacker may use unprotected or insufficiently protected data interfaces for launching an attack. Moreover, unauthorised access to data by outsiders cannot be excluded. If the parties have not agreed on emergency procedures, it could affect the efficiency of responding to emergencies.

2.5 Dependence of a user of a service on the service provider

Outsourcing could lead to a complete dependence of the recipient of a service on the service provider, leading to a loss of know-how and control over business processes. The service provider can take advantage of this situation. Service quality might deteriorate, the security measures implemented by the service provider might no longer comply with the security requirements agreed in the service agreement and the actual protection requirements of the user of the service. This may affect the relationship between the parties and lead to reputational damage and financial consequences related to contractual violations.

2.6 Inadequate management of access rights

If granting, managing, and controlling access rights is poorly organised by a service provider, granting rights to the staff of a client may be delayed or mistakes may be made when granting the rights. If the IT department of a service provider grants excessive rights to clients, they might gain access to the data of other clients as a result. Breaches of data confidentiality and integrity could mean that a service provider would have to face claims for compensation for damages resulting from contractual violations.

2.7 Service provider lacks multi-tenancy capabilities

If the IT systems and data of various clients are not separated securely enough, there is a risk that one client can access the data of another client. Service provider must also decide which client's interests it will protect first. If the affected clients are competitors, it might put the service provider in very uncomfortable situations.

2.8 The dependence of a service provider on subcontractors

If a service provider relies on outsourcing, the service provider might become dependent on the functioning of services provided by its partners. The service provider would not have complete control over its business processes so any disruptions in outsourced services could have a negative impact on the quality of services it provides externally. The service provider might suffer financial losses and reputational damage due to failing to perform its contractual obligations.

2.9 Inadequate procedure for terminating a service agreement

If the procedure for terminating a service agreement is inadequate, problems with delivering data to a client might arise. For example, data might not be transferred to the client fully and compliantly in the case of an extraordinary termination of the agreement. If data is not deleted by the service provider, the secure storage of data is not guaranteed and the data might fall into the hands of unauthorised persons. When storing data for a long period, there is a risk of violating statutory data retention periods.

2.10 Service Provider IT System Failure

Interruptions in the service provider's IT systems affect the availability of the service. Similar issues arise in the event of interface failures between the service provider and the client. If agreed upon in the contract, this may also entail financial costs for the service provider to satisfy the client's claims for damages.

2.11 Weaknesses in Integration with Service Provider's IT Systems

If the IT integration between the client's outsourced service and the service provider is not adequately protected, the confidentiality and integrity of the transmitted data may be at risk. Unprotected or poorly protected integrations may also result in unauthorized access to data by third parties.

2.12 Social Engineering

Social engineering can be used to manipulate people into acting in unauthorized ways. If the target of a social engineering attack is the service provider's employees, the attacker may gain access to the data of many companies.

2.13 Lack of Concurrent Service Capability at the Service Provider

If the IT systems and data of different clients are not adequately separated, there is a risk that one client may access another client's data. Additionally, the service provider must decide whose interests to prioritize. If the involved clients are competitors, this can lead to very uncomfortable situations for the service provider.

3 Measures

3.1 Life cycle

Planning

OPS.3.2.M1	Planning service security
OPS.3.2.M2	Standard terms and conditions of service agreements
OPS.3.2.M3	Security requirements when relying on subcontractors
OPS.3.2.M8	Principles for the provision of a service

Operation

OPS.3.2.M4	Principles for separating the data of clients
OPS.3.2.M6	Procedure for the ordinary and extraordinary termination of a service agreement
OPS.3.2.M9	Regular review of service agreements
OPS.3.2.M12	Risk assessment of the processes and IT systems of a service provider
OPS.3.2.M14	Monitoring the processes and IT systems of a service provider
OPS.3.2.M15	Reports submitted to clients
OPS.3.2.M16	Ensuring the transparency of the supply chain of a service
OPS.3.2.M17	Access control

Implementation

OPS.3.2.M5	Security concept of services
OPS.3.2.M7	Procedure for the replacement of subcontractors
OPS.3.2.M10	Establishing secure communication channels and assigning contact persons
OPS.3.2.M13	Secure data communication channels
OPS.3.2.M18	Raising awareness among the employees of a subcontractor

Emergency response

OPS.3.2.M11	Emergency response for a service

Additional advanced measures

OPS.3.2.M19	Background checks for the staff of a service provider

OPS.3.2.M20 Encryption of data communication channels and stored data

OPS.3.2.M21 Joint emergency and crisis trainings

3.2 Key measures

OPS.3.2.M1 Planning service security

a. The service provider has taken into account the information security needs of the users of a service when planning services.
b. The service provider is capable of ensuring the minimum acceptable level of information security to its clients.
c. The service complies with statutory requirements (including data protection).

OPS.3.2.M2 Standard terms and conditions of service agreements

a. The service provider has prepared standard terms and conditions for service agreements.
b. As a minimum, the standard terms and conditions of service agreements contain the following:
- general security requirements for using a service;
- protection principles of sensitive information and, if necessary, concluding the respective agreement (a non-disclosure agreement, NDA);
- rights and restrictions of the service provider when outsourcing (for example, using third-party cloud services);
- the right of the client to conduct information security reviews or audits to check compliance with information security requirements in the organisation of the service provider;
- procedure for exchanging information;
- service level descriptions.

c. The service provider has prepared service agreement forms containing standard terms and conditions.
d. The standard terms and conditions of service agreements are implemented in all service agreements concluded with clients.

OPS.3.2.M3 Security requirements when relying on subcontractors

a. Where a service provider relies on subcontractors, it guarantees that the conditions stipulated in the service agreements concluded with a client have been met and the required security level is maintained.

b. When transferring any tasks to a subcontractor that are necessary for the functioning of the service provided to a client, the service provider and the subcontractor conclude a contract that describes the transferred tasks and the related security requirements.
c. The client is entitled to review any agreements between the service provider and its subcontractors in regard to the services provided to the client.

OPS.3.2.M4 Principles for separating the data of clients

a. The service provider has developed and documented means and procedures for the sufficiently secure separation of the data and operational environments of different clients in the IT systems of the service provider.
b. The service provider has implemented measures that correspond to the protection requirements to separate the data of clients in its IT systems.
c. A client can review the measures and procedures for ensuring the separation of their data from the data of other clients if they so wish.

OPS.3.2.M5 Security concept of services

a. The service provider has prepared a security concept that covers all services provided to clients.
b. The security concept contains all general security measures and additional security measures applied to individual services.
c. Before concluding a service agreement, the security concept of services is approved by the client. If necessary, the client may propose changes regarding the service that is provided to the client.
d. The security concept and the rules for the categorisation of information approved by the client are parts of the service agreement concluded with the client.
e. The service provider inspects the application of the security concept of the services and the implementation of measures regularly.

OPS.3.2.M6 Procedure for the ordinary and extraordinary termination of a service agreement

a. A service agreement establishes the conditions for the ordinary termination of the agreement.
b. In the service agreement, the parties have agreed on the conditions for the extraordinary termination of the agreement to make sure that the termination of the agreement would not have a negative impact on the business processes of the client or the service provider.
c. The service agreement stipulates the right of ownership of the hardware and software used for

providing the service and the terms and conditions for their continued use after the termination of the agreement.
d. The service agreement documents data that is transferred at the termination of the agreement as well as procedures for returning data and hardware.
e. Unless agreed otherwise, client data still stored by the service provider is deleted securely after the end of the statutory retention period. The fact of deleting the data is documented.
f. When the agreement is terminated, the access rights of the service provider and the employees of the client are reviewed and unnecessary access rights are terminated.

3.3 Standard measures

OPS.3.2.M7 Procedure for the replacement of subcontractors

a. A service provider who relies on subcontractors has prepared a list of alternative subcontractors.
b. When an agreement concluded with a subcontractor is ordinarily or extraordinarily terminated, the service provider is capable of transferring the relevant activities without any negative impact and significant delays to another subcontractor or forgo using a subcontractor.

OPS.3.2.M8 Principles for the provision of a service

a. The service provider has documented its principles for the creation, testing, and commissioning of a service.
b. The service provider has decided whether external partners are allowed to be included in the provision of the service (subcontractors of the service provider).
c. The service provider has created a process for the assessment of risks associated with the service (including subcontracting risks).

OPS.3.2.M9 Regular review of service agreements

a. Compliance with the security measures stipulated in service agreements and the continued suitability of the security measures is inspected regularly and/or on an event basis. Client agreements containing insufficient security measures are updated.
b. Security requirements contained in the service agreements are also reviewed whenever risk assessments and legal acts pertaining to the service change. If necessary, the security requirements are updated.

OPS.3.2.M10 Establishing secure communication channels and assigning contact persons [personnel department]

a. The service provider establishes secure communication channels for exchanging information with its clients.
b. The service provider and the client have agreed and documented the nature of information to be transferred between the communication partners and the appointed contact persons for the parties.
c. The validity of the authorisations of the assigned contact persons is checked regularly.
d. The service provider and the client have agreed in the notifications paths for security incidents, contact persons, and the procedure for handling incidents.

OPS.3.2.M11 Emergency response for a service [head of emergency]

a. An emergency response plan has been prepared, entailing the relevant processes, components, and service interfaces of both parties.
b. The emergency response plan has been approved by the recipient of the service.

OPS.3.2.M12 Risk assessment of the processes and IT systems of a service provider

a. Before making any new applications, IT systems, or processes available to clients, the service provider has completed a risk assessment and determined appropriate measures for handling risks.
b. The results of the risk assessment are documented and used to upgrade information security further.

OPS.3.2.M13 Secure data communication channels

a. Before starting to exchange data, the following is agreed on and documented:
- applications that are used;
- data formats that are used;
- availability criteria of the data (including the response time for queries);
- security measures for data exchange (see also CON.9 Data exchange);
- security mechanisms (virus protection, encryption, signing, key management, etc.).

b. Prior to initiating data exchange, data communication channels are checked for potential vulnerabilities and to make sure that the required security level has been achieved.
c. To make sure that data exchange is functional, it is tested with test data before using the service.

d. The service provider and the client have agreed on security incident reporting routes, contact persons and incident resolution procedures.

OPS.3.2.M14 Monitoring the processes and IT systems of a service provider

a. The processes and IT systems related to services provided to clients are constantly monitored to make sure that they are fully functional.

OPS.3.2.M15 Reports submitted to clients

a. A standard report format and communication channels are agreed with the client.
b. The service provider submits reports on the functioning of the service to clients at agreed intervals.
c. Clients are informed of any upcoming changes in the processes pertaining to the service as early as possible.

OPS.3.2.M16 Ensuring the transparency of the supply chain of a service

a. The service provider has documented the processes where subcontractors participate, the main KPIs, subcontractors involved in the provision of the service, and agreements concluded with the latter.
b. The service provider checks the documentation pertaining to the subcontractors regularly to make sure that it is up to date and relevant. Any amendments in the agreements concluded with the subcontractors are documented.

OPS.3.2.M17 Access control

a. Entrance to premises, systems, and networks and access to data and software by the staff of a service provider and a client are controlled by the appropriate regulatory and technical means.
b. Access rights are allocated based on the least privilege principle according to professional needs.
c. Auditors are ensured the necessary access rights for their responsibilities.

OPS.3.2.M18 Raising awareness among the employees of a subcontractor

a. The staff of a subcontractor has been informed about the requirements for performing their tasks as well as valid information security requirements and documents regulating information security.
b. The employees of the subcontractor have confirmed that they undertake to comply with the

guidelines, rules of procedure, information security requirements, and confidentiality agreements which have been presented to them ahead of time.
c. In the case of enhanced security requirements, background checks are conducted for the staff of subcontractors and their compliance with the qualification requirements established by the service provider or the client is verified.

3.4 Advanced measures

OPS.3.2.M19 Background checks for the staff of a service provider [human resources department] (C-I-A)

a. The service provider verifies the reliability of new staff and the employees of a subcontractor before concluding an employment contract.
b. The parties of the service agree on the criteria for conducting background checks for the employees of the service provider.

OPS.3.2.M20 Encryption of data communication channels and stored data (C)

a. In order to transfer data securely and for the service provider to store it, secure encryption mechanisms based on the protection requirements of the data have been agreed.
b. The encryption mechanism is checked regularly to make sure that it functions properly.

OPS.3.2.M21 Joint emergency and crisis trainings (A)

a. The service provider conducts regular joint emergency and crisis trainings with the clients of the service.
b. The results of the joint trainings are used for upgrading the emergency response plan for services (OPS.3.2.M11 Emergency response plan for a service) and joint emergency procedures.

DER: DETECTION AND REACTION

DER.1 Detection of security incidents

1 Description

1.1 Purpose

To provide measures for the collection, correlation, and evaluation of security event data to ensure the comprehensive and timely detection of security incidents.

1.2 Responsibility

The IT department is responsible for the implementation of the measures for the detection of security incidents.
Additional responsible persons: The user, the responsible specialist, the employee, the manager.

1.3 Limitations

The module does not cover all of the aspects related to the detection of security incidents. The separation of responsibilities is addressed in ORP.1 Organisation of information security. Event logging measures are covered in module OPS.1.1.5 Logging. Data protection aspects of security incidents are addressed in module CON.2 Personal data protection. Intrusion prevention systems are addressed in modules OPS.1.1.4 Protection against malware and NET.3.2 Firewall.

2 Threats

2.1 Non-compliance with the law

The technical solutions used to detect security incidents and analyse log data may collect confidential information and sensitive personal data (for example, information obtained from monitoring the activities of employees). Such processing of personal data may be in breach of the provisions of the General Data Protection Regulation and the Personal Data Protection Act.

2.2 Insufficient qualification of the responsible persons

If, due to lack of training, the responsible persons are not able to distinguish security events from errors and faults that occur frequently in the day-to-day IT operations of the organisation, security incidents may go unnoticed.

2.3 Inadequate configuration of intrusion detection systems

If intrusion detection systems are not configured correctly, they can generate a large number of irrelevant alerts. The alert indicating a security incident cannot be distinguished from them and a potential attack may go undetected.

2.4 Lack of information about the IT system being protected

If there is insufficient information about the IT system in use, it is likely that critical components of the IT system will not be adequately protected and will remain uncovered by the detection systems. The activities of an attacker who has penetrated a computer network may remain undetected for a long period of time.

2.5 Infrequent use of detection systems

If detection systems are not used and the security event detection functions of IT systems and applications are not activated, it is much easier for an attacker to penetrate the network. The risk is even greater if the network is unsegmented and traffic between networks is not monitored. The attacker's activity on the network remains undetected.

2.6 Insufficient human resources

If there are insufficient human resources to analyse log data and attack vectors, or if employees do not monitor external sources of information about security vulnerabilities, security events may go undetected or the incident may be discovered only after significant damage has been caused. If security vulnerabilities in an organisation's IT systems are not remediated in a timely manner, an attacker is able to use the security vulnerability to launch an attack against the organisation.

3 Measures

3.1 Life cycle

Planning

DER.1.M1	Regulation on the detection of security incidents
DER.1.M2	Legality of log data analysis
DER.1.M3	Procedure for reporting security events
DER.1.M4	Raising employees' awareness
DER.1.M7	Training of the responsible persons

Operation

DER.1.M5	Implementation of the detection functions of the IT system
DER.1.M6	Continuous monitoring and analysis of log data
DER.1.M9	Additional detection systems
DER.1.M11	Centralised logging infrastructure for security event analysis

Improvement

DER.1.M12	Analysis of information from external sources
DER.1.M13	Regular review of detection systems

Additional advanced measures

DER.1.M10	TLS and SSH proxies
DER.1.M14	Employees specialised in log data analysis (C-l)
DER.1.M15	Centralised real-time management of event notifications
DER.1.M16	Implementation of detection systems based on the protection requirements
DER.1.M17	Automatic response to security events
DER.1.M18	Regular integrity checks

3.2 Key measures

DER.1.M1 Regulation on the detection of security incidents

a. Based on the overall security policy of the organisation, a regulation has been developed to describe the planning and operational activities required to detect security incidents in a timely manner.
b. The persons responsible for the detection of security incidents are aware of the regulation and use it as a basis for their actions. Changes to the regulation and deviations from it are coordinated with the information security manager and documented.
c. Compliance with the regulation for the detection of security incidents is regularly verified, and the results of the audits are documented.

DER.1.M2 Legality of log data analysis

a. A guide for the analysis of log data is prepared, setting out the applicable legal requirements. The guide is updated as the legal framework conditions change.
b. The analysis of log data and the use of detection systems comply with the requirements of data

protection-related and other applicable legislative acts (for example, legislation regulating the organisation of work relations).

DER.1.M3 Procedure for reporting security events

a. The organisation has established procedures for reporting security events, documenting communication channels and recipients for different types of incidents, the persons to be notified, the availability of persons, and the choice of communication channels depending on the urgency of the incident.
b. Employees are aware of their tasks and responsibilities. In the case of a suspected security event, the persons designated in the procedure for reporting security events are informed immediately, using the notification and communication channels set out in the procedure.
c. The functioning of the communication channels put in place is regularly tested and, if necessary, the procedure for reporting security events is updated.

DER.1.M4 Raising employees' awareness [manager, user, employee]

a. Employees are able to recognise a security incident and are motivated to report it.
b. Employees have been made aware that incident reports sent by customers or IT systems should not be ignored.
c. Employees know to whom to report security events and which communication channels to use (see DER.2.1 Handling of security incidents).

DER.1.M5 Implementation of the detection functions of the IT system [responsible specialist]

a. If the IT system in use has features that can be implemented to detect security incidents, these are enabled.
b. In the case of a security event, the event reports of the affected IT system are analysed and, where possible, events logged in other IT systems at the same time are assessed.
c. The collection of event reports in IT systems is regularly checked.
d. Where possible, event reporting is automated. A malware detection scanner automatically forwards the security event message to the responsible persons for further analysis.

3.3 Standard measures

DER.1.M6 Continuous monitoring and analysis of log data

a. The organisation has designated employees responsible for the continuous monitoring and analysis of log data.
b. IT systems-based log data analysis guidelines are in place to detect security incidents.
c. Adequate human resources are in place to carry out continuous monitoring and analysis of log data.

DER.1.M7 Training of the responsible persons [manager]

a. The persons responsible for the analysis of event reports have the necessary qualifications and have completed the relevant training.
b. When procuring IT systems or applications, the budget takes into account the training needs of the employees dealing with security events.

DER.1.M9 Additional detection systems [responsible specialist]

a. Based on the network diagram (see NET.1.1 Network architecture and solution), it is determined which network segments are protected by additional detection systems.
b. Additional detection systems and sensors are implemented to enhance the detection of security incidents.
c. Intrusion detection systems (IDS) are centrally managed.
d. A network intrusion detection system (NIDS) is used to protect the traffic between the external network and the internal network segments.

DER.1.M11 Centralised logging infrastructure for security event analysis [responsible specialist]

a. Event reports collected from IT systems are stored in a central logging infrastructure (see OPS.1.1.5 Logging).
b. The logging infrastructure allows event reports from multiple sources to be synchronised, correlated, analysed, and stored.
c. The collected event reports are analysed regularly to detect anomalies.
d. Security events stored in the logging infrastructure can also be analysed afterwards.

DER.1.M12 Analysis of information from external sources [responsible specialist]

a. Information on security vulnerabilities in IT systems is obtained from qualified external sources, with the relevant information reaching the right employees.
b. The relevance of information from qualified sources is assessed and, if necessary, the process for detecting and handling security incidents is modified (see also DER.2.1. Handling of security incidents).

DER.1.M13 Regular review of detection systems

a. Detection systems and the measures implemented within them are regularly checked to ensure that they are up to date and operational.
b. The results of the review are documented and compared with the results of previous reviews. Anomalies are verified.

3.4 Advanced measures

DER.1.M10 TLS and SSH proxies [responsible specialist] (C)

a. When migrating to an external network, TLS and SSH proxies are used to break the encrypted connection and to allow the transmitted data to be checked for malware.
b. TLS and SSH proxies use the automatic detection and notification of security events.

DER.1.M14 Employees specialised in log data analysis (C-l)

a. Employees specialised in log data analysis are appropriately qualified and have received appropriate training.
b. Specialised employees are involved in log analysis requiring specific knowledge (for example, in the field of forensics).

DER.1.M15 Centralised real-time management of event notifications (C-I-A)

a. Automated analysis based on a centralised software solution is used to identify security events, establish correlations, and make security-related circumstances visible.
b. The log data collected is complete and can be automatically analysed.
c. Log analysis is performed continuously and in real time, and when predefined thresholds for analysis parameters are exceeded, the designated employee is automatically alerted of the event.

d. The analysis parameters and decision criteria are regularly adjusted, and when new parameters are applied, previously validated data is also analysed.

DER.1.M16 Implementation of detection systems based on the protection requirements (C-I-A)

a. IT systems with higher protection requirements are protected by detection systems with the technical capability and capacity to operate under higher protection requirements.

DER.1.M17 Automatic response to security events (C-I)

a. An automatic intrusion prevention system (IPS) is in place that is capable of:
- identifying attacks, abuses, and violations;
- reporting security events automatically;
- responding to a security event with an automatic protection action.

DER.1.M18 Regular integrity checks (C-I)

a. Regular checks are performed to ensure that all detection systems are in good working order and that users have access rights to the system.
b. Automatic file integrity checks and alerts are in place in the event of loss of integrity.

DER.2 Management of security incidents

DER.2.1 Handling of security incidents

1 Description

1.1 Purpose

To provide guidance on the systematic handling of security incidents.

1.2 Responsibility

The information security manager is responsible for the implementation of security incident handling measures.

Additional responsible persons: The data protection specialist, the responsible specialist, the IT department, the management of the organisation, the emergency manager.

1.3 Limitations

This module does not cover all aspects related to the detection of security incidents. Incident detection measures are presented in the module DER.1 Detection of security incidents. The initial forensic examination is addressed in module DER.2.2 Enabling computer forensics and the follow-up to the advanced persistent threat incident is addressed in module DER.2.3 Resolution of large-scale security incidents. Emergency response to an incident is covered in module DER.4 Emergency management.

2 Threats

2.1 Inadequate handling of security incidents

If security incidents are responded to inappropriately or not acted upon swiftly, an attacker may exploit the security vulnerability for an extended period of time. Wrong decisions in the handling of security incidents can cause extensive damage, including unnecessary damage to third parties. Examples of cases that indicate the inadequate handling of security incidents:

2.2 Destruction of evidence when dealing with a security incident

In the event of a security incident being handled carelessly, important evidence may be destroyed before the facts are established or before subsequent legal proceedings, or the data may lack sufficient probative value.

3 Measures

3.1 Life cycle

Planning

DER.2.1.M1	Defining a security incident
DER.2.1.M2	Guidelines for the handling of security incidents
DER.2.1.M3	Assignment of responsibilities and the appointment of contact persons
DER.2.1.M7	Methodology for the handling of security incidents

DER.2.1.M8 Working group for the handling of security incidents

DER.2.1.M9 Guidelines for the reporting of security incidents

DER.2.1.M11 Assessment of security incidents

DER.2.1.M14 Escalation plan for reporting security incidents

Operation

DER.2.1.M4 Procedure for the reporting of security incidents

DER.2.1.M5 Procedure for the resolution of security incidents

DER.2.1.M10 Limitation of the effects of security incidents

DER.2.1.M12 Combining security incident and IT incident handling

DER.2.1.M13 Integration of security and emergency management

DER.2.1.M15 Preparedness of IT employees to deal with security incidents

DER.2.1.M16 Documentation for the handling of security incidents

Emergency response

DER.2.1.M6 Restoration of the working environment following a security incident

Improvement

DER.2.1.M17 Follow-up actions of security incidents

DER.2.1.M18 Process improvement based on experience and external developments

Additional advanced measures

DER.2.1.M19 Priorities for the handling of security incidents

DER.2.1.M20 Security incident reporting centre of the organisation

DER.2.1.M21 Expert group for the handling of security incidents

DER.2.1.M22 Review of the organisation of the handling of security incidents

3.2 Key measures

DER.2.1.M1 Defining a security incident

a. The organisation determines which incidents are to be considered security incidents. A security incident is clearly distinguishable from an IT failure.

b. Employees involved in the handling of security incidents know the definition of a security incident.

c. The definition and handling of a security incident is based on the protection requirements of specific business processes, IT systems, and applications.

DER.2.1.M2 Guidelines for the handling of security incidents

a. Procedure guidelines have been established for the handling of security incidents. The scope to which the guidelines extend is defined in the guideline itself.
b. The guidelines contain practical and target group-specific instructions on what to do in the event of a security incident.
c. The guidelines are made known to all employees.
d. The guidelines for the handling of security incidents are reviewed and updated regularly.

DER.2.1.M3 Assignment of responsibilities and the appointment of contact persons

a. All employees are subject to the accountability and responsibility for handling security incidents.
b. All employees involved in security incidents have received appropriate training.
c. The organisation defines who can decide to initiate a forensic examination and on what basis.
d. Employees are aware of the contact persons for the different types of security incidents, and the relevant information is up to date and available to the employees.

DER.2.1.M4 Procedure for the reporting of security incidents [management of the organisation, IT department, data protection specialist, emergency manager]

a. In the event of a security incident, the organisation's internal and external parties are notified thereof immediately and in accordance with the guidelines for the handling of security incidents.
b. The decision of whether or not to involve a data protection specialist, a lawyer, or the management of the organisation is made separately for each incident.
c. If external authorities (CERT-EE, the police, the Data Protection Inspectorate) need to be notified of security incidents, this is done within the timeframe specified in the notification obligations, using secure communication channels.

DER.2.1.M5 Procedure for the resolution of security incidents [IT department]

a. The incident is resolved by isolating the affected components, documenting the incident, and identifying the cause.
b. If necessary, the organisation's internal or external specialists are involved in the resolution of the issues related to the different subject areas of the security incident. Secure channels of communication are established for this purpose.

c. The incident is resolved as quickly as possible to restore the normal situation prior to the incident (see DER.2.1.M6 Restoration of the working environment following a security incident).

DER.2.1.M6 Restoration of the working environment following a security incident [IT department]

a. In order to analyse the security incident, the affected devices are disconnected from the network.
b. The data needed to handle the incident is backed up for later analysis.
c. The affected device's operating system and all applications are checked and missing security patches and updates are installed to detect possible impacts and changes.
d. Data accuracy and integrity are verified during data restoration following the incident. When restoring backed-up data, it is ensured that it is not affected by the security incident.
e. All passwords used on the device are changed, a security test is performed, and the functionality of the component is verified with the user prior to the taking the affected devices back into use.
f. To detect new or recurring anomalies, the network traffic of the affected and restored devices is monitored after the work environment has been restored.

3.3 Standard measures

DER.2.1.M7 Methodology for the handling of security incidents [management of the organisation]

a. The guidelines for the handling of security incidents (see DER.2.1.M2 Guidelines for the handling of security incidents) document the methodology and the procedures for handling different types of security incidents.
b. The methodology for the handling of security incidents is approved by the management of the organisation and is communicated to the users.
c. The methodology for the handling of security incidents is regularly reviewed and updated.

DER.2.1.M8 Working group for the handling of security incidents

a. A working group is set up for the handling of security incidents, and its composition may be changed depending on the type of incident.
b. The members of the working group have a predefined specific role and tasks which they are prepared to perform as required.

c. The composition of the working group for the handling of security incidents is modified as necessary.

DER.2.1.M9 Guidelines for the reporting of security incidents

a. Guidelines are established for the reporting of incidents, which provide at least the following:

- the acceptable and appropriate communication channels for different types of incidents;

a list of persons to be definitely informed in case of an incident, and others to be informed if necessary;

- through whom, in what order, and with what accuracy the information is communicated;
- who communicates information relating to security incidents to third parties.

DER.2.1.M10 Limitation of the effects of security incidents [emergency manager, IT department]

a. In parallel with the analysis of the causes of the security incident, information is collected to assess the impact of the incident.
b. For the most likely incident scenarios, an action plan for the handling of incidents has been developed.

DER.2.1.M11 Assessment of security incidents [IT department]

a. A common procedure for the assessment and the categorisation of security incidents and other disruptions (for example, IT failures) is established for the security governance and incident management functions.

DER.2.1.M12 Combining security incident and IT incident handling [emergency manager]

a. The organisation has analysed the points of contact between security incidents and IT incidents and has defined the resources to be used for both types.
b. IT incident responders have been made aware of the differences in handling security incidents.
c. Security governance employees have read-only access to the IT incident management tool.

DER.2.1.M13 Integration of security and emergency management [emergency manager]

a. When a security incident has resulted in the initiation of an emergency management process, the emergency manager coordinates the incident resolution.
b. If necessary, additional specialists with specific skills are involved in resolving the incident.

DER.2.1.M14 Escalation plan for reporting security incidents [IT department]

a. In addition to the communication plan (see DER.2.1.M9 Guidelines for the reporting of security incidents), an escalation plan for reporting security incidents is established and coordinated with the information security manager.
b. The escalation plan for reporting security incidents includes instructions for who and in which cases should be further involved in the resolution of the incident.
c. The escalation plan is implemented through the selection of tools and communication channels that are also available in the event of an emergency and appropriate for sharing confidential information.
d. The escalation plan for reporting security incidents is tested regularly. The escalation plan is updated as necessary.

DER.2.1.M15 Preparedness of IT employees to deal with security incidents [IT department]

a. IT employees know the protection requirements of the systems they manage.
b. IT employees have the tools and checklists to detect security incidents.
c. IT employees are familiar with the guidelines for the handling of security incidents and have been trained in the use of the necessary tools.

DER.2.1.M16 Documentation for the handling of security incidents

a. Security incidents are documented according to a common standard procedure.
b. The documentation of the security incident records all actions taken during the handling process, including the time at which they were carried out, and the log data of the affected components is stored.
c. The security incident handling report is archived in a manner that ensures its integrity and confidentiality.

DER.2.1.M17 Follow-up actions of security incidents

a. The following is assessed after the handling of a security incident:

- how quickly the security incident was identified and resolved;
- whether the communication channels worked;
- whether there was sufficient data to conduct an impact assessment;
- whether the detection and response measures were effective.

b. The experience from previous security incidents is used to draw up an action plan for handling similar incidents. Changes to the action plan are communicated to the target groups.
c. The management is informed of the security incident that has occurred and the results of its handling.

DER.2.1.M18 Process improvement based on experience and external developments [responsible specialist]

a. To improve the handling of security incidents, the opinions of the persons involved in the resolution of security incidents and feedback from the persons responsible are sought.
b. Following changes in IT systems and incident management, incident detection and management tools and guidelines are updated.

3.4 Advanced measures

DER.2.1.M19 Priorities for the handling of security incidents [management of the organisation] (C-I-A)

a. The priorities for the handling of security incidents are determined based on the varying importance of the business processes.
b. Priorities for the handling of security incidents are set by the management of the organisation. On a similar basis, priorities are used also in IT incident management.
c. The decision-makers involved in the handling of security incidents recognise and apply the priorities, taking into account the initial assessment of the security incident (see DER.2.1.M11 Assessment of security incidents).

DER.2.1.M20 Security incident reporting centre of the organisation (C-I-A)

a. The organisation has established a security incident reporting centre.
b. The security incident reporting centre responds to incident reports during normal working hours without delay.

c. The employees of the security incident reporting centre receive adequate information security training.
d. All information related to security incidents is treated as confidential by the security incident reporting centre.

DER.2.1.M21 Expert group for the handling of security incidents (C-I-A)

a. A team of experienced and trusted employees is established to handle security incidents. The expert group is equipped with adequate technical and financial resources.
b. The members of the expert group are well prepared to analyse the organisation's systems. The members of the team are continuously updating their knowledge in the field of both deployed systems and the detection of and reaction to security incidents.
c. The reliability of the members of the expert group is verified, and the composition of the team is updated as necessary.
d. The members of the expert group are involved in incident escalation and communication channels.
e. The expert group is integrated into the incident management organisation (see DER.2.1.M8 Working group for the handling of security incidents), the responsibilities of the expert group are defined and coordinated (see DER.2.1.M3 Assignment of responsibilities and the appointment of contact persons).

DER.2.1.M22 Review of the organisation of the handling of security incidents (C-I-A)

a. The organisation for the handling of security incidents and the related measurable indicators (for example, security incident detection, incident reporting, and incident escalation) are regularly assessed.
b. The performance of the handling of security incidents is verified through both planned and unplanned reviews. The reviews are coordinated with the management in advance.
c. Practical experience is gained by practising incident handling with simulated security incidents.

DER.2.2 Enabling computer forensics

1 Description

1.1 Purpose

To propose measures to implement the measures of the forensic examination of an information security incident. This module will cover the stages of strategic preparation, initiation, evidence security, analysis, and presentation of the results of computer forensics.

1.2 Responsibility

The information security manager is responsible for the implementation of the measures for enabling computer forensics.
Additional responsible persons: The data protection specialist, the responsible specialist, the management of the organisation.

1.3 Limitations

This module does not include measures for attack detection (see DER.1 Detection of security incidents). It also does not explain the criteria and the processes for deciding whether or not a forensic examination is necessary - this will be done during the handling of a security incident (see DER.2.1 Handling of security incidents).
This module also does not cover information security forensic examinations carried out by law enforcement agencies in relation to offences.

2 Threats

2.1 Breach of the legal framework conditions

During a forensic examination, the personal data of customers, employees, or partners is copied and analysed. If personal data is used inappropriately, the organisation is in breach of legal requirements.

2.2 Loss of evidence due to lack of security

If no attention is paid to the security of evidence, and in particular to ensuring the authenticity of evidence, important evidence may be lost or lose its evidential value. Temporary files created during an incident may contain information relevant to the examination. Unless it is stored in another location in a timely manner, this data cannot be used in a forensic examination. If computer forensic tools are used inappropriately, the tools will not serve their purpose.

3 Measures

3.1 Life cycle

Operation

DER.2.2.M1	Compliance with legal framework conditions for data processing
DER.2.2.M8	The correct selection and sequencing of evidence
DER.2.2.M9	The correct selection of data to be analysed
DER.2.2.M10	Computer forensics evidence security
DER.2.2.M11	Documentation of evidence security
DER.2.2.M12	Secure storage of original data media and evidence

Planning

DER.2.2.M2	First response guidelines to an information security incident
DER.2.2.M3	Mapping forensic service providers
DER.2.2.M4	Linking forensic examinations to crisis and incident management
DER.2.2.M5	Guidelines for the security of evidence in the event of an information security incident

Implementation

DER.2.2.M6	Training employees in the field of computer forensics
DER.2.2.M7	The correct selection of computer forensic working tools

Additional advanced measures

DER.2.2.M13	Framework contracts with forensic service providers
DER.2.2.M14	Standard procedures for evidence security
DER.2.2.M15	Evidence security training

3.2 Key measures

DER.2.2.M1 Compliance with legal framework conditions for data processing [data protection specialist, management of the organisation]

a. The collection and analysis of data for the forensic examination is carried out within the limits allowed by the legislation (see ORP.5 Compliance management (requirements management)).
b. Data processing is coordinated with the data protection specialist. Data processing does not violate the organisation's internal regulations and personnel agreements.
c. In the event of a conflict of interest between the organisation and an employee, consideration is given to removing the employee from the process.

DER.2.2.M2 First response guidelines to an information security incident

a. Actions following an information security incident are carried out in the IT systems affected by the incident without disturbing the traces of the incident.
b. The first response guidelines describe how to avoid the destruction of evidence in the IT systems used.

3.3 Standard measures

DER.2.2.M3 Mapping forensic service providers

a. In the absence of in-house computer forensic capabilities, suitable forensic service providers are mapped.
b. The contact details of forensic service providers are provided in the first response guidelines.

DER.2.2.M4 Linking forensic examinations to crisis and incident management

a. The interface between the forensic examination of information security incidents and crisis and incident management is documented in the information security concept.
b. Cross-sectoral communication channels and responsible persons are appointed, contact persons are available if necessary.

DER.2.2.M5 Guidelines for the security of evidence in the event of an information security incident

a. Guidelines for the security of evidence are developed, which include methods, technical tools, legal framework conditions, and documentation requirements to ensure the evidentiary value of evidence.

DER.2.2.M6 Training employees in the field of computer forensics

a. Training is provided for the use of computer forensic working tools and to ensure the security of the collected evidence.

DER.2.2.M7 The correct selection of computer forensic working tools

a. Appropriate working tools are available for the analysis of evidence and traces.
b. Before using a computer forensic working tool, it is ensured that it is in working order and has not been tampered with. The results of the inspection are documented.

DER.2.2.M8 The correct selection and sequencing of evidence [responsible specialist]

a. The forensic examination is targeted as precisely as possible. Data sources are selected in accordance with the objective.
b. An action plan is drawn up for the collection and security of evidence. The sequencing of activities is based on the volatility of the evidence. Data sources with persistent content, such as the contents of hard drives and back-ups, can be dealt with at a later stage.

DER.2.2.M9 The correct selection of data to be analysed [responsible specialist]

a. The legal framework conditions determine which secondary data (for example, log data or network traffic) can be considered evidence, how they can be processed, and for how long they can be retained.

DER.2.2.M10 Computer forensics evidence security [responsible specialist]

a. Where possible, evidence-based data media are cloned in their entirety. If a forensic image cannot be made, a method is chosen to change the data as little as possible.
b. The original data media are kept sealed to ensure data integrity.
c. Where cryptographic verification codes are used to retroactively verify the integrity of the original data or examination copies, multiple copies of the verification codes are made. The copies are stored separately from the data media in a documented and secure manner.
d. To ensure the legality of the data, the operations carried out on the data media and the correctness of the verification codes are verified by independent witnesses.
e. Only suitably trained employees (see DER.2.2.M6 Training employees in the field of computer forensics) or a forensic service provider (see also DER.2.2.M3 Selection of the forensic service provider) are used to provide evidence for forensic examination.

DER.2.2.M11 Documentation of evidence security [responsible specialist]

a. The forensic examination documents all steps taken, the methods used, the reasons for use, and the persons responsible for carrying them out.

b. The documentation will provide comprehensive ex-post proof of how the original evidence was stored and used.

DER.2.2.M12 Secure storage of original data media and evidence [responsible specialist]

a. Original data media are stored in such a way that access to the data media is restricted to those persons involved in the examination who are known by name.
b. There is a time limit for the retention of original data media and evidence.
c. Upon the expiry of the time limit, the need for further retention of the data media and evidence is assessed. If there is no need for further retention, the evidence is destroyed or securely erased, and the original data media are returned to the owner.

3.4 Advanced measures

DER.2.2.M13 Framework contracts with forensic service providers (C-I-A)

a. In order to speed up the initiation of the forensic examination of information security incidents, the organisation has signed engagement contracts or framework agreements with forensic service providers.

DER.2.2.M14 Standard procedures for evidence security (C-I-A)

a. Standard operating procedures compliant with forensic requirements are established for the comprehensive storage of applications, IT systems, and common system configurations with high protection requirements.
- The procedures take into account both volatile and less volatile data.

b. The implementation of the developed standard procedures is automated and pre-tested. The procedures are supported by checklists and assistive technology.

DER.2.2.M15 Evidence security training (C-I-A)

a. Employees involved in a forensic examination and analysis regularly practise the implementation of evidence security for information security incidents.

DER.2.3 Resolution of large-scale security incidents

1 Description

1.1 Purpose

To propose measures to resolve large-scale security incidents.
In this module, an advanced persistent threat is considered an example of a large-scale security incident. This module describes how to restore IT systems to a normal and secure working status in an organisation in the event of an Advanced Persistent Threat (APT).

1.2 Responsibility

The IT department is responsible for the implementation of the measures of the module 'Resolution of large-scale security incidents'.
Additional responsible persons: The information security manager.

1.3 Limitations

This module focuses on cyber incidents - it does not cover the response to large-scale physical attacks or corruption incidents. This module covers the handling of advanced persistent threat incidents, while general security incident management is covered in modules DER.1 Detection of security incidents and DER.2.1 Handling of security incidents.
This module does not cover the detection of advanced persistent threat intrusion traces by means of indicators of compromise and the detection of backdoors.

2 Threats

2.1 Lack of solutions

An attacker will use all means to make the access to an IT system permanent during an advanced persistent threat. It is very difficult to detect hardware components and fixed assets manipulated by the attacker. There is a risk that the incident response will not be able to identify all entry points and completely remove malwares from the IT systems. As a result, the attacker may be able to gain access to IT systems again at a later stage.

2.2 Destruction of traces

Following an advanced persistent threat incident, IT systems are often reinstalled or decommissioned. Unless an analysable copy of the operating system or the fixed assets is made in advance, evidence necessary for further investigation or legal proceedings may be destroyed.

2.3 Premature alerting of an attacker

Prior to the active response to an advanced persistent threat incident, the attack is usually analysed to identify the routes of approach, entry points, and means used. At this stage, if the attacker realises that they have been detected, they may remove their traces or quickly attempt to attack other IT systems. The attacker may also temporarily suspend their activities and create a backdoor to continue the attack in the future.

2.4 Data loss and IT system failure

Responding to an advanced persistent threat incident generally involves reinstalling IT systems and isolating the network segments currently in use. Shutting down IT systems will affect service availability. If the incident takes a long time to be resolved, it can cause significant damage.

2.5 Failure to modify network information after an advanced persistent threat

During an advanced persistent threat, the attacker acquires detailed knowledge of the structure and configurations of the target environment. For example, they may have knowledge of existing network segments, IT system naming schemes, user and service accounts, deployed software, and services. With this knowledge, the same attacker can, if the opportunity arises, re-establish access to and re-infect the target environment after the incident has been resolved.

3 Measures

3.1 Life cycle

Planning and initiation

DER.2.3.M1 Establishing an executive leadership team

DER.2.3.M2 Choosing a resolution strategy

Operation

DER.2.3.M3 Isolation of the affected network elements

DER.2.3.M4 Blocking and modifying access data and encryption keys

DER.2.3.M5 Closing the original intrusion route

DER.2.3.M6 Restoration to working status

DER.2.3.M9 Replacement of the affected IT systems

Improvement

DER.2.3.M7 Targeted reinforcement of the IT system

Acquisition

DER.2.3.M8 Securing communication channels for attack management

Additional advanced measures

DER.2.3.M10 Reconfiguration to prevent a new attack by the same attacker

3.2 Key measures

DER.2.3.M1 Establishing an executive leadership team

a. To resolve an advanced persistent threat (APT) incident, an executive leadership team is set up to plan, coordinate, and monitor the necessary actions. The executive leadership team has the authority and decision-making power to carry out its tasks.
b. If a specialised forensic service provider is used to analyse an advanced persistent threat incident, its experts are also involved in the incident resolution.
c. If the IT systems have been significantly compromised or if the resolution action is very extensive, a business continuity and communications crisis unit is established alongside the executive leadership team. Once the crisis unit has been established, it is the responsibility of the executive leadership team to implement the resolution actions and report the results to the crisis unit.

DER.2.3.M2 Choosing a resolution strategy

a. To resolve an advanced persistent threat incident, the executive leadership team draws up a resolution strategy, deciding whether:

- the malware can be removed from the compromised IT systems;
- the IT systems are reinstalled;
- the IT systems must be completely replaced.

b. During the observation phase, indicators of compromise are collected and investigated in a way that is undetectable to the attacker.
c. In the localisation phase, the compromised part of the system or network is isolated from the others (see DER.2.3.M3 Isolation of the affected network elements) and forensic examination is

performed to provide decision information.
d. Based on the results of the analysis, a decision is made on the manner and timing of the recovery of each affected system.
e. When IT systems are reinstalled, it is verified that no corrupted data or software components are restored from freshly made backups.
f. If the organisation decides not to reinstall the IT systems, a dedicated advanced persistent threat resolution procedure is triggered.
g. After the advanced persistent threat incident has been resolved, data exchanges between the affected IT systems are monitored to detect attempts to connect to the attacker.

DER.2.3.M3 Isolation of the affected network elements

a. The network elements affected by the incident are identified as a result of the forensic examination.
b. The network elements affected by the advanced persistent threat are isolated. If it is not possible to precisely identify the affected network elements, the suspicious and possibly infected network sections are also isolated.
c. The affected network elements are isolated simultaneously to impede an attack.
d. When network elements are isolated, Internet connections from subnetworks are disconnected.

DER.2.3.M4 Blocking and modifying access data and encryption keys

a. After the isolation of a compromised system and/or network element, all access data, including maintenance account data and centrally managed data (for example, Active Directory or LDAP), is replaced.
b. If a central authentication server (domain controller or LDAP server) is also affected by the attack, accesses from it are blocked and all passwords are changed. This will be done by experienced system administrators, with the assistance of forensic specialists if necessary.
c. If the advanced persistent threat has compromised TLS keys or the internal certification authority, the corresponding keys are securely blocked and the keys and their infrastructure are re-created.

DER.2.3.M5 Closing the original intrusion route

a. If the forensic examination identifies that an attacker gained access to an organisation's network due to a technical weakness, the weakness is removed after the network element has been isolated.

Anti-virus, authentication, firewall rules, email filtering, etc. are improved.
b. Patching and upgrades are used to eliminate software vulnerabilities. In the case of a zero-day exploit, the software vendor is contacted and temporary measures are implemented to compensate for the vulnerability until a solution is found.
c. If an attacker managed to compromise IT systems by exploiting a human error, organisational, technical, and personnel measures are implemented to prevent a recurrence of such incidents. Insecure configurations or passwords are replaced.

DER.2.3.M6 Restoration to working status

a. After an effective network clean-up, the IT systems are restored to an appropriate working status. Data exchange between systems already restored and those not restored is avoided. The restored systems are monitored to detect possible attacks.
b. At the end of the monitoring period, temporary monitoring and analysis tools are discontinued or put into regular use.
c. Evidence and disposed IT components are either destroyed, securely deleted, or archived in an appropriate manner.

3.3 Standard measures

DER.2.3.M7 Targeted reinforcement of the IT system

a. Following an advanced persistent threat, the IT systems affected by the incident are strengthened, based on the results of the forensic examination (see DER.2.2. Enabling computer forensics). Afterwards, the security of the IT systems is re-checked.
b. Reinforcement of the IT system is initiated as soon as possible, already at the time of the IT system clean-up. The implementation of the more urgent measures is planned with a later implementation deadline.
c. The information security manager is responsible for the preparation of the reinforcement plan and the implementation of the measures.

DER.2.3.M8 Securing communication channels for attack management

a. The executive leadership team and the persons involved in the resolution use secure communication channels (for example, mobile phone, social networking, face-to-face meetings) whose traffic cannot be monitored by the attacker.

DER.2.3.M9 Replacement of the affected IT systems (C-I-A)

a. In the case of IT systems with high protection requirements, the hardware is completely replaced after an advanced persistent threat incident.
b. If suspicious behaviour (for example, unwarranted network traffic) is still detected in individual IT systems after the advanced persistent threat incident has been resolved, the affected IT system is replaced.

3.4 Advanced measures

DER.2.3.M10 Reconfiguration to prevent a new attack by the same attacker (C-I)

a. In order to prevent a new advanced persistent threat by the same attacker, the internal architecture of the network environment is reconfigured by modifying:

- the IP address ranges of the network segments and the IP addresses of the IT systems;
- the IT system names;
- the naming schemes for user and maintenance accounts;
- the URLs for web applications and web services.

b. Following the network reconfiguration, the documentation is updated and users are informed.
c. Mechanisms are put in place to detect the recurrence of an attack and to monitor whether new accesses are being made based on former network data. Depending on the details of the attack, the monitoring mechanism is upgraded.

DER.3 Assessment of information security

DER.3.1 Audits and reviews

1 Description

1.1 Purpose

To provide general guidance for conducting information security audits and reviews with the aim of improving the organisation's information security, avoiding undesirable trends in the field, and optimising security measures and processes. Unlike audits, reviews do not require the reviewer to be

independent of the audit subject and may also be involved in the implementation of recommendations made on the basis of the findings.

1.2 Responsibility

The information security manager is responsible for the implementation of the measures of the module 'Audits and reviews'.
Additional responsible persons: The management of the organisation, the audit team, the information security review team.

1.3 Limitations

The measures in this module are implemented as generic measures for both internal audits and outsourced audits. This module does not address how audits and reviews can be integrated into an organisation's internal control system.
This module does not apply to certification audits. The conduct of certification and statutory audits required by legislation is covered in module DER.3.2 Information security compliance audits.

2 Threats

2.1 Inadequate or unplanned implementation of security measures

An organisation's ability to deal with information security threats is reduced if security measures are not implemented in a systematic and comprehensive manner. It may also happen that after a temporary restriction of security measures (for example, at a certain stage of a development project), the security situation is not restored because it is forgotten.

2.2 Ineffective or uneconomic implementation of security measures

If security measures are only partially implemented, or if best practices are not taken into account, the implemented measures may prove to be ineffective (for example, securing the main door if the same is not done for the side door). There may also be individual measures that are economically impractical considering the potential risk.

2.3 Inadequate implementation of the information security management system

The involvement of an independent third party in the assessment of the functioning of the information security management system is often overlooked. If the information security manager personally reviews the implementation of security measures, the result may not be objective. As a result, the information security management system may not function effectively in practice.

2.4 Insufficient qualification of the auditor

If the auditor lacks adequate qualifications or is inadequately prepared, they may misjudge the level of maturity of the organisation's information security. As a result, unnecessary or inappropriate suggestions for improvement may end up in the report. This results in uneconomic costs for information security or an underestimation of the protection requirements, leaving significant risks unmitigated.

2.5 Lack of medium-term planning

If audits are not planned centrally and in advance, some areas may be audited very frequently and others not at all. This makes it very difficult to assess the actual information security situation.

2.6 Lack of audit planning and coordination

If the audit plan has not been coordinated with all the relevant employees in the organisation, key personnel may be absent during the audit procedures. If the auditor has set too tight a timetable for checking specific areas, the inspections may be too superficial.

2.7 Uncoordinated use of personal data

During the course of an audit, the auditors may gain access to personal data or draw conclusions about the performance of individual employees. Without the coordination of the data protection specialist and/or the human resources representative, the processing of personal data may result in a breach of the employee's rights.

2.8 Deliberate concealment of security problems

Employees may conceal security problems for fear that an audit will uncover errors or omissions that will cast them in a negative light. As a result, an inaccurate overview of the current state of information security may be created.

3 Measures

3.1 Life cycle

Planning and initiation

DER.3.1.M1	Appointment of the responsible person
DER.3.1.M5	Integration into the information security process
DER.3.1.M6	Establishment of a control basis and a common evaluation system
DER.3.1.M7	Audit programme
DER.3.1.M8	List of the objects of the review
DER.3.1.M11	Procedures for the exchange of information and the conduct of inspections

Operation

DER.3.1.M2	Preparing the audit
DER.3.1.M3	Conducting the audit
DER.3.1.M4	Performing an information security review
DER.3.1.M9	Suitable audit or review team
DER.3.1.M10	Preparing an audit or review plan
DER.3.1.M12	Audit opening meeting
DER.3.1.M13	Review and inspection of documents
DER.3.1.M14	Random inspections
DER.3.1.M15	Suitable control methods
DER.3.1.M16	Action plan for on-site inspections
DER.3.1.M17	Procedure for on-site inspections
DER.3.1.M18	Conducting interviews
DER.3.1.M19	Review of the risk management plan
DER.3.1.M20	Final meeting
DER.3.1.M21	Assessment of the results
DER.3.1.M22	Audit report
DER.3.1.M23	Documentation of the results of the review
DER.3.1.M24	Completion of the audit or the review
DER.3.1.M25	Follow-up actions and follow-up inspection
DER.3.1.M26	Monitoring and adjustment of the audit plan
DER.3.1.M27	Retention and archiving of audit and review documentation

Additional advanced measures

DER.3.1.M28 Auditors' security clearance

3.2 Key measures

DER.3.1.M1 Appointment of the responsible person [management of the organisation]

a. The management of the organisation appoints a person responsible for planning and initiating audits. It is ensured that there is no conflict of interest (for example, auditing one's own department).
b. The person responsible ensures that the results of the audit are handled in accordance with the procedures established within the organisation.

DER.3.1.M2 Preparing the audit

a. The scope and objectives of the audit are agreed and documented during the planning of the audit.
b. Relevant employees are informed before the audit is initiated. In addition, the human resources representative is informed of the audit concerning employees.

DER.3.1.M3 Conducting the audit [audit team]

a. The audit verifies the compliance with the security measures related to the objectives of the audit. The related requirements are known to the audited organisation and the auditees.
b. The audit includes document review, testing, and on-site inspections.
c. During the on-site inspections, the auditors do not intervene independently in the operation of the IT systems or give direct instructions to modify the inspection object.
d. The audit results are documented and formalised in a written audit report.
e. The audit report is submitted to the appointed contact person by the agreed deadline.

DER.3.1.M4 Performing an information security review [information security review team]

a. The review verifies that the measures under review are implemented in a comprehensive, appropriate, and up-to-date manner.
b. Any discrepancies identified are resolved without delay wherever possible.
c. The results of the review are documented. Changes to the results are identifiable and personalisable.

3.3 Standard measures

DER.3.1.M5 Integration into the information security process

a. Regular audits are considered a part of an organisation's information security management system and security process. Audits are initiated on this basis.
b. The results of the audits are used to improve the information security management system.
c. The results of the audits and the actions taken to eliminate the deficiencies and improve the quality are presented in a regular report by the information security manager to the management of the organisation.

DER.3.1.M6 Establishment of a control basis and a common evaluation system

a. An inspection framework based on common grounds for conducting audits and reviews is established.
b. A common evaluation system for assessing the implementation of the measures is established and documented.

DER.3.1.M7 Audit programme

a. The organisation establishes a multi-annual audit and review programme.
b. The audit programme formulates control objectives derived from the objectives of the organisation and information security.
c. A contingency reserve is included in the annual resource planning to allow for changes to the audit programme as necessary.
d. The audit programme is adjusted in accordance with changing risk assessments.

DER.3.1.M8 List of the objects of the review

a. Review programming lists are established to document the current status and the planned reviews of the inspection objects.

DER.3.1.M9 Suitable audit or review team [audit team, information security review team]

a. For each audit or review, a team of suitable members is established, chaired by the audit or review manager responsible for conducting the audit or the review.
b. The composition of the audit or review team is determined on the basis of the area of inspection, taking into account the competency requirements of the area of inspection, the scope of the audit or

review, and the location of the inspection objects.
c. The members of the audit or review team are suitably qualified and neutral and independent of the auditee.
d. Where an external service provider is used as the auditor or reviewer, its independence is verified in advance and the obligation of confidentiality applies.
e. Adequate resources are provided to the audit or review team.

DER.3.1.M10 Preparing an audit or review plan [audit team, information security review team]

a. Prior to the commencement of the audit, the audit manager prepares an audit plan to be used as the basis for conducting the audit.
b. Prior to the commencement of the review, the review manager prepares a review plan to be used as the basis for conducting the review.
c. The audit plan or review plan is adjusted as necessary. In the case of an audit, the audit plan forms part of the final audit report.
d. Minor reviews are planned on the basis of a list of review objects.

DER.3.1.M11 Procedures for the exchange of information and the conduct of inspections [audit team, information security review team]

a. There are established procedures for the exchange of information between the audit team and the employees of the organisation or the department.
b. Appropriate measures are implemented to protect the confidentiality and the integrity of the information communicated during the audit.
c. The persons involved in the audit must not influence the audit procedures.
d. The persons involved in the audit are subject to the obligation of confidentiality.

DER.3.1.M12 Audit opening meeting [audit team]

a. An opening meeting is held with the audit team and the persons concerned to explain the audit or review procedures.
b. During the opening meeting, the terms and conditions of the on-site inspection are coordinated and the audit plan is approved by the responsible persons.

DER.3.1.M13 Review and inspection of documents [audit team, information security review team]

a. Documents are reviewed in accordance with the procedures set out in the inspection framework.
b. The document review verifies that documents are up to date, complete, and understandable.
c. The results of the document review are documented. The results are taken into account when carrying out on-site inspections.

DER.3.1.M14 Random inspections [audit team, information security review team]

a. Random inspections as part of the on-site inspections are selected on a risk basis, documented, and justified.
b. Where random inspections are carried out on the basis of standard target objects and module-based measures, the target objects and measures to be checked are selected in accordance with a predefined procedure.
c. The results of previous audits and reviews are taken into account in the selection of random inspections.

DER.3.1.M15 Suitable control methods [audit team, information security review team]

a. The audit team or information security review team uses inspection methods appropriate to the objectives of the audit or review, such as interviewing (see DER.3.1.M18 Conducting interviews) or document review (see DER.3.1.M13 Review and inspection of documents).
b. The inspection procedures carried out are effective and fit for purpose.

DER.3.1.M16 Action plan for on-site inspections [audit team]

a. The audit team develops an action plan for the on-site inspection together with the auditee's contact persons.
b. The action plan for the on-site inspection is documented in the audit plan.

DER.3.1.M17 Procedure for on-site inspections [audit team, information security review team]

a. At the beginning of the on-site inspection, an opening meeting is organised with the responsible persons of the organisation.
b. The requirements set out in the audit plan are verified in accordance with the established

inspection methods.
c. If the selected objects for the random inspection differ from its documented status, the inspection is extended until the circumstances of the difference have been clarified.
d. After the audit procedures have been carried out, the audit team organises a final meeting, during which a brief and unbiased presentation of the results and further actions are made. Minutes are taken of the final meeting of the on-site inspection.

DER.3.1.M18 Conducting interviews [audit team]

a. The conducted interviews are appropriately structured. The questions asked are concise, precise, and clearly formulated.
b. The interview methodology is appropriate to the objectives of the inspection and the target group.

DER.3.1.M19 Review of the risk management plan [audit team]

a. The audit team assesses whether the residual risks are adequate and accepted by the management. Non-implementation of key measures essential to ensure information security are not accepted.
b. The auditor verifies on a random basis whether and to what extent the measures foreseen in the risk management plan have been implemented.

DER.3.1.M20 Final meeting [audit team]

a. The audit team organises a final meeting with the relevant responsible persons of the audited organisation at the conclusion of the audit.
b. At the final meeting, the preliminary audit findings are presented and further actions are outlined.

DER.3.1.M21 Assessment of the results [audit team]

a. After the audit procedures have been carried out, the audit team collates and analyses the data collected.
b. If necessary, additional evidence material is sought from the auditee. The auditee is given sufficient time to gather evidence material. Documents not submitted by the agreed deadline are considered missing.
c. The audit team provides a final assessment of the implementation of the audited measures after the analysis of the additional evidence material.

DER.3.1.M22 Audit report [audit team]

a. The audit team documents the results of the audit in a clear and comprehensive manner and presents them in an audit report. The audit team is ready to clarify the audit findings if necessary.
b. The audited organisation ensures that relevant extracts from the audit report are made available to the relevant persons within a reasonable time.

DER.3.1.M23 Documentation of the results of the review [information security review team]

a. The results of the review are documented in a consistent, pre-agreed format.

DER.3.1.M24 Completion of the audit or the review [audit team, information security review team]

a. Following an audit or a review, the relevant documents, data media, or other material provided to the auditor in coordination with the audited organisation that are not subject to the applicable legal or other binding document retention requirements are returned or destroyed.
b. The information security manager arranges for the deactivation or revocation of any access rights that have been temporarily created for the members of the audit or review team.
c. Rights and restrictions on the disclosure of results are agreed with auditors and reviewers, including that audit results are not disclosed to other organisations without the consent of the audited organisation.

DER.3.1.M25 Follow-up actions and follow-up inspection

a. Any deficiencies reported in the audit report or identified during the review are corrected within a reasonable time.
b. The planned times for the implementation of corrective measures and the responsible persons are documented.
c. Corrective measures implemented are documented in accordance with the procedures established by the information security management system.
d. In the event of significant deficiencies, the audit or review team conducts a follow-up audit or follow-up inspection of the implementation of corrective measures.

DER.3.1.M26 Monitoring and adjustment of the audit plan

a. The audit programme can be adjusted on an ongoing basis to ensure the timing, objectives, content, and quality of the audit.
b. The scope and the results of the audits carried out are taken into account when modifying the audit programme.

DER.3.1.M27 Retention and archiving of audit and review documentation

a. The audit programme, the audit plans, and the audit and review documentation are retained in accordance with the requirements of the legislation or the internal regulations.
b. Documents are stored securely. Documents are protected against alteration and unauthorised access during their retention period.
c. It is ensured that only authorised persons have access to the audit reports.
d. After the expiry of the archiving period, the relevant documentation is securely destroyed.

3.4 Advanced measures

DER.3.1.M28 Auditors' security clearance (C-I)

a. Where auditors may have access to highly sensitive information during the course of the audit, evidence of the integrity and reputation of the auditors is obtained in advance.
b. If it is necessary for the auditors to have access to information classified as state secrets, they are granted such access in accordance with the procedures established by the state secrets legislation.

DER.3.2 Information security compliance audits

1 Description

1.1 Purpose

To provide guidance to the audited organisation on how to conduct information security compliance audits. The purpose of an information security compliance audit is to ensure compliance with the legislation and the organisation's internal information security policy, to improve the organisation's information security, and to optimise security measures and security processes.

1.2 Responsibility

The information security manager is responsible for the compliance with the measures of the module 'Information security compliance audits' measures.
Additional responsible persons: The management of the organisation, the audit team.

1.3 Limitations

This module takes into account the requirements for conducting compliance audits based on the Estonian Information Security Standard (E-ITS); therefore, not all sub-measures may be relevant for other compliance audits.
This module is not sufficient for conducting independent certification audits (for example, the ISO 27001 certification audit).

2 Threats

2.1 Non-compliance with external security guidelines

Compliance requirements of information security management systems may come not only from the information security standard, but also from sectoral regulations. Regular information security inspections with information security compliance audits may be required by supervising authorities and the organisation's partners. Failure to conduct an audit may result in reputational damage, contract termination, or financial penalties for the organisation.

2.2 Inadequate or unplanned implementation of security measures

An organisation's ability to deal with information security threats is reduced if security measures are not implemented in a systematic and comprehensive manner. It may also happen that after a temporary restriction of security measures (for example, at a certain stage of a development project), the security situation is not restored because it is forgotten.

2.3 Ineffective or uneconomic implementation of security measures

If security measures are only partially implemented, or if best practices are not taken into account, the implemented measures may prove to be ineffective (for example, securing the main door if the same is not done for the side door). There may also be individual measures that are economically impractical considering the potential risk.

2.4 Inadequate implementation of the information security management system

The involvement of an independent third party in the assessment of the functioning of the information security management system is often overlooked. If the information security manager personally reviews the implementation of security measures, the result may not be objective. As a result, the information security management system may not function effectively in practice.

2.5 Insufficient qualification of the auditor

If the auditor lacks adequate qualifications or is inadequately prepared, they may misjudge the level of maturity of the organisation's information security. As a result, unnecessary or inappropriate suggestions for improvement may end up in the report. This results in uneconomic costs for information security or an underestimation of the protection requirements, leaving significant risks unmitigated.

2.6 Conflict of interest within an internal audit team

Where an organisation has formed an audit team of its own employees, the auditors may not be fully independent. If the members of the audit team are frequently exposed to the audited processes in their daily work, the audit result will not be unbiased.

2.7 Lack of medium-term planning

If audits are not planned centrally and in advance, some areas may be audited very frequently and others not at all. This makes it very difficult to assess the actual information security situation.

2.8 Lack of audit planning and coordination

If the audit plan has not been coordinated with all the relevant employees in the organisation, key personnel may be absent during the audit procedures.

2.9 Lack of coordination with human resources representation

During the course of an audit, the auditors may gain access to personal data or draw conclusions about the performance of individual employees. Without the coordination of the human resources representative, this may result in a breach of the employee's rights.

2.10 Deliberate concealment of discrepancies and problems

Employees may conceal security problems for fear that an audit will uncover errors or omissions that will cast them in a negative light. As a result, an inaccurate overview of the current state of information security may be created.

2.11 Leakage of information that requires protection

During the course of an information security audit, auditors have access to confidential information, as well as information on vulnerabilities and attack opportunities. If these facts become known to unauthorised persons, the information could be used to attack or defame the organisation.

3 Measures

3.1 Life cycle

Planning

DER.3.2.M1	Appointment of the person responsible for information security audits
DER.3.2.M2	Guidelines for conducting audits
DER.3.2.M3	Determination of the basis for the inspection
DER.3.2.M4	Planning information security compliance audits
DER.3.2.M9	Integration of information security audits into the information security process
DER.3.2.M10	Exchange of information

Operation

DER.3.2.M6	Preparation of the information security audit
DER.3.2.M8	Retention of audit reports
DER.3.2.M22	Information security audit follow-up actions

3.2 Key measures

DER.3.2.M1 Appointment of the person responsible for information security audits [management of the organisation]

a. The organisation appoints a person responsible for the information security audit who plans and commences the audit and elaborates its results.

DER.3.2.M2 Guidelines for conducting audits

a. The organisation has guidelines for conducting audits, approved by the management, which set out the objectives of the audit, compliance requirements, and information on the commissioning, organisation, and resources of the audit.
b. The guidelines for conducting audits set out the requirements for the submission and the retention of audit documentation and audit results.

DER.3.2.M3 Determination of the basis for the inspection

a. Unless otherwise specified in legislation, the applicable information security standard and the directory of information security measures that forms part of it is taken as the basis for the inspection of an information security compliance audit.
b. The basic and standard measures of the directory of measures are used as the basis for the inspection. If the organisation implements advanced measures as a result of the protection requirements, the implementation of the advanced measures is also audited.
c. All parties concerned are informed in advance of the basis for the inspection.

DER.3.2.M4 Planning information security compliance audits

a. An audit covering the entire scope and all the measures to be implemented is carried out periodically.
b. Following significant changes in the information security information network or in the IT systems, an additional interim audit is carried out on the elements affected by the changes.
c. The head of the audit team draws up an audit programme covering the entire audit cycle, on the basis of which the annual plan for information security audits is specified and approved each year.

DER.3.2.M6 Preparation of the information security audit [audit team]

a. The information security audit is initiated by the management of the organisation.
b. The organisation provides the audit team with the information security concept, the information security policy, the policies related to the object of the audit, and any other documents requested by the audit team.

DER.3.2.M8 Retention of audit reports

a. Unless a longer retention period is required by other legislation or regulations, the information security audit report and the supporting documents are retained securely for at least nine years.

b. Information security audit reports and the related supporting documents are protected against modification. Access to them is restricted to authorised persons.

3.3 Standard measures

DER.3.2.M9 Integration of information security audits into the information security process

a. Periodic information security compliance audits are part of the organisation's information security concept.
b. The results of information security compliance audits are used to improve the information security management system.
c. The results of the audits and the actions taken to eliminate the deficiencies and improve the quality are presented in a regular report by the information security manager to the management of the organisation.

DER.3.2.M10 Exchange of information

a. The acceptable means of communication between the audit team and the organisation are defined in the guidelines for conducting audits (see DER.3.2.M2 Guidelines for conducting audits).
b. The parties ensure the confidentiality and integrity of audit communications.

DER.3.2.M22 Information security audit follow-up actions

a. Discrepancies in the information security audit report are resolved within a reasonable time.
b. The responsible persons for the implementation of corrective measures and the current state for the implementation of the deadlines are documented.
c. The implementation of corrective measures is continuously monitored, and the status of the implementation is updated as necessary.
d. Based on the implementation of the corrective measures, the need for an additional information security follow-up audit is decided, in which case the audit programme is adjusted.

3.4 Advanced measures

There are no advanced measures in this module.

DER.4 Emergency management

1 Description

1.1 Purpose

To provide measures to ensure information security and continuity management in emergency situations.

1.2 Responsibility

The emergency manager is responsible for the implementation of the emergency management measures.
Additional responsible persons: The information security manager, the management of the organisation, the human resources department, the manager.

1.3 Limitations

This module does not provide the criteria for triggering an emergency management - the relevant decision is made during the handling of the security incident (see DER.2.1 Handling of security incidents). Emergencies are dealt with in a separate emergency management framework, which only has points of contact with this module (for example, in the context of further extension of emergency situations).

2 Threats

2.1 Personnel drop-out

Personnel drop-out in general (for example, due to epidemics or strikes) or the departure of key personnel can severely disrupt business processes in the organisation. Information needed to run business processes or restore IT systems may not be available.

2.2 IT system failure

The outage of an IT system caused by the failure of an IT system component (for example, a hardware component) adversely affects the operation of business processes that depend on the IT system.

2.3 Wide Area Network (WAN) failure

Wide Area Network (WAN) failures affect business processes that require continuous Internet access. Prolonged WAN outages can lead to major communication and availability problems across an entire region.

2.4 Building-related emergencies

Exceptional and unforeseen circumstances (for example, fires, storms, floods, explosions) may result in the partial or total destruction of buildings. In the event of a building-related emergency, the building can no longer be accessed and the business process is disrupted.

2.5 Interruption of the service by the supplier or the service provider

Where the business process is dependent on one or more service providers, a partial or total interruption of the service from a supplier or a service provider can have a significant impact on the business continuity of the organisation.

3 Measures

3.1 Life cycle

Planning and initiation

DER.4.M1 Emergency guide

DER.4.M2 Integration of emergency management into inter-organisational processes

Additional advanced measures

DER.4.M3 Scope and strategy of emergency management

DER.4.M4 Emergency management policy and management responsibility

DER.4.M5 Organisation of emergency management

DER.4.M6 Availability of the necessary resources

DER.4.M7 Emergency concept

DER.4.M8 Involvement of employees in the emergency management process

DER.4.M9 Integration of emergency management into inter-organisational processes

DER.4.M10 Tests and emergency trainings

DER.4.M12 Documentation of the emergency management process

DER.4.M13	Review and control of the emergency management system
DER.4.M14	Regular overview and improvement of emergency measures
DER.4.M15	Evaluation of the performance of the emergency management system
DER.4.M16	Emergency response of outsourced components

3.2 Key measures

3.3 Standard measures

DER.4.M1 Emergency guide

a. The organisation has prepared an emergency guide containing instructions for action in the event of an emergency, which include at least:

- the roles involved, the rights and the responsibilities of the employees;
- briefing notes for the employees;
- alarming and broadening the approach;
- procedures for information exchange, business continuity, and restarting;
- recovery plans for IT systems.

b. In the event of an emergency, the availability of appropriately trained employees is ensured. Responsibilities are described and implemented on the basis of the emergency guide.
c. Regular testing and training is conducted to verify that the measures outlined in the emergency guide are working as intended.
d. The emergency guide is regularly updated and, where necessary, supplemented with instructions for typical emergencies (for example, fires), and changes to the emergency guides are communicated to the employees involved in the emergency management.
e. The emergency guide is available to the employees involved in emergency management in the event of an emergency.

DER.4.M2 Integration of emergency management into inter-organisational processes [information security manager]

a. Emergency management is in line with security management (see ISMS.1 Security governance) and incident management (see DER.2.1 Handling of security incidents) processes.

3.4 Advanced measures

DER.4.M3 Scope and strategy of emergency management [management of the organisation] (C-I-A)

a. The scope and strategy for emergency management are set by the management of the organisation according to the organisation's objectives and the level of residual risks.

DER.4.M4 Emergency management policy and management responsibility [management of the organisation] (C-I-A)

a. The management of the organisation approves an emergency management policy.
b. The emergency management policy is regularly reviewed and updated as necessary.
c. The emergency management policy is communicated to all employees.

DER.4.M5 Organisation of emergency management [management of the organisation] (C-I-A)

a. Roles appropriate to the organisation's conditions are defined for emergency management.
b. b. The tasks, rights, and responsibilities of the roles are documented in the emergency guide (see DER.4.M1 Emergency guide).
c. Sufficiently qualified employees are assigned to the roles.
d. The practicality, performance, and efficiency of the organisation of emergency management is regularly reviewed.

DER.4.M6 Availability of the necessary resources [management of the organisation] (C-I-A)

a. Adequate financial, technical, and human resources are allocated to achieve the objectives of emergency management.
b. The emergency manager and the emergency management team have sufficient time to perform their emergency management tasks.

DER.4.M7 Emergency concept [management of the organisation] (C-I-A)

a. Critical business processes and associated assets are identified (for example, through business performance analysis).
b. Significant risks associated with critical business processes and assets are identified.
c. For each risk, a decision is made on the strategy to be implemented in dealing with the risk.
d. As part of the emergency concept, measures are selected and action programmes are drawn up to

restart and recover critical business processes. Recovery must be possible within an agreed time frame.
e. The emergency concept sets out the security measures to be used in the event of an emergency.

DER.4.M8 Involvement of employees in the emergency management process [manager, human resources department] (C-I-A)

a. A role-based emergency management awareness and training programme is in place to regularly inform employees.
b. Regular training is provided to the employees in the emergency management team.

DER.4.M9 Integration of emergency management into inter-organisational processes [management of the organisation] (C-I-A)

a. The emergency management aspect is integrated into all business processes of the organisation.
b. The processes, requirements, and areas of responsibility of emergency management are coordinated with risk and emergency management.

DER.4.M10 Tests and emergency trainings [management of the organisation] (C-I-A)

a. A training plan is in place to test and practise key emergency management action programmes and measures on a regular and case-by-case basis.
b. Adequate resources are allocated for the development, planning, and conduct of tests and trainings.

DER.4.M12 Documentation of the emergency management process (C-I-A)

a. Emergency management activities, interim results, and significant decisions are documented.
b. A procedure is in place for regularly updating emergency management documents.
c. Access to the documentation is permitted only to authorised persons.

DER.4.M13 Review and control of the emergency management system [management of the organisation] (C-I-A)

a. Emergency management reports are regularly submitted to the management.
b. The management monitors, evaluates, and adjusts the operation of the emergency management.

DER.4.M14 Regular overview and improvement of emergency measures [management of the organisation] (C-I-A)

a. The management coordinates IT, information security, and emergency management reviews and appoints emergency inspectors and inspection times.
b. The emergency measures are reviewed on a regular basis or in the event of major changes. It is verified that the measures are still appropriate to achieve the defined objectives.
c. The correctness of the implementation of the technical measures and the configuration of the IT systems and the effectiveness and efficiency of the organisational measures is verified.
d. The causes of any problems identified during the review are identified and appropriate corrective measures are proposed.
e. A performance report on the implementation of corrective measures is approved by the management. Any delays in the implementation of the measures is reported to the management in a timely manner.

DER.4.M15 Evaluation of the performance of the emergency management system [management of the organisation] (C-I-A)

a. The effectiveness and efficiency of the emergency management system is regularly evaluated according to defined measurement and evaluation criteria, and the results are compared with the results of previous evaluations.
b. The results of the evaluation are reported to the management, who decides on improvements to emergency management. The decisions of the management are documented.

DER.4.M16 Emergency response of outsourced components [management of the organisation] (C-I-A)

a. When planning the emergency response of outsourced components, the level of maturity of the supplier's or service provider's emergency management is assessed by a responsible person designated by the management.
b. Emergency tests and trainings are coordinated with the supplier or the service provider, joint trainings are organised as appropriate.
c. Information on test results, inspections, and improvement actions is exchanged regularly with the supplier or the service provider.

INF: INFRASTRUCTURE

INF.1 The building in general

1 Description

1.1 Purpose

To provide measures to address the typical technical and organisational security aspects of a building of the organisation. This takes into account the whole life cycle of the buildings, from the preparation of requirements, design, construction, use, to repair and moving out.

1.2 Responsibility

The technical department is responsible for the implementation of the measures for the module 'The building in general'.
Additional responsible persons: The construction manager, the construction company, the information security manager, the management of the organisation, the employee, the architect, the administrative department, the fire safety specialist.

1.3 Limitations

The communication and electrical cabling of the building is covered by module INF.12 Cabling, special rooms (for example, server and archive rooms) are covered by the corresponding modules of module group INF (Infrastructure). The involvement of external employees is addressed in module ORP.1 Organisation of information security.

2 Threats

2.1 Fire

Fire can cause significant damage to the building and its interior. People can be seriously injured or killed in a fire. In people, smoke inhalation can cause carbon monoxide poisoning. Smoke and high temperatures from fire can damage IT equipment, goods stored in the building, and the building's interior.

2.2 Lightning

During a thunderstorm, the current of the lightning can reach two hundred thousand amperes at a voltage of several hundred thousand volts. This enormous amount of energy is released and dissipated in 50-100 microseconds. If the lightning strikes a building directly, the energy from the lightning can cause significant damage to the building. A lightning strike can cause a fire and destroy nearby electrical equipment.

2.3 Water

Water can damage parts of buildings as a result of heavy rain, high water, or flooding. Water damage can also be caused by a water incident inside the building, for example due to defective water pipes or the careless use of water taps.

2.4 Threats caused by weather and natural disasters

Depending on its geographical location, the building is exposed to risks from weather and natural disasters. Extreme weather events include, for example, storms, hurricanes, and cyclones. Natural disasters can be caused by seismic or climatic events. Floods and landslides are significant threats in Estonia.

2.5 Environmental threats

Buildings can be damaged by nearby events, which are often completely unexpected (for example, the explosion of a chemical storage facility or leakage of toxic substances). All employees must be evacuated indefinitely from the vicinity of the accident site. Due to rescue operations in the area or road blockages, the building will be inaccessible or can only be used to a limited extent.

2.6 Unauthorised access

Persons who have entered the building unlawfully may intentionally damage or steal the organisation's property. Intruders may steal IT equipment, erase data or tamper with it. Burglary alone will cause property damage in the form of broken windows or doors. The purpose of a break-in is usually the theft of products that can be easily resold. A pre-planned attack with the purpose of copying or tampering with data without permission can cause much greater damage than the

destruction of IT equipment. An attacker may install an unauthorised interception device in the building, which can then be used to carry out subsequent tampering.

2.7 Breach of building regulations

Failure to comply with fire safety or structural safety requirements during the construction of a building (for example, use of non-compliant building materials) can lead to very severe consequences at a certain point. The risk is increased by the fact that such breaches are difficult to detect.

2.8 Inadequate fire barriers

Buildings contain a large number of pipes and cables (for example, water and sewage pipes, heating systems, electricity and communication cables) that run through different rooms. If appropriate fire barriers are not installed, fire and fumes can spread uncontrolled through the bushings.

2.9 Power outage

In the event of a power outage, entire buildings or parts of buildings may become unusable. It is not only normal electrical appliances, such as IT equipment or lighting, that depend on the availability of electricity, but all components of modern infrastructure (for example, lifts, air conditioning, security detection systems, security gates, automatic door locking systems, water pumps, sprinkler or telephone systems). Power outages are caused by errors in the cabling design, which means that cables are located in easily accessible places.

3 Measures

3.1 Life cycle

Planning

INF.1.M1	Planning building security
INF.1.M4	Fire alarm system of the building
INF.1.M5	Manual extinguishers
INF.1.M9	Building security programme
INF.1.M14	Lightning protection system
INF.1.M15	Layout diagrams for wiring and piping

INF.1.M16	Non-assignment of the purpose of the parts of the building requiring protection
INF.1.M17	Smoke control

Operation

INF.1.M2	Suitability of the electrical system
INF.1.M6	Closing windows and doors
INF.1.M12	Management of security tokens and keys
INF.1.M18	Fire safety inspections
INF.1.M19	Timely notification of the employee responsible for fire safety
INF.1.M36	Regular updating of infrastructure documentation

Implementation

INF.1.M3	Compliance with fire safety requirements
INF.1.M7	Access regulation and control
INF.1.M8	Smoking ban
INF.1.M10	Compliance with standards and regulations
INF.1.M27	Intrusion protection
INF.1.M13	Regulating access to technical systems

Emergency response

INF.1.M20	Fire emergency plan and fire safety drills

Additional advanced measures

INF.1.M22	Secure doors and windows
INF.1.M23	Security zones
INF.1.M24	Automatic water drainage systems
INF.1.M25	Selection of a suitable location
INF.1.M26	Surveillance and security services
INF.1.M30	Selection of a suitable building
INF.1.M31	Moving out safely
INF.1.M34	Alarm and warning systems
INF.1.M35	Protection of the external perimeter

3.2 Key measures

INF.1.M1 Planning building security [architect, information security manager]

a. The security measures of the building are designed according to the intended use of the building and the needs and the protection requirements of the business processes.
b. Security aspects ranging from fire safety and the electrical system to access control are taken into account to protect people, assets, and IT systems in the building.
c. Security measures are selected in consultation with the responsible parties and the security requirements of the sectors are harmonised.

INF.1.M2 Suitability of the electrical system

a. The technical parameters of the electrical system meet the actual needs.
b. The power consumed by the electrical system is evenly distributed between the three phases of the network.
c. The electrical control circuit and the fuses comply with the design of the control circuit.
d. Changes in the use of the premises and in the technical equipment (IT, air conditioning, lighting, etc.) are monitored and, if necessary, the electrical system is adapted.

INF.1.M3 Compliance with fire safety requirements [fire safety specialist]

a. The organisation's employees follow the fire safety rules.
b. The building is designed and constructed so that in the event of a fire:
- the load-bearing capacity of the building is maintained for the prescribed time;
- the generation and spread of fire and smoke in the building is limited;
- the spread of fire to neighbouring buildings is limited;
- safe evacuation is ensured;
- the safety and operational capabilities of the rescue team have been taken into account.

c. The fire safety requirements are complied with during the service life of the building.
d. Evacuation routes are clearly and properly marked and unobstructed. The usability of evacuation routes is regularly checked.
e. Fire doors are in a permanently closed position or close automatically in the event of an alarm.
f. To improve fire safety, unnecessary paper documents, packaging material, and flammable waste is removed from the premises.
g. A person responsible for fire safety is appointed. The responsible person has the necessary training.

INF.1.M4 Fire alarm system of the building [architect, fire safety specialist]

a. Smoke detectors are installed in the building.
b. At least the following locations are selected for the installation of smoke detectors:
- corridors;
- server rooms, technical rooms, and switchboard rooms;
- meeting rooms;
- ventilation ducts, if an air conditioning system is installed.

c. Smoke detectors are connected to a central fire alarm system.
d. If smoke is detected, an alarm is triggered that is audible to all occupants in the building.
e. The condition of the smoke detectors and the fire alarm system is verified regularly.

INF.1.M5 Manual extinguishers [fire safety specialist]

a. A sufficient number of manual extinguishers of the appropriate type and size is installed in the building in accordance with fire safety requirements.
b. The manual extinguishers are located in places where they are easily accessible in the event of a fire.
c. Only gas extinguishers are installed in rooms containing electrical and electronic equipment and data media.
d. Manual extinguishers are inspected and maintained regularly, with the time and frequency of inspections being documented.
e. Employees are proficient in the use of manual extinguishers, and the practical use of extinguishers is regularly practised.

INF.1.M6 Closing windows and doors [employee, administrative department]

a. If there are no people in the building, windows are kept closed and external doors (including balcony or terrace doors) are kept locked.
b. The procedure for closing doors and windows is known to the employees and regularly checked.

INF.1.M7 Access regulation and control [administrative department, information security manager]

a. Where appropriate, the building, buildings, or parts of the building are divided into security zones with different protection requirements (see INF.1.M23 Security zones).
b. Access to premises is controlled by technical measures (for example, security gates, self-closing

doors, security token-operated locking systems) and organisational measures (for example, visitor registration) according to the protection requirements of the premises.
c. The admission of visitors to buildings and premises is subject to established procedures.
d. Access to buildings and premises with high protection requirements is restricted. Access is restricted to authorised persons on the basis of an established access control list. Visitors are accompanied when entering premises with high protection requirements.
e. Visitors are required to wear a visitor's badge, clearly visible to everyone, distinguishable from the employees' badges.
f. The effectiveness of access control measures is regularly monitored.

INF.1.M8 Smoking ban [employees, administrative department]

a. Smoking is only permitted away from the building.
b. Smoking is strictly forbidden in rooms containing IT equipment or data media (for example, server rooms, archives), where fire and pollution can cause significant damage.
c. External doors leading to the smoking area are protected by an access control system and are not left open.

INF.1.M10 Compliance with standards and regulations [construction company, construction manager]

a. The applicable construction standards are followed in the design, construction, furnishing, repair, and installation of technical systems.

INF.1.M27 Intrusion protection

a. Measures that are both adequate and appropriate to local conditions are taken to prevent intrusion:
- doors and windows are secure;
- where necessary, windows are protected by security film or bars, and doors and windows by metal bars;
- where necessary, additional locks and latches are fitted to the doors;
- any additional entrances not in use are closed, emergency exits are intrusion-proof;
- ventilation openings and other technical openings are covered with grilles;
- outside working hours, lifts are key-operated.

b. The effectiveness of intrusion protection measures is regularly monitored.
c. Employees are aware of the intrusion protection measures and their responsibilities.

3.3 Standard measures

INF.1.M9 Building security programme [architect, information security manager]

a. Based on the organisation's overall security concept, a building security programme is in place, which provides, inter alia:

- principles for the layout of premises with high protection requirements;
- regulation of access to premises;
- use of surveillance systems;
- measures to reduce the impact of water and fire accidents;
- additional measures based on the location of the building;
- fire protection measures for IT infrastructure;
- security of technical services.

b. Following a security incident or a change in the use of buildings, the security programme is updated.
c. The rooms and parts of the building in need of protection are located away from high-risk areas (for example, ground floor, basements). The rooms in need of protection are preferably located in the interior of the building.

INF.1.M12 Management of security tokens and keys [administrative department]

a. The management and issuance of security tokens and keys is arranged centrally.
b. Security tokens and keys are issued only in justified cases and to authorised persons, and their issue and return is documented.
c. It is the responsibility of the employee to keep and use the security token and keys issued to them in a secure manner. Unauthorised copying of keys and security tokens is prohibited.
d. Spare keys are kept in a secure place and are accessible in case of emergency.
e. Procedures are in place to deal with the loss of security tokens or keys (notification, replacement, reimbursement, changing locks, etc.).
f. When an employee leaves work, they return the security token and keys issued to them.

INF.1.M13 Regulating access to technical systems

a. The switchgear of the technical systems is located in such a way as to prevent access by unauthorised persons.
b. Locks on cabinets and equipment are in good working order. Distribution cabinets are only opened by persons responsible for the specific technical system (see INF.1.M12 Management of security tokens and keys).
c. Backup keys are stored securely and are available when needed.
d. The components of the switchgear are clearly and permanently marked.
e. If fuses are used, the required number of spare fuses is kept in the equipment cabinet.

INF.1.M14 Lightning protection system

a. The selection of the protection class of the building's lightning protection system is based on the results of the risk analysis carried out in accordance with the relevant standard (standards EN 62305, EVS-HD 60364, and EVS-EN 60099).
b. In addition to the external lightning protection system, internal overvoltage arresters for electrical equipment are installed (see INF.12 Cabling).
c. The lightning protection system is regularly inspected and maintained.

INF.1.M15 Layout diagrams for wiring and piping

a. Persons are appointed to manage and update the layout diagrams for wiring and piping.
b. Layout diagrams are up to date and accurate, with accompanying explanatory text where needed.
c. As a minimum, the layout diagrams include the following information:
- precise routing of wiring and piping on each floor;
- precise technical data (type of cable or pipe, dimensions);
- purpose and user;
- labelling.

d. The maintenance works of wiring and piping are documented.
e. The layout diagrams are protected against unauthorised access. The layout diagrams are readily available when required.

INF.1.M16 Non-assignment of the purpose of the parts of the building requiring protection

a. Public building guides do not indicate the location of parts of the building that require protection (server rooms, data centres, archives, etc.).

b. The location of the parts of the building that require protection is not identifiable from the outside.
c. Door labels on the rooms requiring protection do not indicate the actual purpose of the rooms.

INF.1.M17 Smoke control [architect]

a. The performance of the smoke barrier of the structure is tested immediately after the completion of installation or repair works.
b. It is possible to quickly remove smoke from rooms containing IT equipment.
c. Fire doors are also smoke-tight (RS type).

INF.1.M18 Fire safety inspections [fire safety specialist]

a. Fire safety inspections are carried out regularly, at least once a year.
b. At least the following is assessed:
- the storage of flammable and explosive materials;
- the presence of combustible materials in technical and server rooms;
- the presence and maintenance of smoke detectors and fire extinguishers;
- the use of fire barriers;
- accessibility of evacuation routes.

c. Any deficiencies identified during the fire safety inspection are rectified as soon as possible.

INF.1.M19 Timely notification of the employee responsible for fire safety [fire safety specialist]

a. The employee responsible for fire safety is informed in good time of any forthcoming work affecting fire safety.
b. The employee responsible for fire safety checks the correct application of fire safety measures both during the construction of the building and after the completion of the works (see INF.1.M3 Compliance with fire safety requirements).

INF.1.M20 Fire emergency plan and fire safety drills [fire safety specialist]

a. A fire emergency plan is prepared to deal with a fire hazard.
b. Employees are provided with emergency and fire safety drills based on a plan of action in the event of a fire.

INF.1.M36 Regular updating of infrastructure documentation

a. Infrastructure documentation (structure, route, and cable diagrams, piping layout diagrams, evacuation route descriptions, and fire plans) is kept up to date.
b. Employees have a needs-based access to the documentation.
c. The fire action plan and the evacuation route plan are reviewed regularly. The plan is revised as necessary.
d. All employees are aware of changes to the fire safety and building use instructions.
e. Infrastructure documentation is kept up to date at least every three years.

3.4 Advanced measures

INF.1.M22 Secure doors and windows (C-I-A)

a. The doors and windows of the buildings comply with at least the protection class RC2 according to the standard EVS-EN 1627.
b. Where a data centre is present, its doors and their installation comply at least with protection class RC3.
c. The intrusion, fire, and smoke resistance of the windows, doors, and walls of the premises is at least equivalent to that of the other components.
d. The condition of security doors and windows is checked regularly.

INF.1.M23 Security zones [architect] (C)

a. Premises and areas are grouped into two, three, or four security zones according to similar protection requirements (for example, external area, controlled internal area, internal area, area with high protection requirements).
b. Postal, delivery, and loading zones are located in such a way that consignments can be received without the supplier having to enter other areas of the building.
c. Additional access controls (for example, security gates) are applied when entering a security zone with high protection requirements. The number of persons authorised to enter an area with high protection requirement is very limited.
d. The security zones of buildings and premises and their protection requirements are documented.

INF.1.M24 Automatic water drainage systems (A)

a. Areas at risk of water are equipped with leak detectors and water drainage systems.
b. Passive water drainage systems (via floor drains directly to the sewerage system) are provided

with non-return valves.
c. In the absence of a passive water drainage system, water pumps with an adequate capacity and reliability (active water drainage) are used to control the water.
d. Regular inspections are carried out to ensure that the water drainage systems are in good working order.

INF.1.M25 Selection of a suitable location [management of the organisation] (A)

a. The following environmental risks are taken into account in the choice of the location of the building:

- vibrations from traffic (road, rail);
- the risk of accidents due to the proximity of traffic routes;
- interference from high-voltage lines or radio masts;
- the possibility of flooding;
- technical accidents at neighbouring structures;
- crime in the surrounding area.

INF.1.M26 Surveillance and security services [administrative department] (C-I-A)

a. The tasks of the surveillance and security service are clearly documented.
b. Surveillance and security employees record the movement of persons through the main entrance (gate) and monitor other entrances by video surveillance. The duties of the surveillance and security services also include security inspections at the end of the working day (verifying that the external doors of the buildings are locked and the windows closed, activating the alarm system, etc.).
c. Employees and visitors present a photo access card (if implemented) or an identity document upon request by an employee of the surveillance and security services.
d. Visitor's badges are issued to visitors after their identity has been verified and they are instructed on how to use the badge. The visitor's badge is returned when the visitor leaves.
e. A contact person is designated for communication with the surveillance and security services. Employees of the surveillance and security services are informed of changes to access rights in a timely manner.

INF.1.M30 Selection of a suitable building [information security manager] (C-I-A)

a. A functional and security specification is prepared to assess the suitability of the buildings.
b. From an information security point of view, the following aspects are taken into account when assessing the suitability of a building:

- the extent of the building perimeter;
- whether the building structure is strong enough to accommodate server rooms, uninterruptible power supplies, and IT equipment in the most suitable locations within the building;
- whether security zones can be separated from each other, whether security gates and access routes can be created;
- whether access routes are suitable for the transport of large IT components;
- whether the leased building is also used by others at the same time.

c. The selection of the building is based on the need to ensure that the necessary security measures can be implemented in the building, especially in the case of leased buildings.

INF.1.M31 Moving out safely [administrative department] (C)

a. An inventory of assets (for example, hardware, software, data media, folders, and documents) that are critical from an information security perspective is prepared prior to moving out.
b. Each employee is informed of the items for which they are responsible for moving.
c. Useless equipment, data media, etc. are decommissioned before moving.
d. After moving out, all rooms are inspected for property left behind.

INF.1.M34 Alarm and warning systems (A)

a. An alarm and warning system appropriate to the premises and risks is used.
b. The alarm and warning system complies with the standard EVS-EN 50518.
c. In the absence of a centralised alarm and warning system, autonomous surveillance systems are used in premises with high protection requirements.
d. The alarm and warning system is regularly inspected and maintained.
e. A procedure is in place for responding to alarms.
f. The response to alarms is analysed and, if necessary, the procedure is adjusted.

INF.1.M35 Protection of the external perimeter [architect] (C-A)

a. Measures are taken to protect the external perimeter of the building.
b. The following protection measures are considered for the operation of the perimeter:

- enclosing buildings with a fence;
- measures to prevent accidental access to the territory;
- measures to make it more difficult for an intentional intruder to enter the territory:
- outdoor cameras and video recording equipment;
- automatic detection of the movements of persons and vehicles;
- automatic alarm and warning systems.

INF.2 Server room and data centre

1 Description

1.1 Purpose

To provide measures for creating and maintaining secure and sustainable operating conditions in the server room and data centre. The measures in this module are implemented for each data centre and server room.

1.2 Responsibility

The IT department is responsible for the application of the measures related to the server room and the data centre.
Additional responsible persons: The data protection specialist, the technical department, the employee, the architect, the maintenance personnel, the fire safety specialist.

1.3 Limitations

Not all organisations may have a data centre, but instead have one or more server rooms. Basic measures are implemented to ensure the security of the server room, with the remaining measures commensurate with the protection requirements (based on a C-I-A assessment).
The measures in this module are not adapted to small organisations with a few IT workstations and a server in a separate room. In this case, it is sufficient to apply the module INF.5 Technical infrastructure room or cabinet to the equipment room and the technical infrastructure equipment cabinet. Additional measures are implemented to protect the building (INF.1 The building in general) and cabling (INF.12 Cabling).

2 Threats

2.1 Data centre design errors

Threats arising from the location of a data centre (for example, industrial accidents, earthquakes, or floods) can affect the reliability and availability of IT systems. The lack of adequate power supply or data connectivity has a significant impact on the operation of the data centre.

2.2 Unauthorised access

In the event of inadequate access control, unauthorised persons may enter the data centre and cause damage either through negligence (for example, inadequate domain knowledge) or intentionally. Intentional damage consists in particular of theft of or tampering with equipment.

2.3 Inadequate monitoring

If the monitoring and management of the data centre infrastructure is inadequate, failures of technical components are detected too late and the failure is not responded to in a timely manner. Technical failures have a direct impact on server availability.

2.4 Unsuitable microclimate in the data centre

Failure to maintain the temperature, humidity, or fine particles in the air of the data centre at the levels specified by the equipment manufacturers will result in the malfunction or failure of technical components. Failure of the air conditioner will cause the temperature in the server room to rise rapidly, which may lead to the overheating of technical components and failures. High temperatures or humidity can also damage data media.

2.5 Fire

Fire and smoke can cause serious damage. A fire in a server room is a rather rare event, but one with very serious consequences. The most common cause of fires is faulty electrical equipment (for example, malfunction of the equipment related to the data centre's support functions such as the emergency power generator, uninterruptible power supplies, air conditioning). If the data centre does not have an internal fire protection system, the fire can spread quickly. Similarly, a fire outside the building can spread to the data centre. Fire and smoke pose a threat to people's life and health.

2.6 Water

Water can enter the data centre, for example due to leaking water pipes, flooding, broken pipes, faulty sprinkler or air conditioning systems. A water accident will cause the equipment to shut down and be damaged. Equipment damage may also take time to become apparent. A water accident can cause a short circuit, which can lead to a fire or widespread failures.

2.7 Missing or inadequate intrusion prevention

Even with a well-functioning access control, a targeted attacker may gain access to a data centre if no intrusion prevention measures are implemented. An attacker can leak sensitive data and steal or manipulate IT components. They can also destroy equipment or damage the data centre.

2.8 Power outage

A power outage significantly disrupts the operation of the data centre and therefore the business processes of the entire organisation. The IT services enabled by the data centre are suddenly no longer available. A power outage can cause data loss, damage to IT systems, damage to communication systems or to monitoring equipment.

2.9 Unclean environment

Dust in the data centre will cause technical components to fail over time. Equipment with fast-moving parts (for example, fans) will wear out faster and have more failures in dusty environments.

3 Measures

3.1 Life cycle

Planning

INF.2.M1	Establishment of security requirements for a data centre
INF.2.M12	Perimeter security of the data centre
INF.2.M13	Surveillance system of the data centre

Implementation

INF.2.M2	Fire compartments
INF.2.M3	Uninterruptible power supply (UPS)

INF.2.M4	Emergency power switch
INF.2.M9	Fire extinguishing system and extinguishing equipment
INF.2.M17	Early detection of fires
INF.2.M29	Inspection of wiring
INF.2.M15	Overcurrent protection system

Operation

INF.2.M5	Air temperature and humidity control
INF.2.M6	Access control
INF.2.M7	Locking and security of doors and windows
INF.2.M8	Fire alarm system
INF.2.M10	Inspection and maintenance of infrastructure
INF.2.M11	Monitoring of infrastructure
INF.2.M14	Emergency power generator
INF.2.M16	Environmental conditions of the data centre
INF.2.M19	Testing the technical infrastructure

Additional advanced measures

INF.2.M21	Backup data centre
INF.2.M22	Dust control
INF.2.M23	Secure cabling of the data centre
INF.2.M24	Video surveillance system
INF.2.M25	Duplication of uninterruptible power supplies
INF.2.M26	Duplication of emergency power generators
INF.2.M28	Surveillance system complying with advanced requirements

3.2 Key measures

INF.2.M1 Establishment of security requirements for a data centre [technical department, architect]

a. Technical and organisational requirements are in place for a data centre or a server room.
b. The design of a data centre or the choice of suitable premises takes into account the protection requirements of IT components located therein (in particular in terms of availability) and the possibility of implementing the necessary security measures.
c. The data centre is designed as a closed security area divided into security zones according to

protection requirements. The organisation also decides whether it is feasible to establish different security zones within the server room.
d. The zones for data centre management, logistics, support, and IT equipment are clearly separated.

INF.2.M2 Fire compartments [architect]

a. To limit the spread of fire and smoke, the data centre and, where possible, the server room is divided into fire and smoke compartments.
b. The zoning complies with current building and fire regulations.

INF.2.M3 Uninterruptible power supply (UPS) [technical department]

a. Electrical and IT equipment essential to the operation of the data centre, with the exception of equipment with a high energy consumption (for example, air conditioning), is connected to an uninterruptible power supply (UPS) to ensure uninterrupted power.
b. The uninterruptible power supply is of sufficient capacity, and its adequacy is verified after any major change to the electrical equipment.
c. In the UPS system of the data centre, the energy storage batteries are kept within the temperature and humidity range specified by the manufacturer, and to this end, it is recommended that the batteries are located separately from the electrical equipment.
d. The uninterruptible power supplies are maintained and their operability inspected periodically at the frequency specified by the manufacturer (see INF.2.M10 Inspection and maintenance of infrastructure).

INF.2.M4 Emergency power switch [technical department]

a. In the event of an emergency, the power supply to the data centre can be switched off in groups of individual electrical appliances.
b. In the event of an emergency, the power is switched off according to a well-planned programme; the entire data centre power supply is not switched off if possible. This takes into consideration the connection of the uninterruptible power supplies to the mains and the electrical appliances connected to them.
c. Emergency switches are protected against accidental or unauthorised switching off.

INF.2.M5 Air temperature and humidity control [technical department]

a. The air temperature and humidity of the IT equipment locations is within acceptable limits.
b. After any change in the composition and layout of the electrical equipment, the change in the thermal load of the cooled areas is verified.
c. Where possible, air conditioners are located in a separate room with the possibility of water drainage.
d. The air conditioners are maintained regularly.
e. It is possible to detect the exceeding of the limit values set for temperature and humidity later.

INF.2.M6 Access control [technical department]

a. The access management of data centre and server room access rights is in line with module ORP.4 Administration of identity and rights.
b. It is defined which persons, internal and external to the organisation, have the right to access the data centre, during which period, to which rooms, and for which purpose.
c. All access to the data centre is recorded.
d. There are no entrances to the data centre other than those through which entry is recorded.
e. For the server room, the need for a separate access control system is assessed.
f. The functioning of the access systems and the registration of entrants is regularly checked.

INF.2.M7 Locking and security of doors and windows [employee, technical department]

a. All doors to the data centre are locked at all times.
b. The data centre is designed without windows. If windows are present, they are always locked in the same way as doors.
c. Doors and windows provide protection against attacks and environmental impacts.
d. All peripheral structures of the data centre or server room have equivalent protection.

INF.2.M8 Fire alarm system [architect, fire safety specialist]

a. A fire alarm system covering all rooms is installed in the data centre.
b. The fire alarm messages are transmitted in accordance with the prescribed procedures (see INF.2.M13 Surveillance system).
c. The fire alarm system is maintained regularly.
d. The data centre is free from excess flammable materials.

INF.2.M9 Fire extinguishing system and extinguishing equipment [technical department, fire safety specialist]

a. An up-to-date fire extinguishing system is installed in the data centre. In server rooms without automatic fire extinguishing systems, fire and smoke detectors are installed for the early detection of fires (see INF.2.M17 Early detection of fires).
b. Employees have been informed of how to act when the fire extinguishing system is triggered.
c. Manual extinguishers of the required size and with the prescribed extinguishing agent are made available in the server room.
d. A sufficient number of extinguishers is available and they are located in easily accessible places. An extinguisher can be reached in less than three minutes.
e. Employees with access to the data centre or server room know how to use the manual extinguishers and the fire extinguishing system safely.
f. The fire extinguishing system is regularly inspected and maintained.

INF.2.M10 Inspection and maintenance of infrastructure [technical department, maintenance personnel]

a. The maintenance of structural and technical infrastructure components is carried out in accordance with the maintenance intervals recommended by the manufacturer or specified in the requirements.
b. Infrastructure inspections and maintenance are documented.
c. The fire barriers of cable and pipe bushings between fire and smoke compartments are inspected regularly.

INF.2.M11 Monitoring of infrastructure [technical department]

a. Failure and other messages of infrastructure automation (for example, leak detection, air conditioning, power supply and UPS systems) are monitored, if possible, automatically.
b. Notifications are communicated in the prescribed manner and responded to as quickly as possible.
c. Remote monitoring is available for infrequently used IT and support equipment of the server room.

INF.2.M17 Early detection of fires [architect, technical department]

a. Fire and smoke detectors are installed in the data centre and server room for the early detection of smoke or fumes.

b. Sensor signals are automatically transmitted to the alarm centre, which responds to the alarm within a maximum of five minutes.
c. In the case of duplication of IT equipment, the corresponding equipment is located in different power cut-off zones.

INF.2.M29 Inspection of wiring [architect, technical department]

a. Only the electrical cables necessary to power the equipment of the data centre are installed in the data centre.
b. The wiring is properly installed in the data centre or server room, and the routing of the wires is traceable.
c. If other wiring runs through the data centre or server room, the reason for its use is documented. These cables are also handled and protected in accordance with the requirements of the data centre.
d. The condition of the wiring is inspected regularly.

3.3 Standard measures

INF.2.M12 Perimeter security of the data centre [architect, technical department]

a. Perimeter security measures of the data centre comply with the security programme and the building protection requirements.
b. Perimeter security of the data centre includes the following measures:

- secure perimeter enclosures;
- fencing of the data centre;
- measures to prevent accidental entry into restricted areas;
- measures to make it more difficult to break into the data centre:
- outdoor cameras and video recording equipment;
- automatic detection of the movements of persons and vehicles;
- automatic alarm and warning systems.

INF.2.M13 Surveillance system of the data centre [technical department]

a. The design of the surveillance system is based on the security requirements of the data centre and takes into account different protection requirements and possible changes in the use of the different sections of the data centre building.
b. The equipment of the surveillance system is suitable for the environmental conditions at the

installation site.
c. The configuration of the surveillance system is adapted to changes in the use of different parts of the building.
d. Surveillance system notifications and alarms are directed to responsible persons who are capable of responding to alarms around the clock.

INF.2.M14 Emergency power generator [architect, technical department]

a. In the event of a power outage, an emergency power generator is used in addition to UPSs to provide power to the data centre.
b. The generator is regularly maintained; the date of maintenance and the work carried out is documented. During the maintenance, the generator is started through a check run.
c. The fuel for the emergency power generator is stored in a secure manner, in accordance with fuel storage requirements.
d. The fuel supply of the emergency power generator is checked regularly. The amount of fuel is kept within the permitted limits, but is sufficient to ensure continuity of operation.
e. Refuelling the generator fuel tank is documented.

INF.2.M15 Overcurrent protection system [architect, technical department]

a. The overcurrent protection and its installation comply with standard EVS-EN 62305-4 and the equipment specifications.
b. Overcurrent protection is tested at least once a year.

INF.2.M16 Environmental conditions of the data centre [architect, technical department]

a. Suitable environmental conditions are established in the data centre.
b. The data centre's air temperature and humidity meet the standard conditions and equipment specifications.
c. The air conditioners selected for the data centre are of sufficient capacity and robustness.
d. The air parameters are monitored regularly, and any deviations are automatically reported to the responsible person.

INF.2.M19 Testing the technical infrastructure [technical department]

a. The performance of the technical infrastructure of the data centre is tested at least once a year. In addition, the infrastructure is tested after incidents, major system modifications, or major repairs.
b. The results of infrastructure testing are documented.

3.4 Advanced measures

INF.2.M21 Backup data centre (A)

a. A backup data centre in another geographical location is available for emergencies.
b. The backup data centre is able to continue all the processes performed in the data centre.
c. Operational data is either mirrored or regularly copied from the main data centre.
d. The migration to the backup data centre is regularly tested and practised.
e. The data channels in the backup data centre are secure and duplicated.

INF.2.M22 Dust control [technical department] (I-A)

a. Dust and air pollution control is designed and implemented during the construction and expansion of the data centre.
b. The effectiveness of the dust control measures is regularly verified during the construction. The inspections are carried out by persons not directly involved in the construction work.

INF.2.M23 Secure cabling of the data centre [technical department] (A)

a. Cables of the data centre cables are protected against unwanted mechanical stress, tampering, interception, and fire damage.
b. Cables and support systems meet the requirements arising from the protection requirements of the data centre.
c. Cables for multi-source IT equipment and other duplicating cables are placed in separate cable trays and exit the room through different bushings.

INF.2.M24 Video surveillance system [architect, technical department, data protection specialist] (I-A)

a. Access control systems and intrusion detection systems are supplemented by a video surveillance system in sensitive locations.
b. The use of the video surveillance system is in line with the overall security concept.

c. The data protection specialist is involved in the design of the video surveillance system and approves the implementation of the video surveillance system.
d. The central equipment of the video surveillance system is located in a secure environment and protected against unauthorised access.
e. The functioning of the video surveillance system is regularly monitored.

INF.2.M25 Duplication of uninterruptible power supplies [architect] (A)

a. The UPS systems in the data centre are sufficiently redundant.
b. If the data centre is connected to multiple power lines, each power line is equipped with an independent UPS system.
c. The UPS systems provide power to the essential components of the data centre until a switch to an alternative power source is made.

INF.2.M26 Duplication of emergency power generators [architect] (A)

a. The emergency power generator is duplicated in case of high availability.
b. The emergency power generator system receives regular maintenance.

INF.2.M28 Surveillance system complying with advanced requirements [architect] (I-A)

a. The surveillance system of the data centre locations with high protection requirements complies with Grade 3 or 4 of the standard EVS-EN 50131-1.

INF.5 Technical infrastructure room or cabinet

1 Description

1.1 Purpose

To provide measures for ensuring the security of the technical infrastructure room or technical infrastructure cabinet. For example, power supply and ventilation equipment, communication system components, cable panels, switches, or routers may be located in the technical infrastructure room.

1.2 Responsibility

The information security manager is responsible for the security measures of the module 'Technical infrastructure room or cabinet'.
Additional responsible persons: The technical department, the IT department, the employee, the architect, the maintenance personnel.

1.3 Limitations

When hosting servers, additional measures are implemented from module INF.2 Data centre and server room. If the technical infrastructure to be protected cannot be placed in a separate room, the technical infrastructure can also be placed in a dedicated cabinet.
The communication and electrical cabling of the room containing the technical infrastructure is dealt with in module INF.12 Cabling.
In a small organisation with only a few central IT devices, this module is implemented instead of INF.2 Data centre and server room.

2 Threats

2.1 Poor planning

In case of the unsuitable location of the technical infrastructure room (technical room), water may enter the room. IT components can overheat due to direct sunlight. The unsuitable location of the room significantly increases the possibility of break-ins.

2.2 Unauthorised access

Unauthorised persons may gain access to the technical infrastructure room and cause damage to the room, either unintentionally (for example, due to lack of knowledge of the area) or intentionally, if access controls are insufficient or measures to prevent intrusion are ineffective. In addition to equipment theft, an intruder who gains access to the room can also replace, tamper with, or destroy the equipment in the room.

2.3 Insufficient ventilation

Insufficient ventilation of technical equipment causes the temperature in an enclosed space or cabinet to rise above the normal operating limit of the equipment. As a consequence, equipment malfunctions may occur. Sensitive equipment can be permanently damaged by high temperatures.

2.4 Fire

In the event of a fire, the technical infrastructure room can be significantly damaged or completely destroyed. As a result, business processes that depend on the equipment in the room are disrupted. Common causes of fire are carelessness (for example, when smoking in the room ignites cables and equipment made of flammable materials) or equipment failure (for example, when safety switches or equipment fuses fail to operate in the event of an overvoltage). A fire that starts in a technical infrastructure space may spread to other parts of the building and, vice versa, a fire that starts in the building may spread to the technical infrastructure room.

2.5 Water

Flooding of the technical infrastructure room causes water damage to the equipment in the room as well as to the room itself. Flooding can be caused by leaks in nearby water pipes, blockages in sewer pipes, or rainwater that has entered the room as a result of heavy rain. Water damage can cause short circuits in the electrical equipment. Mould and corrosion can form in the equipment when exposed to water.

2.6 Power outage

In the event of a power outage and in the absence of a backup power supply, equipment will stop working, leading to disruptions in the organisation's business processes. A sudden and uncontrolled power cut will cause damage to equipment, the real impact of which will only become apparent once power is restored. Equipment failure due to a power outage can also cause indirect damage (for example, if a ventilation system does not start automatically after a power failure, the temperature in the room can rise rapidly and other equipment may stop working as a result).

2.7 Lightning and overvoltage

The effects of a lightning strike can also be dangerous for electrical equipment located within a few hundred metres of the point of impact due to the induction effect. Momentary overvoltage in cables and electrical equipment in the technical infrastructure room can cause equipment malfunction or even total destruction.

2.8 Electromagnetic disturbances

Sources of electromagnetic fields (for example, lift motors, transmitting aerials, or the grounding of a lightning protection system) in the vicinity of the technical infrastructure room or cabinet may interfere with the operation of automation and IT equipment. Electromagnetic disturbances can cause failures of and damage to sensitive components that consume electricity. The pieces of equipment in the technical infrastructure room itself can also interfere with each other.

2.9 Electrostatic disturbances

The build-up and sudden release of electrostatic charges, for example when a device is touched, can damage equipment with sensitive electronic components in the technical infrastructure room. In more severe cases, the electrostatic charge may completely destroy the equipment.

3 Measures

3.1 Life cycle

Planning

INF.5.M1	Design of the security of the technical infrastructure room
INF.5.M2	Appropriate location and size of the technical infrastructure room
INF.5.M4	Protection against intrusion
INF.5.M5	Protection against electromagnetic interference
INF.5.M6	Reduction of reaction to fire
INF.5.M9	Suitable electrical supply system
INF.5.M8	Prevention of uncontrolled electrostatic charges
INF.5.M10	Suitable air temperature and humidity
INF.5.M11	Avoidance of utility and gas piping
INF.5.M12	Protection of connecting ducts against accidental damage
INF.5.M13	Protection against damage from fire and smoke
INF.5.M14	Minimising the risk of fire in neighbouring areas
INF.5.M15	Lightning and overvoltage protection
INF.5.M18	Location of the technical infrastructure room

Operation

INF.5.M3	Access regulation and control
INF.5.M7	Appropriate use of the room

INF.5.M16 Uninterruptible power supply (UPS)

INF.5.M17 Inspection and maintenance of the infrastructure

Additional advanced measures

INF.5.M19 Backup location of the technical infrastructure

INF.5.M20 Extended protection against intrusion

INF.5.M22 Backup power

INF.5.M23 Emergency power generator

INF.5.M24 Ventilation and cooling system

INF.5.M25 Enhanced protection against damage from fire and smoke

INF.5.M26 Monitoring of the electrical equipment

3.2 Key measures

INF.5.M1 Design of the security of the technical infrastructure room [architect]

a. Appropriate technical and organisational security measures are implemented in the technical infrastructure room, in accordance with the protection requirements, legislation, and regulations.
b. The design of security takes into account the environmental and intrusion risks posed by the location of the room.

INF.5.M2 Appropriate location and size of the technical infrastructure room [architect]

a. The technical infrastructure room is not passable. The technical infrastructure cabinet is not in a passable location.
b. There is sufficient space for working and evacuation if necessary.

INF.5.M3 Access regulation and control [technical department, IT department]

a. It is defined who has the right of access to the technical infrastructure room, for what period, and for what purpose.
b. The granting of unduly extensive access rights is avoided.
c. All presences in the technical infrastructure room are recorded.

INF.5.M4 Protection against intrusion [architect, technical department]

a. The technical infrastructure room is protected against unauthorised access.
b. The walls, ceilings, floors, windows, and doors of the technical infrastructure room are appropriate to the protection requirements of the room.
c. The intrusion resistance of the enclosures complies with the requirements of the standard EVS-EN 1627. The door of the room has the appropriate protection class.

INF.5.M5 Protection against electromagnetic interference [architect]

a. It is tested that there is no disturbing electromagnetic radiation in the immediate vicinity of the technical infrastructure room.
b. The technical infrastructure room or cabinet is not in the immediate vicinity of large electric motors (for example, lift motors).

INF.5.M6 Reduction of reaction to fire [employee, architect]

a. No flammable materials are stored in or in the immediate vicinity of the technical infrastructure room.
b. The peripheral structure of the room and the furnishings of the room do not contain flammable materials.

INF.5.M7 Appropriate use of the room [employee, architect]

a. The technical infrastructure room is not used for any other purpose.

INF.5.M9 Suitable electrical supply system [technical department]

a. The low-voltage network of the technical infrastructure room is set up in a TN-S (isolated neutral and protective conductor) wiring system.

INF.5.M16 Uninterruptible power supply (UPS) [technical department]

a. It is specified which devices must be connected to the uninterruptible power supply and which devices must not be connected to the UPS.
b. The voltage and amperage of the uninterruptible power supply are calculated according to the connected electrical appliances. The adequacy of the capacity of the UPS systems is verified following major changes affecting electricity consumption.
c. To prolong the lifetime of the batteries in the uninterruptible power supply, the batteries are kept

in the optimal temperature range.
d. The UPS backup power supply has a duration sufficient to safely shut down all the electrical equipment connected to it.
e. The uninterruptible power supply is maintained and its performance is verified at least at the intervals recommended by the manufacturer.

3.3 Standard measures

INF.5.M8 Prevention of uncontrolled electrostatic charges [architect]

a. The technical infrastructure room is equipped with a non-electrostatic floor covering that complies with the standard EVS-EN 14041.

INF.5.M10 Suitable air temperature and humidity [technical department]

a. The air temperature and humidity of the technical infrastructure room are within the values specified in the specifications of the equipment to be operated.
b. The ventilation system has an adequate power reserve.

INF.5.M11 Avoidance of utility and gas piping [architect, technical department]

a. Only the piping necessary for the operation of the technology in the room is located in the technical infrastructure room.
b. No water, gas, fuel, heating, sewerage, or similar pipes pass through the technical infrastructure room.

INF.5.M12 Protection of connecting ducts against accidental damage [architect]

a. Connection ducts (for example, protective pipes and cable ducts) outside the technical infrastructure room are protected against accidental damage.

INF.5.M13 Protection against damage from fire and smoke [architect, technical department]

a. All structural elements (including doors and windows) have similar smoke control properties.
b. The peripheral structure of the technical infrastructure room can withstand fire and smoke for at least 30 minutes.
c. There are no flammable materials in the vicinity of the cable routes.

INF.5.M14 Minimising the risk of fire in neighbouring areas [architect, technical department]

a. There are no technical rooms containing flammable materials in the immediate vicinity of the technical infrastructure room.

INF.5.M15 Lightning and overvoltage protection [architect, technical department]

a. The electrical system of the building is protected against overvoltage.
b. The technical infrastructure room complies at least with Lightning protection zone 2 (LPZ 2) of the standard EVS-EN 62305.
c. The surge protection equipment is inspected regularly and replaced if necessary.

INF.5.M17 Inspection and maintenance of the infrastructure [technical department, IT department, maintenance personnel]

a. Maintenance of structural and technical infrastructure components is carried out in accordance with the maintenance intervals recommended by the manufacturer or specified in the normative documents.
b. The fire barriers of cable and pipe bushings between fire and smoke compartments are inspected regularly.
c. Infrastructure inspections and maintenance are documented.

3.4 Advanced measures

INF.5.M18 Location of the technical infrastructure room [architect]

a. The design of the technical infrastructure room takes into account internal and external threats.
b. The technical infrastructure room is protected against water-related threats (for example, rain, water, waste water). If the room is located on the top floor of the building, it is ensured that water does not enter the building from the roof.
c. Technical infrastructure rooms are protected from heating due to solar radiation.

INF.5.M19 Backup location of the technical infrastructure [architect]

a. In the event of an emergency, it is possible to relocate the technical infrastructure to another location prepared for this purpose.
b. The main and backup room of the technical infrastructure are powered by a number of electrical

switchgears.
c. The rooms are located in separate fire compartments and have independent air conditioning systems.

INF.5.M20 Extended protection against intrusion [architect]

a. The technical infrastructure room does not have windows. If windows are present, they are always closed and protection measures are implemented to protect the windows based on the floor height.
b. Openings to the room other than windows and doors (for example, ventilation ducts) are protected in the same way as other peripheral structures.
c. In the technical infrastructure room, all windows, doors, and other access openings are covered by the security alarm system.
d. Communication and electrical cables are fully protected against unauthorised access.
e. The intrusion resistance of the peripheral structures, including windows and doors, is equivalent to the protection requirement of the room.
f. The quality of locks, lock cores, and safety bars is appropriate to the protection class of the door.

INF.5.M22 Backup power [architect]

a. The electrical supply is duplicated from the main switchboard to the electrical equipment in the technical infrastructure room by means of power supply lines in a separate fire compartment.
b. The low-voltage distribution system has the possibility to add backup lines.

INF.5.M23 Emergency power generator [architect, technical department, maintenance personnel]

a. An emergency power generator complements the power supply company's grid supply.
b. The fuel for the emergency power generator is stored in a secure manner, in accordance with fuel storage requirements.
c. The fuel supply of the emergency power generator is checked regularly. The amount of fuel is kept within the permitted limits, but is sufficient to ensure continuity of operation.
d. Emergency power generators are regularly maintained.
e. During emergency power generator maintenance, generator check runs and load testing are carried out.

INF.5.M24 Ventilation and cooling system [architect, technical department, maintenance personnel]

a. The ventilation and cooling equipment in the technical infrastructure room is duplicated.
b. The ventilation and cooling systems are regularly maintained.
c. In the case of very high protection requirements, the maintenance of ventilation and cooling equipment is duplicated.

INF.5.M25 Enhanced protection against damage from fire and smoke [architect]

a. The peripheral structure, air dampers, and supply lines of the technical infrastructure room can withstand fire and smoke for at least 90 minutes.
b. In the case of very high protection requirements, individual rooms are treated as independent fire compartments.
c. Cable routes outside the technical infrastructure room are located in separate fire compartments.
d. Fire and smoke detectors connected to the central fire alarm system are installed in the technical infrastructure rooms.
e. Fire dampers responding to smoke detectors are installed in the ventilation ducts.
f. In the case of very high protection requirements, an automatic fire extinguishing system is installed in the technical infrastructure room.
g. The fire alarm system, the smoke detectors, and the automatic extinguishing system are connected to an uninterruptible power supply and to an emergency power generator.

INF.5.M26 Monitoring of the electrical equipment [architect, technical department]

a. Monitoring equipment is installed to detect and report faults in the electrical supply.
b. Leak and ground current test measurements are performed regularly.

INF.6 Data media archive

1 Description

1.1 Purpose

To provide measures to protect the data media archives and the information on the data media to be archived. The module is applied to all rooms used as data media archives.

1.2 Responsibility

The information security manager is responsible for the implementation of the measures for the data media archive.
Additional responsible persons: The fire safety specialist, the technical department, the employee, the architect.

1.3 Limitations

This module deals with the security measures for the data media archive. Measures for archiving are provided in OPS.1.2.2 Archiving.

2 Threats

2.1 Unacceptable temperature and humidity levels

When storing data media for long periods of time, temperature changes and excessive humidity can cause errors in the data and shorten the shelf life of the data media.

2.2 Absence or inadequacy of regulations

If there are no procedures in place for working in the archive room, employees may unintentionally cause dangerous situations. For example, if employees do not close and lock windows and doors after leaving the archive, data media can be stolen from the archive. Unauthorised persons can access, view, store, or transmit sensitive data. Problems also arise when operational procedures are in place but not followed.

2.3 Unauthorised access to rooms requiring protection

In case of inadequate or non-existent access control, unauthorised persons can enter the data media archives and view, steal, or tamper with sensitive information. Regardless of the initial damage caused, manipulated data can have a significant impact on operational processes.

2.4 Theft

Due to the small size of data media, it is easy to conceal them inconspicuously in pockets or under clothing and take them away. If there is no backup of the data, the organisation will lose the data. Persons who steal the data media have the opportunity to view and disclose confidential data. The damage caused by the theft is significantly higher than the cost of replacing the data media.

3 Measures

3.1 Life cycle

Planning

INF.6.M1	Manual extinguishers
INF.6.M3	Protection against dust and soiling
INF.6.M6	Avoiding water pipes
INF.6.M7	Suitable indoor climate

Operation

INF.6.M2	Access regulation and control
INF.6.M4	Closing and locking windows and doors
INF.6.M5	Protective cabinets

Implementation

INF.6.M8	Secure doors and windows

Additional advanced measures

INF.6.M9	Surveillance system

3.2 Key measures

INF.6.M1 Manual extinguishers [fire safety specialist]

a. The data media archives are equipped with manual gas extinguishers (weighing up to 20 kg).
b. In the event of a fire, the manual extinguishers are easily accessible.
c. Manual extinguishers are regularly inspected and maintained.
d. Employees know where the manual extinguishers are located and how to use them.

INF.6.M2 Access regulation and control [technical department]

a. Access to the data media archive is restricted to certain positions.
b. The access system allows access only to authorised persons.
c. Granted access rights are documented, employees are able to identify unauthorised persons.
d. The efficiency of access control measures is regularly verified.
e. The intrusion resistance of the archive room is at least RC2 pursuant to standard EVS-EN 1627.

INF.6.M3 Protection against dust and soiling [employee]

a. The need for protection against dust and soiling is already taken into account when the archive room is built.
b. The data media are packaged and stored in such a way that they are not damaged by dust, even during long-term storage.
c. Smoking in the data media archive is strictly prohibited.

INF.6.M4 Closing and locking windows and doors [employee]

a. The data media archive does not have windows wherever possible. If windows are present, they are closed before leaving the archives.
b. All windows are closed and doors locked when no one is present in the data media archive.
c. The requirement to close windows and lock doors is laid down in the regulations for the use of the archive room.
d. Employees are familiar with the regulations for the use of the archive room and comply with them.
e. The closing and locking of windows and doors is verified regularly.

3.3 Standard measures

INF.6.M5 Protective cabinets [employee]

a. In order to protect the data media against fire and unauthorised use, the data media are kept in suitable protective cabinets in the archive.

INF.6.M6 Avoiding water pipes [technical department]

a. Only water pipes that are absolutely necessary are located in a data media archive.
b. Water pipes passing through a data media archive are regularly inspected for leaks.
c. Measures are implemented to detect leaks early (leak detectors) and to minimise damage (water

drainage channels).
d. An incident management plan is drawn up for the archives with high protection requirements, specifying who is informed in the event of a leak and what is done to stop the leak.

INF.6.M7 Suitable indoor climate [technical department]

a. The air temperature, humidity, and particulate concentration in the data media archive are within the limits specified by the data media manufacturers.
b. The archive ventilation and air conditioning systems are regularly inspected and maintained.
c. Readings of air temperature and humidity are recorded. Abnormalities are responded to immediately.

INF.6.M8 Secure doors and windows [architect]

a. The intrusion resistance of the peripheral structures of the archive is at least RC3 pursuant to standard EVS-EN 1627.
b. Doors and windows have adequate fire and smoke resistance.
c. The intrusion, fire, and smoke resistance of the peripheral structures of the archive room is equivalent.
d. The security of doors and windows is regularly verified.

3.4 Advanced measures

INF.6.M9 Surveillance system [technical department] (C-I-A)

a. A surveillance system (central or local) appropriate to the protection requirements is installed in the data media archive.
b. Surveillance system notifications and alarms are directed to the responsible persons, who have the 24/7 capability to respond to alarms.
c. The surveillance system is regularly inspected and maintained.

INF.7 Office workplace

1 Description

1.1 Purpose

To present information security measures adaptable to office premises and office workplaces. An office workplace is an area within the organisation that is used by one or more employees to perform their work tasks.

1.2 Responsibility

The information security manager is responsible for compliance with the office workplace measures. **Additional responsible persons:** The technical department, the employee, the director, the administrative department.

1.3 Limitations

The module does not cover the recommendations related to the configuration and security of IT systems; these measures are included in the SYS module group. Measures related to cabling of office premises are presented in module INF.12 Cabling. Measures for fire safety and access control in buildings are included in module INF.1 The building in general.

2 Threats

2.1 Unauthorised access

In the case of inadequate or non-existent access control, unauthorised persons can enter the office premises and view, steal, or tamper with sensitive information. Regardless of the initial damage caused, manipulated data can have a significant impact on operational processes.

2.2 Unsuitable working conditions

A non-ergonomic workplace, inefficient use of space, or an unsuitable working environment can pose a risk to the health and fitness for work of people working in the premises. Office noise levels, frequent movement of customers, poor lighting, or inadequate ventilation can lead to reduced performance. When employees cannot concentrate undisturbed, human errors increase and data integrity is compromised.

2.3 Risks related to visitors and external personnel

Persons who are present in the office premises as visitors or on a temporary assignment may also pose a threat to the security of the organisation. A visitor to the premises may inadvertently disclose internal information of the organisation. The employee of an external service provider may be able to read documents left out in the open or access the organisation's IT systems through an unlocked computer.

2.4 Tampering with or destruction of IT assets

An attacker may set the destruction of an organisation's IT systems and assets for as their purpose. Destroying or tampering with a data media can lead to significant downtime in the operational processes. The impact of an attack is more widespread the later it is discovered and the wider the perpetrator's expertise.

2.5 Theft

If the office premises are not locked or the IT equipment is not sufficiently secured, it is very easy to quickly and inconspicuously slip a data medium or a smart device into the pocket and take it away. The indirect damage caused by the theft is significantly higher than the cost of replacing the data medium.

2.6 Disorganisation of cabling

Depending on how carefully the layout of the cable connections and plugs in the office premises is designed, employees will use extension cords or cable extensions for necessity or convenience. Often, extension cords are routed across floors and walkways. Such free cabling can result in people tripping and injuring themselves. Employees can also knock IT equipment from the desk or otherwise damage it by getting caught behind a cable.

3 Measures

3.1 Life cycle

Planning

INF.7.M1	Selection of suitable office premises
INF.7.M3	Secure installation of power and communication cables
INF.7.M5	Ergonomic workplace

Operation

INF.7.M2	Closing windows and locking doors
INF.7.M6	Organised workplace
INF.7.M7	Procedures for the storage of documents and data media

Additional advanced measures

INF.7.M8	Anti-theft devices

3.2 Key measures

INF.7.M1 Selection of suitable office premises [director]

a. Only premises intended for this purpose and equipped accordingly are used as office spaces.
b. Security and access control systems are appropriate to the protection requirements of the information handled in the room.
c. Public office premises are separated from areas with high protection requirements.

INF.7.M2 Closing windows and locking doors [employee, administrative department]

a. The windows of the office premises are closed during non-working hours.
b. Where confidential information is held in the office premises, employees lock the door when leaving the room.
c. Fire and smoke doors are closed at all times.
d. The obligation to close and lock windows and doors is laid down in the regulations, which employees are familiar with and comply with.
e. Compliance with the regulations on closing windows and locking doors is checked regularly.

INF.7.M6 Organised workplace [employee]

a. Employees are required to keep their workplace organised. There are no excessive documents, data media, or other objects at the workplace.
b. The employee protects IT applications and sensitive information from unauthorised access.
c. The monitor is out of the line of sight of unauthorised persons and a screen filter is used where necessary.
d. When the employee is away from their workplace, the screen is locked and data media and

documents are removed from the desk (clean desk policy).
e. Workplace organisation is checked on a random basis.

3.3 Standard measures

INF.7.M3 Secure installation of power and communication cables

a. The number of power and network outlets in the office premises is sufficient and they are located close to the IT equipment.
b. If placing loose power or communication cables on the floor is unavoidable, the cables are covered with cable protection tape.

INF.7.M5 Ergonomic workplace [administrative department, director]

a. Employees' workplaces are ergonomic and comply with occupational safety requirements.
b. The desk and chair at the computer workplace are adjustable according to the individual needs of the employee.
c. The screen, keyboard, and mouse are ergonomic and, as far as possible, are selected to suit the employee's habits.
d. For employees using a computer there are procedures for working with the monitor, which provides for regular rest breaks.

INF.7.M7 Procedures for the storage of documents and data media [employee, technical department]

a. There are storage facilities in or near the office premises with adequate storage capacity for documents and data media containing sensitive information.
b. Documents and data media containing sensitive information that are currently not in use are placed in a lockable drawer or cabinet allocated to each employee.
c. The intrusion resistance of the storage for sensitive material and the lock meet the information protection requirements.

3.4 Advanced measures

INF.7.M8 Anti-theft devices [employee] (C-I-A)

a. In the absence of an access control system, IT devices are secured either by mechanical (for example, cable lock, Kensington lock) or electronic anti-theft devices.
b. The use of anti-theft devices is mandatory when IT equipment is used in public areas.

INF.8 Home workplace

1 Description

1.1 Purpose

To provide measures for protecting the organisation's information and to establish a secure infrastructure at the home workplace. As a general rule, the home workplace is also accessible to family members, guests, and pets.

1.2 Responsibility

The employee is responsible for the implementation of the home workplace measures.

1.3 Limitations

The module INF.8 Home workplace applies to premises used as a remote workplace. Security measures for IT systems are covered in OPS.1.2.4 Remote work and in the relevant system-specific modules. The module is complemented by the measures in modules NET.3.3 Virtual private network (VPN) and SYS.2.1 Client computer in general.

2 Threats

2.1 Absence or inadequacy of regulations on working from home

In the absence of a specific code of conduct for working from home, IT systems can fail and lead to prolonged downtime. If IT problems cannot be solved through remote management, in emergency cases, an IT employee will have to be on site, which will further prolong the downtime caused.

2.2 Unauthorised access to the home workplace

Unauthorised persons may have access to the premises of a home workplace where data or equipment requiring protection is processed or stored. A computer left unattended could be stolen or infected with malware. Along with the stolen IT device, important data would be lost. Even sensitive documents cannot be adequately secured and protected from unauthorised access in the home workplace.

2.3 Unsuitable working conditions

A suitable working environment cannot always be guaranteed in the home workplace. Using a computer is not ergonomic, so working for long periods in a row reduces productivity and is bad for the employee's health. Ambient noise as well as disturbances from family members and pets have an adverse effect and can lead to data entry errors. Inadequate lighting or poor ventilation is also often a problem.

2.4 Unsafe transport of data media and documents

During transport between the organisation and the home workplace, documents or data media can be stolen and lost. Sensitive data may be accessed, read, or tampered with by unauthorised persons. Significant loss of confidentiality can occur if unencrypted data media fall into the wrong hands.

2.5 Unsafe disposal of data media and documents

If a home workplace does not have the conditions in place to safely dispose of data media and documents, they can end up as household waste. An attacker could then gain valuable information that can be used to carry out targeted cybercrimes against the organisation (for example, fraudulent letter writing) or extortion attempts. In more severe cases, the consequences can threaten the entire organisation, for example, if the attack results in the loss of important orders or the disruption of partnerships.

2.6 Manipulating or tampering with IT equipment, data, or software

Tampering with IT equipment in the home workplace is much more likely than on the organisation's premises. Data manipulation is also easier at a remote location because there are no security measures in place in the office premises and no colleagues to spot and prevent data manipulation or equipment tampering.

2.7 Risk of theft in the home workplace

The home workplace is usually not as well protected as the premises of an organisation. A private home may not have the security features of an office, such as security doors, security services, or security cameras. Therefore, the risk of unauthorised access at home is much higher than on the office premises. Intruders tend to first steal expensive items and items that can be sold quickly and easily. IT equipment falls into this category. As the loss to the organisation is greater than the market value of the equipment, a more knowledgeable intruder will try to reap more by extortion or resale of the data.

3 Measures

3.1 Life cycle

Operation

INF.8.M1	Security of documents and data media in the home workplace
INF.8.M2	Secure transport of documents and data media to the home workplace
INF.8.M3	Protection against unauthorised access to the home workplace

Planning

INF.8.M4	Correct organisation of the home workplace

Replacement

INF.8.M5	Secure disposal of confidential data

Additional advanced measures

INF.8.M6	Safe handling of work documents with high protection requirements

3.2 Key measures

INF.8.M1 Security of documents and data media in the home workplace

a. Work documents and data media are protected from unauthorised access in the home workplace.
b. Data media containing sensitive data are encrypted.
c. The work room is locked when away from the workplace. If the room cannot be locked, documents and data media are kept in a locked cupboard or desk drawer.
d. The screen of the display is locked when the employee is absent from the workplace for short

periods, and the computer is locked when the employee is absent for long periods.
e. The employee keeps the home office tidy and the desk clean of excess papers and documents.

INF.8.M2 Secure transport of documents and data media to the home workplace

a. Procedures are in place for the handling of the organisation's documents and data media, which specifies:

- what materials may be transported and by what means (mail, courier, etc.);
- what security measures are applied during transport (appropriate packaging, labelling, etc.);
- which materials may only be transported by hand;
- what data is backed up before transport.

b. Data on digital data media is encrypted before transport.
c. Where possible, the removal of single copies of documents from the organisation's premises is avoided.
d. Procedures for the handling of documents and data media are made known to employees. Employees comply with the established procedures.

INF.8.M3 Protection against unauthorised access to the home workplace

a. Employees are informed which intrusion and access protection measures are mandatory in the home workplace and what the employee's responsibilities are.
b. Appropriate intrusion protection measures (for example, security doors and windows, security door locks) are in place in the home workplace.
c. When the employee is not in the home workplace, the windows of the work room are closed and the doors locked.

3.3 Standard measures

INF.8.M4 Correct organisation of the home workplace

a. Where possible, the home workplace is located in a room with a lockable door, separate from the living quarters.
b. The furnishings and fittings of the home workplace are chosen with due regard to ergonomics, health, and occupational safety.
c. At the home workplace, the organisation's general requirements for the workplace and working environment are complied with.

d. The computer screen is positioned in such a way that light is not reflected directly from the screen and that unauthorised persons cannot see the screen from behind the employee.
e. The home workplace is adequately equipped for the specific tasks, with the necessary tools provided by the employer.

3.4 Advanced measures

INF.8.M5 Secure disposal of confidential data (C)

a. Procedures are in place for the disposal of confidential data. Disposal of data in the home workplace follows the procedures established by the organisation.
b. Data is securely erased from reusable data media. Disposable data media are mechanically destroyed upon disposal (see CON.6 Data erasure and destruction).
c. The home workplace has the necessary facilities for the secure disposal of materials.
d. Sensitive documents and data media containing sensitive data are stored in a locked storage area, protected from unauthorised access, prior to disposal.

INF.8.M6 Safe handling of work documents with high protection requirements (C-I-A)

a. The handling of work documents with high protection requirements is normally carried out at the main workplace, and the issuing of materials for working at home is avoided.
b. If, exceptionally, an employee uses work documents with high protection requirements in the home workplace, stricter security measures than normal are applied to the home workplace.
c. Lockable cupboards and drawers in the home workplace are appropriate to the protection requirements of documents and data media.

INF.9 Mobile workplace

1 Description

1.1 Purpose

To provide the organisational, technical, and personnel measures applicable to the mobile workplace that are considered and implemented when employees work in off-site workplaces instead of on the organisation's premises.

1.2 Responsibility

The information security manager is responsible for compliance with mobile workplace measures. **Additional responsible persons:** The IT department, the employee, the human resources department, the administrative department.

1.3 Limitations

For the security of mobile IT systems, data media, and documents, the system-specific modules SYS.3.1 Laptops, SYS.3.2 Smartphones and tablets in general, SYS.4.5 Removable data media, NET.3.3 Virtual private network (VPN), and SYS.2.1 Client computer in general are considered. This module is complemented by the permanent remote working measures from the module OPS.1.2.4 Remote work. Security measures for the home workplace infrastructure are covered in module INF.8 Home workplace.

2 Threats

2.1 Absence or inadequacy of regulations

If mobile working in an organisation is not governed by regulations, employees may inadvertently leak confidential information because they are not aware of their obligation to use security measures. For example, information may fall into the wrong hands in the course of unsafe communication. An attacker can use leaked inside information to launch attacks against the organisation.

2.2 Adverse environmental impacts

Mobile devices and data media are used in a wide range of environmental conditions. IT equipment can be damaged by excessively high or low temperatures, dust, or humidity. Mobile devices can fall and break. In addition to the physical environment, there are also threats from the technological environment and the associated IT infrastructure. Mobile devices may connect to networks with unreliable security. Mobile devices can be connected to additional devices, not all of which may be secure. This can lead to malware being transferred to the mobile device or sensitive data being copied from the device.

2.3 Tampering with or destroying IT equipment, supplies, and systems in a mobile workplace

Portable IT equipment, supplies, and systems can generally be more easily tampered with or destroyed than those on the premises of an organisation. The mobile workplace is accessible to unauthorised persons and cannot be subject to centrally controlled security measures (for example, surveillance service). The destruction or loss of a mobile device will result in disruptions in the employee's work, as access to the organisation's IT systems will be temporarily unavailable. Replacing mobile devices is also a significant cost to the organisation if there are many mobile workplaces.

2.4 Restricted employee availability

In most cases, the mobile device is not continuously connected to the organisation's internal network. It is also difficult to achieve this when located outside the organisation. The flow of information is slowed down. Even if information is transmitted by email, it is not certain that the mobile employee will read the email in the near future. The impact of limited availability can be significant, depending on the situation and the organisation.

2.5 Unsafe transport of data media and documents

During transport between the organisation and the mobile workplace, documents or data media can be stolen and lost. Sensitive data may be accessed, read, or tampered with by unauthorised persons. Significant loss of confidentiality can occur if unencrypted data media fall into the wrong hands.

2.6 Unsafe disposal of data media and documents

If a mobile workplace does not have the conditions in place to safely dispose of data media and documents, they can end up as household waste. An attacker could then gain access to valuable information that can be used to carry out targeted cybercrimes against the organisation (for example, fraudulent letter writing or extortion attempts). In more severe cases, the consequences can threaten the entire organisation (for example, if the attack results in the loss of important orders or in the disruption of partnerships).

2.7 Loss of data confidentiality

It is significantly easier for an attacker to access data on a hard disk, on a removable or paper data medium in a mobile workplace than in an office. It is also possible to intercept communications. Exposing such data or using it to launch an attack can have significant consequences for the

organisation. A data leak could result in a breach of the law (for example, through the disclosure of personal data) or an unfavourable competitive situation.

2.8 Theft or loss of data media and documents

A mobile workplace is not as well protected as the workplace on the premises of the organisation. The theft of IT equipment or documents on a train, from a hotel room, or from a conference room outside the organisation is much more likely than from an office room with an access control system and co-employees. An employee may lose the mobile device (for example, forgetting it in a taxi).

3 Measures

3.1 Life cycle

Planning

INF.9.M1	Criteria for the suitability of a mobile workplace
INF.9.M2	Regulations for the use of mobile devices
INF.9.M7	Legal framework conditions for mobile work
INF.9.M8	Establishment of security requirements for mobile workplaces

Operation

INF.9.M3	Protection against unauthorised access
INF.9.M4	Procedures for working with an external IT system
INF.9.M5	Reporting the loss of a mobile device
INF.9.M12	The use of screen filters

Disposal

INF.9.M6	Secure disposal of confidential information

Implementation

INF.9.M9	Encryption of mobile devices and data media

Additional advanced measures

INF.9.M10	Implementation of anti-theft measures
INF.9.M11	Prohibition of mobile work in unsafe conditions

3.2 Key measures

INF.9.M1 Criteria for the suitability of a mobile workplace [IT department]

a. The organisation sets requirements that the mobile workplace must meet.
b. The employee complies with the requirements set by the organisation.
c. The employee is aware of the conditions under which mobile working is completely prohibited.

INF.9.M2 Regulations for the use of mobile devices [human resources department]

a. There are regulations in place on the use of mobile devices which state:
- what data may not be handled outside the organisation;
- under what conditions the mobile employee can access the organisation's resources;
- the security measures to be implemented on the mobile device (including acceptable authentication methods);
- what data is encrypted and how;
- the procedures for the use of personal mobile devices at work;
- the requirements for the secure and well-managed use of mobile devices;
- how to prevent the loss or theft of mobile devices;
- the procedures for the acquisition and cost accounting of mobile devices;
- how the maintenance and management of mobile devices and their applications are organised;
- how to dispose of mobile devices securely.

b. All users of mobile devices are familiar and comply with the regulations on the use of mobile devices.

INF.9.M3 Protection against unauthorised access [administrative department, employee]

a. Users of mobile workplaces are aware of the threats of theft and unauthorised access and know how to implement security measures in the mobile workplace.
b. Mobile devices are not left unattended.
c. When leaving the mobile workplace for a short period of time, the windows are closed and the door is locked (for example, in a hotel room). If the door cannot be locked (for example, on a train), documents and mobile devices are kept in a secure place.
d. When leaving the room for a short period, the screen of the IT device is locked so that work in progress can only be resumed after successful authentication.

INF.9.M4 Procedures for working with an external IT system [IT department, employee]

a. Procedures are in place for the professional use of IT systems outside of the organisation (Internet caf', office computer of the visited enterprise, etc.).
b. All mobile employees are aware of the risks of using an external IT system.
c. There is a clear definition of what data may and may not be processed on external IT systems.
d. Temporary data (for example, automatic storage of usernames and passwords in the browser) created during work is deleted from the computer when work is completed on an external IT system.

3.3 Standard measures

INF.9.M5 Reporting the loss of a mobile device [employee]

a. Employees have the obligation to report to the organisation the loss or theft of documents, mobile devices, or data media as soon as possible.
b. The organisation designates specific reporting channels and contact persons for reporting the loss.
c. Whenever possible, remote lock, remote erasure, or device locator functions are used following the loss of a mobile device.
d. When a lost mobile device is recovered, it is ensured that the device has not been tampered with in the meantime. In case of suspicion, the device is decommissioned or reloaded with the original operating system and all necessary applications.

INF.9.M6 Secure disposal of confidential information [employee]

a. When outside the organisation or when travelling, the organisation's procedures for the secure disposal of data media are followed.
b. Before disposing of used data media and documents, it is ensured that no sensitive data is present.
c. When travelling, data media containing confidential data are not destroyed wherever possible, but are returned to the organisation where facilities are in place for the secure disposal of the data media (see CON.6 Data erasure and destruction).

INF.9.M7 Legal framework conditions for mobile work [human resources department]

a. Mobile working arrangements comply with labour laws and other applicable legislation.
b. Other important aspects of mobile working (responsibility of the employee, reimbursement of expenses, etc.) are regulated by the employment contract between the employee and the employer and by additional agreements on mobile working.

INF.9.M8 Establishment of security requirements for mobile workplaces [IT department]

a. Based on the general security policy, mobile workplace security regulations are established or mobile device security regulations are supplemented with regulations for the use of mobile devices (see INF.9.M2 Regulations for the use of mobile devices).
b. The mobile workplace security requirements define:
- the agreed data exchange times, the response times;
- the procedures for handling confidential information;
- the procedures for reporting security incidents;
- the permitted and prohibited work equipment;
- the use of screen filters on mobile devices;
- the transport of documents and data media;
- data backup;
- data protection requirements;
- the procedures for the disposal of documents and data media.

c. The security requirements for the mobile workplace are agreed with the relevant sub-units, employees are aware of the regulations, and they are binding for mobile employees.
d. The mobile workplace security regulations are regularly updated.

INF.9.M9 Encryption of mobile devices and data media [IT department, user]

a. Mobile devices and data media are encrypted according to the organisation's procedures (see CON.1 Cryptography concept).
b. When a cryptographic key is used, it is kept separate from the encrypted device or data medium.

INF.9.M12 The use of screen filters [employee]

a. A full-screen filter is used to protect the information displayed on the screen of a mobile IT device used in a mobile workplace.

3.4 Advanced measures

INF.9.M10 Implementation of anti-theft measures [employee] (C-I-A)

a. If the IT device has a functionality to prevent theft or to facilitate the retrieval of the device in case of loss, this functionality is enabled.

b. Anti-theft devices (for example, a cable lock when using a laptop) are used in crowded areas whenever possible.
c. Anti-theft devices are appropriate to the protection requirements of the data.

INF.9.M11 Prohibition of mobile work in unsafe conditions [IT department] (C-I-A)

a. Criteria are in place to prohibit mobile working in unsafe environments.
b. Mobile working is prohibited if the screen of the mobile device cannot be hidden from unauthorised persons.
c. Mobile working is prohibited on public Wi-Fi networks and on those without a password.

INF.10 Meeting, event, and training rooms

1 Description

1.1 Purpose

To set out measures to protect the information processed in meeting, event, and training rooms and the IT equipment in those rooms.
Meeting, event, and training rooms are characterised by the fact that they are mostly used by both employees and visitors, and not only with the organisation's equipment, but also by using IT equipment external to the company.

1.2 Responsibility

The administrative department is responsible for implementing the measures for meeting, event, and training rooms.
Additional responsible persons: The technical department, the IT department, the employee.

1.3 Limitations

Data communication aspects relevant to meeting rooms are covered in the modules NET.2 Wireless networks and NET.4 Communications. Cabling in the rooms is covered by module INF.12 Cabling. Measures for fire safety are covered in module INF.1 The building in general. Security measures related to visitors are covered in module ORP.1 Organisation of information security.

2 Threats

2.1 Absence or inadequacy of regulations

Many security problems arise when employees do not follow or are unaware of the procedures for using the rooms. If employees do not close windows and doors after leaving the training room, an unauthorised person can gain access to the room, damage property, or steal equipment. If confidential information is not removed from the marker or paper board after the meeting, it is freely accessible to unauthorised persons.

2.2 Incompatibility of IT equipment

IT equipment from different manufacturers may use different cabling and connection standards for power supply or for video or audio transmission. Older devices may not have the same connectivity options as newer devices. As a result, IT equipment in the meeting room may not be usable as intended. The problem arises in particular with the use of external devices, for example, connecting a guest's laptop to a fixed projector in the meeting room.

2.3 Threats caused by visitors

As visitors are unaware of the organisation's requirements, there can be no assurance that the data and IT equipment made available to visitors will be used securely by them. Visitors may also gain access to confidential information due to employees' inattention. For example, a visitor looking for the toilet may choose the wrong door and enter the office room with confidential information written on the marker board.

2.4 Loose cables

The users of meeting, event, and training rooms, the layout of the tables, and the use of the rooms may change. It is therefore necessary to change the positioning of the IT equipment installed in the rooms and the cables connected to them. Depending on the location of the connection points in the room (power and data network sockets), cables may be routed through the room, even across walkways. This creates a tripping hazard that can cause damage to people's health and damage IT equipment if the cable is pulled along with the IT equipment.

2.5 Theft

The theft of data media, IT equipment, and other assets in the meeting room will lead to replacement costs. It also means that these rooms cannot be used to their full capacity temporarily. The theft will result in the loss of confidential data that can be used by the thief against the organisation, causing further damage.

2.6 Loss of the confidentiality of information

Due to technical failures, employees' inattention, or ignorance, it is possible that confidential information on data media (for example, hard disk), on removable media (for example, a flash drive or a DVD), on paper, or on a drawing pad on an IT device may be compromised. An attacker will also look for ways to gain access to sensitive information. The leakage of confidential data has significant consequences for the organisation (for example, legal offence, competitive disadvantage, or financial impact).

3 Measures

3.1 Life cycle

Planning

INF.10.M1	Secure use of the meeting, event, and training rooms
INF.10.M4	Secure location of the meeting, event, and training rooms
INF.10.M6	Arranging secure network access

Operation

INF.10.M3	Closing windows and doors
INF.10.M5	Secure installation of power and communication cables

Implementation

INF.10.M7	Secure configuration of training and presentation computers
INF.10.M8	Procedure for the registration of the use of the room

Additional advanced measures

INF.10.M9	Initial configuration of training and presentation computers

3.2 Key measures

INF.10.M1 Secure use of the meeting, event, and training rooms [technical department, IT management]

a. There are established and documented procedures for the use of the rooms, which specify:

- who manages the IT and other systems in the room;
- the conditions under which visitors may use the IT devices provided;
- what network connections and interfaces visitors are allowed to use.

b. Contact details for solving technical problems are available in meeting, event, and training rooms.
c. Equipment in the room is secured and/or protected against theft by appropriate access control systems and anti-theft devices.
d. Prior to the presentation, all unnecessary applications and data connections are closed on the presentation computer to prevent possible accidental data leakage.
e. At the end of the meeting or event, all materials that may contain sensitive information are taken or securely disposed of.
f. The doors of the room are locked when temporarily leaving the event or training room and when there is no supervision.
g. Instructions on fire procedures and evacuation routes are prominently displayed in the rooms.

INF.10.M3 Closing windows and doors [employee]

a. The windows of the meeting, event, and training rooms are locked outside the time of the events, and the doors of the rooms outside the organisation's security perimeter is also locked.
b. When temporarily leaving the meeting, event, and training rooms without direct supervision, the doors are locked and the windows from which the room can be entered are closed.
c. The closing and locking of windows and doors is checked regularly.

3.3 Standard measures

INF.10.M4 Secure location of the meeting, event, and training rooms

a. The design of meeting, event, and training rooms takes into account the threats arising from their location and use.
b. Rooms for visitors are not located in areas of the building where confidential information is regularly handled.
c. The choice of meeting, event, and training rooms and the access routes to them is such that the movement of visitors and the events taking place in the rooms do not interfere with normal operations.
d. Meetings on confidential information are held in meeting rooms identified as suitable for this

purpose and marked accordingly, where measures have been taken to limit eavesdropping (for example, reducing the permeability of walls and doors).

INF.10.M5 Secure installation of power and communication cables

a. Meeting, event, and training rooms have ample power and network sockets for visitors' equipment.
b. If placing loose power or communication cables on the floor is unavoidable, the cables are covered with cable protection tape.

INF.10.M6 Arranging secure network access [IT management]

a. In-room IT systems cannot be connected to the intranet and the Internet at the same time.
b. The visitors' data network is separated from the organisation's local area network. Visitors' IT systems cannot be connected to the organisation's local area network.
c. Unauthorised persons are not able to monitor or eavesdrop on the use of the employees' local area network and data traffic from the meeting room.
d. The electrical power supply for meeting, event, and training rooms is separated from the electrical power supply for other rooms in the organisation from the switchboard.

INF.10.M7 Secure configuration of training and presentation computers [IT management]

a. Training and presentation computers have standard configurations that are minimal and do not contain redundant applications.
b. Prior to the training, IT systems are inspected to ensure that they are configured appropriately for the training.
c. The training and presentation computers are separated from the organisation's local area network.
d. Users' rights are restricted as necessary. Users are not allowed to install software on the computers or copy data from the computers.

INF.10.M8 Procedure for the registration of the use of the room

a. Regardless of the type of use of the meeting, event, or training room, it is possible to verify who used the room and for how long.
b. The organisation has procedures and processes in place to reserve meeting, event, and training rooms in advance.

3.4 Advanced measures

INF.10.M9 Initial configuration of training and presentation computers [IT management] (C-A)

a. When the room is no longer used, all event-related data is removed from the computers and the computer is set to the initial state specified by the type configuration (see INF.10.M7 Secure configuration of training and presentation computers).

INF.11 IT components of vehicles

1 Description

1.1 Purpose

To present the security measures for the organisation's vehicles if the vehicle (passenger car, truck, boat, ship, helicopter, aeroplane, etc.) is equipped with modern IT components.

1.2 Responsibility

The information security manager is responsible for the implementation of the measures of the module 'IT components of vehicles'.
Additional responsible persons: The user, the procurement department, the data protection specialist, the responsible specialist, the IT department, the employee.

1.3 Limitations

The module deals with vehicles in general. For special-purpose vehicles (for example, ambulances, rescue helicopters, military vehicles), additional needs-based safety measures apply.
In addition, measures from module SYS.3.1 Laptops and module groups SYS.3.2 Smartphones and tablets and NET.2 Wireless networks may apply to the vehicle.
The erasure of data in the vehicle's IT equipment before transfer to another user or disposal is covered in module CON.6 Data erasure and destruction.

2 Threats

2.1 Missing or inadequate procedures for the use of the vehicle

If users are not instructed on what data is allowed to be stored in the vehicle's IT system and which devices and how to connect to it (via USB or Bluetooth), sensitive information may remain in the vehicle's IT system. This information may be visible to the next user of the vehicle or to other unauthorised persons (for example, in the case of theft of the vehicle).

2.2 Non-compliance with safety requirements

If users are not aware of the possible consequences of the incorrect use of the controls of a vehicle, the physical safety of persons may be endangered as a result of a user's negligence or ignorance. If someone changes the settings of a ship's navigation and control system without the appropriate authorisation or without informing others, this could result in a shipwreck.

2.3 Unsafe data exchange

In addition to Bluetooth and wireless data interfaces, many modern vehicles have integrated additional data interfaces that are hidden from the user. The vehicle's IT components can exchange information with external parties via the integrated radio interfaces without the user being able to influence this exchange (for example, the eCall system installed in new passenger cars). However, a car can also send detailed data to the car manufacturer about the location of the car, the number of kilometres driven, or the driving habits of the driver. This means that a wide range of personal data can be collected about vehicle users without their knowledge or explicit consent to the collection and processing of such data. Unsafe data exchange interfaces allow data interception and manipulation.

2.4 Unauthorised or unsafe modification of the vehicle

Nobody usually rebuilds a passenger car, but it is a common practice for special purpose vehicles, including watercraft. If the modification is done incorrectly (for example, in the case of special-purpose vehicles, if a specialised company is not involved), even the incorrect placement of an additional cable can lead to significant damage.

2.5 Vehicle theft and unauthorised access

Vehicle remote access systems may contain security weaknesses. An attacker can open the doors of a remotely locked car and start the car without an authentic car key. The risk of intrusion and theft is

higher for vehicles that are often left in unattended parking spaces (in the case of watercraft, in unattended boat harbours).

2.6 Threats related to vehicle maintenance and IT component updates

If the functioning of vehicle IT components is not verified with sufficient regularity, some of them may stop working over time or may only work with partial functionality. This can lead to malfunctions in the use of the vehicle and, in the worst case, an accident.

2.7 Failure to delete user data

In the event of transfer of a vehicle or change of user, there is a risk that the previous user will not delete their data from the vehicle's IT systems. As a result, the next user will know the previous user's phone book, the numbers called, the places of residence and work stored in the navigation application, the addresses entered, and other personal data.

2.8 Unsuitable environmental conditions

Extreme heat or inappropriate humidity conditions can have a destructive effect on the IT components of vehicles. IT systems may stop working and render the vehicle inoperable. In sunny conditions, the interior temperature of the cabin can rise above 70 degrees Celsius, which is well above the recommended operating temperature for lithium-ion batteries.

3 Measures

3.1 Life cycle

Planning

INF.11.M1	Planning vehicle procurements

Operation

INF.11.M2	Proper maintenance and updating of IT components
INF.11.M12	Anti-theft devices
INF.11.M5	Vehicle inventory list
INF.11.M7	Safe use of the vehicle
INF.11.M8	Protection of the vehicle against the effects of the elements

Implementation

INF.11.M3 Information security manuals for vehicles

INF.11.M4 Enforcement of information security regulations for vehicles

INF.11.M9 Ensuring the readiness for use of vehicles

Emergency response

INF.11.M6 Detailed operational instructions

Disposal

INF.11.M10 Procedure for the disposal of vehicles

Additional advanced measures

INF.11.M11 Replacement procedure

INF.11.M13 Protection of the vehicle against harmful external effects

INF.11.M14 Protection of confidential information

INF.11.M15 Protection of vehicle interfaces

INF.11.M16 Fire extinguishing system

INF.11.M17 Separation of the internal network of the vehicle

3.2 Key measures

INF.11.M1 Planning vehicle procurements [responsible person, procurement department, data protection specialist]

a. In addition to the vehicle's intended use, functional requirements, and cost-effectiveness, the procurement of a vehicle is also based on information security and data protection aspects.
b. Information security requirements must be met throughout the life cycle of the vehicle.
c. The vehicle's locking system is sufficiently secure (or the physical security of the vehicle is ensured by other measures).
d. When procuring a vehicle, it is taken into account that many vehicles will transfer operational data to the manufacturer of the vehicle or other third parties.

INF.11.M2 Proper maintenance and updating of IT components [responsible person, IT department]

a. Vehicles and integrated IT components are maintained in accordance with the manufacturer's specifications and maintenance intervals.
b. The installation of IT component upgrades may also take place between routine maintenance works.

c. Over-the-air (OTA) software upgrades are performed in a secure and controlled manner.
d. Vehicle maintenance and repair works are carried out by authorised companies and qualified maintenance personnel.
e. IT components containing sensitive information are removed from the vehicle for the duration of vehicle maintenance or repair works carried out externally.
f. After the vehicle maintenance works and/or the installation of software updates are completed, the proper functioning of the IT components is verified.

INF.11.M3 Information security manuals for vehicles [IT department, responsible person, user, data protection specialist]

a. The data processed in the vehicle (including personal data) is mapped and documented.
b. The data processed in the vehicle (including recordings of in-vehicle conversations) is protected on the basis of data protection requirements. It is determined who has access to this data and under what conditions.
c. It is determined which data may be synchronised with or manually entered into the vehicle infotainment system.
d. It is determined which security measures can be used to protect the vehicle's data communication interfaces.
e. Guidelines are provided on the secure use and management of vehicle IT systems.

INF.11.M12 Anti-theft devices [responsible specialist, employee]

a. The organisation's vehicles are equipped with an anti-theft alarm system and an immobiliser to prevent engine starting.
b. When the vehicle is left unattended, the anti-theft devices are always activated.

3.3 Standard measures

INF.11.M4 Enforcement of information security regulations for vehicles [responsible specialist, IT department]

a. When using vehicles owned by the organisation, the application of appropriate safety measures is made mandatory for all employees and vehicle users.
b. The information security regulations for vehicles are documented, and the employees concerned follow the approved vehicle information security regulations for vehicles.

c. The information security regulations for vehicles are reviewed periodically and updated as necessary.

INF.11.M5 Vehicle inventory list

a. A list of IT components built into the vehicle (for example, the navigation system) and equipment subsequently added to the vehicle (for example, a hand-held radio station) is compiled.
b. The inventory list of the vehicle includes information on the smart device(s) connected to the vehicle IT systems via Bluetooth.
c. The IT components included in the inventory list are accompanied by technical manuals and user guides to assist the user in working with the IT systems.
d. The inventory list is updated as necessary.
e. Periodic inspections are carried out to ensure that the inventory list of vehicles corresponds to the actual situation. During the inspection, the vehicle's infotainment system is inspected to ensure that it is not connected to unauthorised smart devices.

INF.11.M6 Detailed operational instructions [responsible person, user]

a. A detailed code of conduct is drawn up to deal with vehicle emergencies and IT component failures.
b. The emergency and IT component failure procedures are located in an accessible location in the vehicle.
c. A code of conduct is established for responding to vehicle theft or unauthorised intrusion.

INF.11.M7 Safe use of the vehicle [responsible person, user]

a. The organisation establishes procedures for the use of vehicles which specify:
- who may use the vehicle and for what purpose;
- how the parking of the vehicle is arranged;
- the anti-theft devices to be activated when the vehicle is parked (or docked, in case of watercraft);
- the measures for the protection of persons and cargo on board.

b. Persons authorised to drive the vehicle shall:
- hold a valid driving licence;
- be able to operate the vehicle and its IT systems;
- be aware of the security risks involved.

INF.11.M8 Protection of the vehicle against the effects of the elements [user, responsible specialist]

a. Vehicles and the IT components installed therein are adequately protected from the weather.
b. In the event of extreme weather conditions and depending on the type of vehicle, its location, and environmental conditions, the authorised user of the vehicle has the obligation to implement additional protection measures.

INF.11.M9 Ensuring the readiness for use of vehicles [responsible specialist]

a. Before the vehicle is put into service, it is known where the vehicle will be serviced and where the necessary spare parts and consumables for the vehicle are obtained.
b. Adequate stocks of spare parts and consumables for the vehicle are held on site. The availability of consumables is ensured for the lifetime of the vehicle.

INF.11.M10 Procedure for the disposal of vehicles [IT department, responsible specialist]

a. All sensitive data stored in the IT components of the vehicle is securely erased prior to the disposal of the vehicle.
b. The deletion of data in the vehicle is done using a pre-mapped list of IT components (see INF.11.M5 Vehicle inventory list).

3.4 Advanced measures

INF.11.M11 Replacement procedure [responsible specialist] (A)

a. The organisation has a plan of action in the event of an unexpected technical failure or another circumstance that makes the vehicle unavailable for use at the time.
b. For vehicles with a business-critical function, it is possible to find an equivalent replacement vehicle within a reasonable period of time.
c. Each driver is assigned a replacement as necessary.

INF.11.M13 Protection of the vehicle against harmful external effects [responsible specialist] (A)

a. Depending on the type of vehicle, prolonged presence of the vehicle in a location with harmful external influences (for example, interfering radio emissions) is avoided.
b. Appropriate protective measures are implemented against harmful external effects.

INF.11.M14 Protection of confidential information [IT department, responsible specialist] (C-I-A)

a. Vehicles and vehicle IT components are protected against data theft, data manipulation, and unauthorised use.
b. The data protection measures designed by the vehicle manufacturer are implemented and their effectiveness is verified.
c. Where necessary, existing security measures are upgraded (for example, an additional anti-theft alarm system is installed).

INF.11.M15 Protection of vehicle interfaces [IT department, responsible specialist] (C-I-A)

a. All physical external interfaces and data interfaces of the vehicle are protected against unauthorised access and use.

INF.11.M16 Fire extinguishing system [responsible specialist] (A)

a. In addition to the mandatory manual extinguisher, the vehicle is equipped with an autonomous fire extinguishing system.

INF.11.M17 Separation of the internal network of the vehicle [administrative department] (C)

a. The In-Vehicle Network (IVN) is a network of IT components containing user data separated by a security gateway.

INF.12 Cabling

1 Description

1.1 Purpose

To provide measures to protect electrical and communication cabling from faults, interference, and tampering.

1.2 Responsibility

The responsible specialist is responsible for the implementation of the cabling measures.
Additional responsible persons: The technical department, the IT department.

1.3 Limitations

The module deals with cabling in general, the measures in the module apply to both electrical cabling and IT and communication cabling.
For the layout and fire safety of cabling in buildings and premises, additional measures are provided in the module INF.1 The building in general.
The module does not cover the security of active network components (routers, switches, etc.) or wireless networks. The corresponding topics are dealt with in the NET module group.

2 Threats

2.1 Cable ignition

The ignition of a cable can cause considerable damage if it develops into a fire. Further consequences include electrical breakdowns and damage to electrical equipment. The ignition of a cable leads to the release of aggressive gas compounds, glowing combustion, or an open fire. In the event of a cable ignition, the temperature of the surrounding environment does not usually rise sharply, so the risk of carbon monoxide occurs before the ceiling-mounted smoke detectors have time to operate.

2.2 Underdimensioning cabling

Cabling for workplaces, server rooms, and data centres is often designed based only on current needs. As it is often not possible to replace or add cables, the current carrying capacity of the electrical network (for example, for additional servers) is determined by the existing cables. Underdimensioned cables pose a risk of overheating and ignition.

2.3 Inadequate documentation of cabling installation

If the exact location of cables is not known due to inadequate documentation, cables may be damaged by construction works outside or inside the building. Inadequate documentation also hinders the inspection, maintenance, and repair of cables.

2.4 Inadequate security of switchgear

Frequently, distribution boards and power supply cabinets are unlocked and located in freely accessible areas. Insufficient physical security allows anyone to open the distribution cabinets, tamper with the communication cables, or cause power outages.

2.5 Cable damage

In the case of inaccessible and unsafely positioned cables, there is a risk that someone could accidentally or intentionally damage the cables. Damage to a cable can cause data communication problems or cause a short circuit in the cable, which, in turn, damages the connected electrical equipment. The damage may not be immediate, the effects of the outage may be felt over time.

2.6 Voltage oscillation, over- and undervoltage

Voltage oscillations can cause failures and damage to IT systems. Oscillations can range from very short-lived, small events with little to no impact on IT systems to complete outages or equipment-destroying overvoltage. Voltage oscillations can occur anywhere on the electricity network, from the mains of the energy supply company to the power lines connecting local equipment.

2.7 Excessive use of extension cords

The number of sockets permanently installed in a suitable location is often insufficient to connect a large number of devices. To compensate for this, extension cords are used. If the extension cords are not of good quality and do not meet the requirements, they can cause a fire. If several extension cords are connected in series to provide a sufficient number of sockets for the devices, the risk of fire is further increased by overloading the connections.

2.8 Unauthorised connections

Unauthorised and undocumented cable connections between IT systems or other technical components and the use of unauthorised equipment can lead to security problems and malfunctions.

Such unauthorised connections may allow unauthorised access to networks, systems, information, or applications.

2.9 Line interference

The transmission of electrical signals can be affected by electric and magnetic fields in the environment. A special form of line interference is crosstalk. In this case, the interference is usually not caused by the environment, but by the electrical current flowing through the signals transmitted from adjacent lines.

2.10 Interception and manipulation

Interception attacks on lines are a threat to information security. Communication cables are never completely interception-proof. Whether or not a line is actually being intercepted can only be determined by sophisticated measurements. The risk is higher if the communication cabling is located partly outside the protected security perimeter. Manipulation of communication lines is intended to disrupt the operation of information technology and cause financial loss to the organisation.

3 Measures

3.1 Life cycle

Planning

INF.12.M1	Selection of the suitable cable type
INF.12.M2	Cabling design
INF.12.M4	Avoiding ground currents in shields
INF.12.M5	Analysis of cabling requirements
INF.12.M7	Overcurrent protection

Implementation

INF.12.M3	Professional cable installation
INF.12.M10	Documentation and labelling of cabling
INF.12.M11	Documentation of switchgear
INF.12.M6	Acceptance of the cabling
INF.12.M16	Secure protection cabinets

Operation

INF.12.M13 Avoiding the ignition of electrical equipment

INF.12.M9 Fire safety of cables

INF.12.M12 Inspection of electrical installations and connections

Disposal

INF.12.M8 Disposal of excess cables

Additional advanced measures

INF.12.M14 Duplicated power supply

INF.12.M15 Physical security of cabling

INF.12.M17 Duplication of communication cables

3.2 Key measures

INF.12.M1 Selection of the suitable cable type [IT department, technical department]

a. The current carrying capacity of the electrical cables is sufficient and is selected with a margin.

b. The following factors are taken into account when selecting the cable type:

- the surrounding environment (water, soil, gas, light, etc.) and its temperature;
- protection against rodents and cable cutting;
- the cable's tensile strength (for example, when used as an overhead line) and bending radius;
- cable shielding and electromagnetic interference;
- the installation method, the characteristics of the installation route or the cable tray;
- the distance between transmission equipment;
- resistance to attacks;
- the characteristics of the electrical equipment.

c. Electric cables are selected in accordance with the applicable standards, requirements, and regulations.

d. Communication cables are selected with a sufficient bandwidth and transfer rate margin.

e. The reasons for choosing the communication cable type (coaxial, twisted pair, fibre-optic cable) and cable type are documented.

INF.12.M2 Cabling design [IT department, technical department]

a. Prior to the selection and installation of cables, an electrical and communication cabling plan is drawn up, determining the safe layout of cables, distribution points, bushings, and reserve

requirements.
b. The cables, cable ducts, and cable trays also allow for future needs, i.e. the existing cables are able to cope with the increase in consumption capacity and it is possible to install additional cables in the ducts if necessary.
c. If full-size cable trays are not installed immediately, the diameters of wall and ceiling bushings should be designed with a sufficient margin and filled with soft fireproofing material.
d. Wherever possible, cables are installed in locations accessible only from within the organisation.
e. Wherever possible, cables are avoided in walkways and areas with a high fire risk.
f. Communication and electrical cables in the same cable tray are installed in different sections of the cable tray.

INF.12.M3 Professional cable installation [IT department, technical department]

a. The electrical cabling is installed by appropriately qualified personnel.
b. The installer of the cabling ensures that the cables supplied and the materials and fittings required comply with the specification and are not damaged during the installation.
c. At all stages of the work, the contracting authority checks that the requirements for the execution of the cabling are met.

INF.12.M10 Documentation and labelling of cabling [IT department, technical department]

a. The cabling documentation includes cable diagrams, building plans, tray location plans, socket locations, and cable connection drawings of the distribution cabinets.
b. The internal documentation includes, in addition to the documentation on the installation of cables, also records of maintenance and modifications carried out.
c. The labelling of the cables in the documentation is consistent and unambiguous throughout.
d. The use of the internal documentation is limited to operational needs.
e. The cabling documentation distributed externally does not contain sensitive or redundant information.
f. Changes to cabling are documented as soon as possible.
g. The documentation of the cabling and associated network equipment is reviewed at least once every three years.

INF.12.M11 Documentation of switchgear [IT department, technical department]

a. Each switchgear (switchboard) is accompanied by a cable layout diagram for that equipment.
b. The layout diagram is unambiguous to ensure safe maintenance.
c. The documentation of the switchgear is objective and does not indicate the purpose of the lines or present other sensitive information. As an exception, the purpose is indicated on the emergency power supply line.

INF.12.M13 Avoiding the ignition of electrical equipment [technical department]

a. The electrical equipment is inspected by a qualified electrician before being put into service.
b. The use of personal electrical equipment is regulated and subject to established procedures.
c. Household appliances are used only in designated areas.
d. Sockets are installed in existing cable ducts or fixed to the wall.
e. Where the use of extension cords is unavoidable, the following is taken into account:
- only high-quality and inspected extension cords are used;
- the power consumption is in accordance with the specification of the extension cord and does not exceed 3,500 W;
- extension cords are not connected to each other;
- the extension cords do not obstruct people's paths or walkways at the place of use.

f. Fans are cleaned of accumulated dust at least once a year and more frequently if necessary.

3.3 Standard measures

INF.12.M4 Avoiding ground currents in shields [technical department]

a. The power supply cables for the IT components are selected so that ground currents do not interfere with the shielding of the communication cables.
b. The low-voltage network for the IT equipment is installed in a TN-S wiring system (neutral and protection are separated).
c. The spacing, shielding, and earthing of the cables comply with the applicable standards, requirements, and regulations.
d. Regular test measurements of ground currents are carried out.

INF.12.M5 Analysis of cabling requirements [IT department, technical department]

a. To ensure future-proof, needs-based, and cost-effective cabling, the organisation's current needs and long-term development needs are assessed.

b. When designing the communication cabling, an analysis of the requirements for the choice of cable type and construction is carried out, taking into account:

- the bandwidth required in the short term;
- the increase in bandwidth requirements due to the addition of future services and applications;
- the availability, integrity, and confidentiality of data transmission;
- different cables for specific applications (for example, surveillance system, process control);
- separate cables for areas with different needs or protection requirements;
- power requirements of active components from the communication cable;
- the cost of the solution.

c. Based on the results of the requirements analysis, the electrical and communication cabling plan is adjusted (see INF.12.M2 Cabling design).

INF.12.M6 Acceptance of the cabling [IT department, technical department]

a. A procedure and checklist for the acceptance of the cabling is established and documented.
b. The acceptance procedure is only initiated when the installer of the cabling has notified the completion of all works.
c. At the time of acceptance, the contracting authority verifies:

- compliance with the cabling plan;
- the absence of defects;
- the compliance with standards and regulations;
- the actual volume of the installation work and the accuracy of the invoices.

d. The acceptance checklist and the handover acceptance report, duly signed by all parties, are kept as part of the internal documentation of the cabling.

INF.12.M7 Overcurrent protection [technical department]

a. Measures are designed and implemented to protect electrical equipment against overcurrents.
b. The maximum amount of energy caused by overcurrent downstream of each protective device (overcurrent cut-off switch) does not exceed the amount of energy that the downstream electrical equipment (including downstream overcurrent cut-off switch) can withstand.
c. Overcurrent cut-off of electrical systems complies with the applicable standards and regulations.
d. The overcurrent cut-off plan also covers emergency power generators and uninterruptible power supplies.
e. The operation of the overcurrent cut-off switches is verified periodically, and additionally when

events indicating a lack of protection occur. If necessary, the overcurrent cut-off switches are replaced by new ones.

INF.12.M8 Disposal of excess cables [IT department, technical department]

a. Cables that have become unnecessary due to a change of use of the building or for any other reason are completely removed.
b. After the removal of the excess cables, fire barriers are reinstalled in the bushings.
c. Excess cables that can be used for backup are kept in good working order and marked accordingly.
d. There is an up-to-date overview of which cables are currently not in use, disconnected, or removed. Changes in cabling are documented.

INF.12.M9 Fire safety of cables [technical department]

a. The correct type of electrical cables (see INF.12.M1 Suitable cable types) and cable trays of adequate dimensions are selected to prevent the ignition cables.
b. The cable routes are approved by the person responsible for fire safety.
c. Cables are not laid too close together; fire barriers separating the cables are provided where necessary.
d. Adequate air exchange is ensured in the cable trays.

INF.12.M12 Inspection of electrical installations and connections [IT department, technical department]

a. After the installation and periodically thereafter, electrical installations, switchgear, and junction boxes are inspected by an accredited specialist.
b. The inspection is carried out in accordance with the relevant sectoral standards and legislation.
c. During the inspection, it is verified whether:
- the electrical installations have been installed in accordance with the manufacturer's specifications;
- the fire barriers of the bushings have been made correctly;
- the cables are selected according to the permissible amperage, the choice of protection devices, and the configuration;
- connection diagrams are complete and correct;
- warning labels are in place;

• the automatic circuit breaker of the safety switches is functioning.

d. Any deficiencies found during the testing and visual inspection are documented and forwarded to the responsible persons for rectification and identification of the causes.

INF.12.M16 Secure protection cabinets [technical department]

a. To ensure the operational safety of electrical connections and switchgear, electrical and IT equipment is housed in secure and locked protection cabinets.

b. The protection cabinets are arranged according to the protection requirements and fitted with suitable doors, side walls, and locking.

c. Network equipment is housed in equipment racks or protection cabinets.

d. Access to equipment in the protection cabinets is restricted on a professional basis.

e. The total heat dissipation of the equipment in the protection cabinet does not exceed the permissible limit.

f. Adequate expansion space is provided in the cabinets.

3.4 Advanced measures

INF.12.M14 Duplicated power supply [technical department] (A)

a. Two separate lines are used to supply the essential IT components with high availability requirements, coming from different switchgear.

b. Wherever possible, duplicate power cables are installed in separate locations.

c. Automatic monitoring is implemented on both power supply lines, with immediate alarms in case of failure.

INF.12.M15 Physical security of cabling [IT department, technical department] (I-A)

a. Cables and switchgear in public areas and non-traceable building locations are protected against unauthorised access.

b. The cabling is concealed and protected by cable ducts or reinforced mounting pipes.

c. Switchgear is locked and access rights are restricted on a professional basis. Procedures are in place for access control and key management.

INF.12.M17 Duplication of communication cables [IT department] (A)

a. A duplicate communication cable is installed for systems with high availability requirements.
b. The duplicated cables are installed in different risers and cable trays, possibly located in different fire compartments of the building.
c. For systems with high availability requirements, simultaneous external connections to several IT or communication service providers are considered.
d. Where parallel use of cables is not implemented, the condition of duplicated cables is regularly checked.

INF.13 Technical building management

1 Description

1.1 Purpose

Presenting the measures used for the secure design, implementation, operation, and development of the utility equipment and systems of the building or campus (heating, cooling, ventilation, air conditioning, water supply, lighting, fire protection, and weak-current systems). The abbreviated name of the process is TBM (technical building management).

1.2 Responsibility

The technology department is responsible for implementing the measures of technical building management.
Additional responsible persons: The architect, the IT department, the management of the organisation.

1.3 Limitations

The measures provided in the module apply to all buildings which contain utility systems. The security measures of building automation and control systems are discussed in detail in the module INF.14 Building automation and control systems. In the case of automatic utility systems, measures from both modules are applied.
Depending on the infrastructure of the technical management system and the architecture of automatic management systems, further measures from IND and SYS groups are applied, such as

IND.2.1 Components of an industrial control system in general or SYS.4.4 Device in the Internet of Things (IoT) in general.
The technical building management process as a whole is subject to measures from the module groups OPS.1 Own operations and OPS.2 Operations as a service. The security measures applicable to the individuals related to management operations are specified in the modules ORP.2 Personnel and ORP.4 Administration of identity and rights.
The measures for secure remote maintenance of the technical building management system components are described in the modules OPS.1.2.5: Remote maintenance and IND.3.2 Remote maintenance of operational technology components. If cloud services are used in the TBM process, measures from the module OPS.2.2 Using cloud services are added.
The physical security of buildings is covered in the module INF.1 The building in general.

2 Threats

2.1 Lack of requirements for utility systems in the design stage

If no responsible persons are appointed in the design stage and the stage of planning the construction works of the building and the exact need for and layout of the utility systems remains unclear, it is difficult to build utility systems which meet the needs of the contracting entity and are safe. The resulting building will not be aligned with the actual needs of the users.

2.2 Lacking or insufficient technical building management documentation

Technical building management is often delegated to different external service providers. If no specific contact persons have been agreed on and the documentation related to the service and the service level agreements (SLAs) specifying the obligations are insufficient or inaccessible when needed, unnecessary delays arise in an emergency situation. In more severe cases, the failure of a vital utility system or an interruption in the functioning of a utility system may put to risk the lives or health of those in the building.

2.3 Errors made in the interfacing of utility systems

The alarms or automatic notifications generated by utility systems may activate certain operations in other utility systems. If errors have been made in interfacing critical utility systems (e.g. safety automation systems, automatic fire alarm systems) with other systems or if there are failures in the

interfaces, this may result in violations of the law or the lives or health of the people in the building may be at risk.

2.4 Insufficient monitoring of the functioning of utility systems

If the functioning of the utility systems of the building is monitored insufficiently, events which are important from the perspective of security (e.g. leaks of water supply pipes) may not be detected in a timely manner.

2.5 Insufficient management of access rights

If the utility systems of the building are physically separated from the IT systems of the organisation, the management of the access rights of the utility systems is often treated as a separate process.

3 Measures

3.1 Life cycle

Planning

INF.13.M1	Assessment of the condition of the utility systems upon the receipt of a building
INF.13.M2	Defining the competencies required and appointing the responsible persons
INF.13.M4	Security rules of technical building management
INF.13.M5	Designing the technical building management system
INF.13.M6	Concept of technical building management
INF.13.M9	Procedure for using CAFM software
INF.13.M10	Secure management of digital building information modelling (BIM) software
INF.13.M14	Management of the special roles and authorisations of technical building management

Implementation

INF.13.M3	Sufficient technical documentation of a building
INF.13.M7	List of radio frequencies used
INF.13.M8	List of the technical building management objects
INF.13.M12	Secure configuration of a technical building management application
INF.13.M13	Secure interfacing of the technical building management system

Operation

INF.13.M11	Hardening the security of the technical building management process

INF.13.M15	Protection of the technical building management system from malware
INF.13.M16	Management of changes in the technical building management system
INF.13.M17	Secure maintenance and repair works in the buildings
INF.13.M18	Preventive maintenance works in technical building management
INF.13.M19	Monitoring the technical building management system
INF.13.M20	Handling the events of the technical building management system
INF.13.M21	Logging of the technical building management system
INF.13.M22	Testing the technical building management system
INF.13.M23	Monitoring the information on the security vulnerabilities and updates of the technical building management system
INF.13.M24	Secure cloud computing of the technical building management system

Additional advanced measures

INF.13.M25	Testing environment of the technical building management system
INF.13.M26	Validation of digital building information modelling (BIM) software
INF.13.M27	Using private clouds in the technical building management system
INF.13.M28	Secure use of artificial intelligence in technical building management
INF.13.M29	Integration of the technical building management system with the SIEM solution
INF.13.M30	Penetration testing of the technical building management system

3.2 Key measures

INF.13.M1 Assessment of the condition of the utility systems upon the receipt of a building

a. In the event of receiving a new or existing building, the condition, security, and sustainability of the utility systems installed in the building are assessed.
b. Assessment of the utility systems involves checking the integrity, sufficiency, and accuracy of the documentation of the utility systems (e.g. the alignment of the documentation of the manufacturer with the products and product versions used).
c. The conditions of the utility systems and system documentation are mapped and any deficiencies found are eliminated as soon as possible. Action plans are drawn up for making large-scale changes (e.g. the replacement of utility systems).

INF.13.M2 Defining the competencies required and appointing the responsible persons [management of the organisation, architect]

a. As different skills are needed for different fields of technical building management, the rights, obligations, and tasks related to the processes of each field have been defined and documented.
b. The participants and responsible persons of the technical building management (TBM) process have been defined.
c. Where an external partner is involved in the technical building management process (e.g. the owner of an office building), all rights, obligations, tasks, and competencies of the partner are specified in the procurement contract or rental agreement (see OPS 2.3 Outsourcing).
d. Information exchange, reporting, and communication channels have been agreed on and documented between all parties involved in technical building management.

INF.13.M3 Sufficient technical documentation of a building

a. There is construction documentation compliant with the regulation in force for all buildings. Authorisations for use have been issued for the buildings.
b. The documentation of the buildings includes technical documentation. The technical documentation of a building includes information about the following, among other aspects:

- electrical wiring, incl. UPSs and emergency power supply generators;
- communication cables;
- the lightning protection system;
- the sewerage system;
- the heating system;
- the ventilation and air conditioning systems;
- the fire alarm system;
- access systems;
- elevator systems;
- security and surveillance camera systems;
- building automation control systems.

c. At least the following information is documented about each utility system:

- the manufacturer;
- the details of the hardware and software (incl. model and version numbers);
- acquisition dates of the equipment;
- interfaces with other utility or IT systems;
- access rules;
- details of contact persons;

• special requirements (e.g. the requirement for 24/7 availability).

d. The documentation of the buildings, technical building management, and specific utility systems is up to date and available to the authorised person, if necessary.

3.3 Standard measures

INF.13.M4 Security rules of technical building management

a. The organisation has established security rules of technical building management, which are aligned with the general security policy.

b. The security rules form the basis for drawing up the security instructions of the field. The security rules of technical building management involve the following issues:

• implementation of the main tools of technical management;
• automation of processes (incl. the requirements for testing and configuration management);
• the tools and means of automation permitted;
• access management;
• security of data communication;
• use of privileged accounts and rights;
• logging and monitoring.

c. The security rules of technical building management are reviewed regularly and updated, if necessary.

d. All individuals responsible for technical building management are familiar with the security rules and follow them.

INF.13.M5 Designing the technical building management system

a. The current and planned infrastructure of the building and the related processes are taken into consideration in designing the technical building management.

b. At least the following is documented in the course of the designing:

• analysis of the needs (functionality, interfacing with other systems);
• detailed specifications of the requirements (incl. the requirements for technical security and availability);
• implementation plan (the devices and tools required, configuration, users);

c. If there are no detailed requirements, basic requirements are drawn up based on modern technology which may be used in the selection of devices and tools.

d. The implementation plan includes conducting compatibility and system tests of the utility systems before using external services or purchasing hardware or software (see INF.13.M22 Testing of utility systems).
e. Before the deployment of artificial intelligence in technical building management, the security of the solution is verified (e.g. by consulting the manufacturer and reading about actual usage cases).
f. The planning involves taking into consideration all the requirements specified in the security rules of technical building management (see INF.13.M4 Security rules of technical building management).

INF.13.M6 Concept of technical building management [architect]

a. The planning of and security requirements for technical building management are included in the concept of technical building management.
b. The concept of technical building management includes at least the following:
- description of the processes of technical building management;
- the methods and tools for technical building management;
- the rules for managing access rights and information exchange;
- network segmentation and the security of information exchange in the network;
- monitoring of operations, logging of events, and automatic notifications;
- administration access and the security thereof;
- notification changes in the case of failures and security incidents (incl. notification by email or text messages);
- information exchange with the processes and IT systems of another field;
- integration of the technical building management process with the general emergency response of the organisation.

c. The technical building management concept is validated and updated regularly, if necessary.
d. Compliance with the technical building management concept is inspected regularly. The inspection involves making sure that the utility systems are configured based on the technical specifications and are compliant with the principle of management.
e. The results of the inspection are documented and any potential discrepancies are dealt with as soon as possible.

INF.13.M7 List of radio frequencies used

a. All utility systems which use wireless data communication (incl. WLAN, Bluetooth, and mobile data communication) are mapped by the different locations of the organisation. Different frequency

bands and the users thereof are specified in the list of radio frequencies.
b. Any use of wireless data communication is coordinated with the IT department and the operational technology department. There are no conflicts between different devices in the case of the radio frequencies used.
c. The alignment of the list of radio frequencies with the actual situation is checked regularly and the list is updated, if necessary.

INF.13.M8 List of the technical building management objects [architect]

a. The technical building management components are mapped and included in the list of technical building management objects.
b. At least the following information is described about each object:
- the details of the manufacturer;
- the details of the hardware and software;
- the information exchange interfaces;
- regulation of access;
- scheduled maintenances and the maintenance cycle;
- contact details of the responsible persons and technical support.

c. All components of the technical building management infrastructure are also included in the list.

INF.13.M9 Procedure for using CAFM software [architect]

a. Building resource management software (Computer Aided Facilities Management, CAFM) is only used under the conditions described in the procedure for using the software.
b. Only authorised persons have access rights to the CAFM software. This is especially important if the employees of an external partner are also involved in the process.

INF.13.M10 Secure management of digital building information modelling (BIM) software [architect]

a. A BIM execution plan has been drawn up for the implementation of the software for digital building information modelling (BIM).
b. The BIM execution plan includes at least the following information:
- description of the BIM software used;
- the roles and users related, the obligations of the users;

• integration of BIM with other systems (e.g. CAFM);
• technical specifications of BIM (e.g. software file formats).

c. All BIM data is relevant and up to date.

d. Any delicate BIM information (e.g. the details of the intrusion detection system) can only be accessed by respectively authorised employees.

e. The security of BIM software is assessed before approving the software for use. Deployment of the software is coordinated with the information security manager.

INF.13.M11 Hardening the security of the technical building management process

a. The measures used for hardening the information security process of the technical building management (TBM) process are documented.

b. Hardening of information security includes at least the following:
• monitoring the information security requirements and recommendations of the manufacturer;
• secure password management;
• use of secure protocols;
• deactivation of unnecessary protocols, interfaces, and services;
• installation of security updates.

c. The manufacturer must ensure security updates for a technical building management application until the end of the expected service life of the application.

d. A TBM application with known security vulnerabilities is removed from use. If this is not possible, the technical building management application is separated from the remaining IT systems by network segmentation.

e. The functioning of the security measures of TBM is checked regularly. If necessary, the existing information security measures are changed or new measures are added.

INF.13.M12 Secure configuration of a technical building management application

a. Before the deployment of a technical building management application, the security of the configuration of the application is ensured.

b. Any changes in the configuration are tested and are only installed in the operational environment based on approvals.

c. Back-up copies are made of the configuration of the technical building management applications. The configuration in use before the latest changes made in the application can be restored, if necessary.

d. The restoration of the configuration has been tested in a test system or within the maintenance times allocated for installing system updates.
e. The software updates and configuration changes of the technical building management applications are enforced automatically and as simultaneously as possible on all applications of the same type.
f. All parties concerned (incl. the employees involved with troubleshooting and user support) are notified of an upcoming configuration change, especially if the change in the configuration of a technical building management application concerns access mechanisms or information exchange parameters.
g. In the event of a potential failure, the manager can change the configuration of the application and restart the application.
h. The compliance of the configuration of technical building management applications with the technical specifications is checked as regularly as possible. The results of the checks are documented and any departures from the technical specifications are fixed as soon as possible.

INF.13.M13 Secure interfacing of the technical building management system [architect]

a. If it is necessary to add an application with a limited level of reliability to the technical building management system under justified circumstances (e.g. an application which is no longer supported by the manufacturer), the network traffic of the application is restricted by a firewall to prevent unauthorised access.
b. The technology department is responsible for the general security of the components of the technical building management system.

INF.13.M14 Management of the special roles and authorisations of technical building management

a. Measures from the module ORP.4 Administration of identity and rights are applied in designating the roles in the technical building management system and granting rights.
b. Only a minimum number of access rights of applications are associated with one role.
c. The access of the manufacturers of the components of the technical building management system and the external maintenance partners is as limited as possible (if possible, only read-only access is permitted).
d. The roles of technical users (i.e. the roles for communication between devices) are documented. Any unnecessary technical users are deactivated.

INF.13.M15 Protection of the technical building management system from malware

a. In order to protect the technical building management system, measures are applied from the module OPS.1.1.4 Protection against malware.
b. If it is not possible to use anti-malware software (e.g. if the system does not allow the installation of third-party software or due to limited IT resources), appropriate alternative protection measures are used (e.g. regular backups and restricted access).
c. Before connecting an external data medium to a component of the technical building management system, the data medium is checked for malware.

INF.13.M16 Management of changes in the technical building management system

a. Any changes planned in the technical building management system take into consideration the interests of all parties concerned and are coordinated with all parties (incl. external maintenance and information exchange partners) in a timely manner.
b. Instructions have been drawn up for a situation in which an unsuccessfully implemented change cannot be reversed or if significant efforts would be required for restoring the previous situation.
c. Before implementing a change in the technical building management system, tests must be conducted which include the possibility of reverse-engineering the system. The specifics and depth of the test depend on the complexity of the system and of the number of system components involved (see INF.13.M22 Testing the technical building management system).

INF.13.M17 Secure maintenance and repair works in the buildings

a. A maintenance plan has been drawn up for the regular maintenance of the buildings, which includes the security aspects of the maintenance and repair works, among other things.
b. The persons responsible for the maintenance and repair of the buildings have been appointed.
c. Any maintenance and repair works performed by external partners are coordinated by an employee authorised by the organisation. All maintenance works are coordinated with the technology department in advance; instruments of delivery and receipt are drawn up for receiving the works.
d. The maintenance and repair works performed in the buildings are documented.

INF.13.M18 Preventive maintenance works in technical building management [architect]

a. Maintenance intervals have been defined for the regular maintenance of the components of the technical building management system.

b. Maintenance works involve checking whether the components of the system function within the ranges of the parameters defined and identifying any components, the useful lives of which are about to end.

INF.13.M19 Monitoring the technical building management system

a. Preliminary analysis involves identifying which components of the technical building management system can be included in the common monitoring system and which indicators will be observed in the course of monitoring.
b. Regular checks are conducted to assess whether the systems monitored and the indicators observed are up to date and sufficient.
c. Status messages and other monitoring information is only sent via secure communication channels.

INF.13.M20 Handling the events of the technical building management system [architect]

a. The events of the technical building management system are classified based on the weight of the event (incl. potential impact).
b. Threshold values of indicators have been established for the automatic classification of events.
c. Depending on the weight of the event, notification paths have been defined and the procedure for responding to the event agreed on.

INF.13.M21 Logging of the technical building management system

a. All events of the technical building management system which are classified as significant (incl. all security events) are logged as specified in the module OPS.1.1.5 Logging.
b. All logins by using a privileged account and changes in the configuration of the components are logged.
c. The log data of the technical building management system is stored in the central log server.
d. Secure communication channels are used to send the log data.
e. Any critical security events are reported to the managers responsible automatically.

INF.13.M22 Testing the technical building management system [architect]

a. The technical building management systems and the functioning of the management processes are tested at least before deployment of the system and after enforcing significant changes in the system.

b. The testing of the technical building management system for non-functional requirements also involves testing for compliance with the information security requirements. At least the following information security requirements are tested:

- observing the rules for the complexity of the passwords of the user accounts;
- replacement of default passwords upon the deployment of the system;
- the security of network protocols and technologies;
- the use of encryption (if possible and necessary).

c. The chosen test stories and test results are documented.

INF.13.M23 Monitoring the information on the security vulnerabilities and updates of the technical building management system

a. The managers are constantly monitoring the information on the known vulnerabilities of the technical building management system and on any hardware or software security updates issued.
b. The components of the technical building management system are configured with the aim of minimising taking advantage of the known vulnerabilities, as well as any damage caused by potential incidents.
c. Security checks and scans are conducted to detect the security vulnerabilities of the system. Potential accompanying technical interruptions are also taken into consideration in the case of conducting a security scan of the technical building management system in the production environment (e.g. employees are notified of conducting the test in advance).

INF.13.M24 Secure cloud computing of the technical building management system [architect]

a. If technical building management systems are implemented in the form of a cloud service, the measures specified in the module group OPS.2 Operations as a service are observed.
b. The model of the cloud service and the service provider are selected based on the applicable security requirements and regulations.
c. Irrespective of the location of the information of the technical building management system, the organisation has full control over the building information.
d. The security aspects related to the service are specified in the contract concluded with the service provider.

3.4 Advanced measures

INF.13.M25 Testing environment of the technical building management system [architect] (C-I-A)

a. Technical building management systems are tested in the test environment before deployment in the operational environment.
b. If there is no testing environment, there are procedures for the efficient handling of any failures or errors of the hardware or software added to the operational environment and for quick recovery of the situation before the changes were made.

INF.13.M26 Validation of digital building information modelling (BIM) software [architect] (C-I-A)

a. If a digital building information modelling (BIM) software includes information which is significant for security, the architecture, implementation, and operation of BIM are subject to further security measures.
b. The further security measures of BIM may include the following:

- more detailed rules for distributing roles and authorisations;
- secure authentication methods (e.g. multifactor authentication);
- data encryption;
- network segmentation;
- detailed logging of BIM events.

INF.13.M27 Using private clouds in the technical building management system [architect] (C-I-A)

a. Technical building management systems are assembled into a private cloud of a reliable cloud service provider. An internal private cloud may also be used.
b. No data of the technical building management system is located in a public cloud.
c. Before using an external cloud service provider, the organisation makes sure that the security level of the service is compliant with the security requirements of the organisation.
d. If necessary, the service provider can be replaced. The respective procedure is described in the contract concluded with the cloud service provider.

INF.13.M28 Secure use of artificial intelligence in technical building management (C-I-A)

a. The components using artificial intelligence, the functionalities thereof, and the operating principles are documented.
b. The security of any artificial intelligence used in technical building management is proven; for example, the AI functions may be tested under and increased load and with faulty input parameters.
c. Before the deployment of AI, it is made sure that the data of the organisation will not be processed by unauthorised parties (e.g. the data is not sent to the server of an external service provider for analysis).
d. The regulations in force are observed in the case of using cloud-based artificial intelligence.

INF.13.M29 Integration of the technical building management system with the SIEM solution [IT department] (C-I-A)

a. If there is a security information and event management (SIEM) solution, the events of the technical building management system are included in the SIEM solution.
b. The events of the TBM process are analysed in real time with the events and log information of other IT systems.

INF.13.M30 Penetration testing of the technical building management system [architect] (C-I-A)

a. Penetration tests are conducted to check the level of security of the technical building management system and the infrastructure supporting the system.
b. Penetration tests are carried out in the testing environment before the deployment of the TBM system, as well as after executing significant system changes.
c. Penetration tests of TBM systems are only performed in the production environment if it is unavoidable with the testing schedule coordinated with all parties concerned.
d. Penetration tests also involve testing the AI functions of the technical building management system (with the aim of forcing the AI into making incorrect decisions by manipulating the data).

INF.14 Building automation and control systems

1 Description

1.1 Purpose

Presenting the measures for the secure design, implementation, operation, and development of building automation and control systems (BACS). BACS includes the functions which are related to controlling, automating, operating, and increasing the user convenience and energy efficiency of the functions of a building. Utility systems are usually also usable separately, but may be integrated into the central automation system of the building.

1.2 Responsibility

The technology department is responsible for the implementation of the security measures of building automation and control systems.
Additional responsible persons: Architect, IT department.

1.3 Limitations

The measures provided in the module apply to all buildings which contain utility systems interfaced to a building automation and control system. The module also includes information security aspects related to the network and network components of a building automation and control system.
The security aspects of technical building management (TBM) (heating, cooling, ventilation, air conditioning, water supply, lighting, fire protection and weak-current systems) are discussed in module INF.13 Technical building management.
The physical security of buildings is covered in module INF.1 The building in general.
If the building automation and control systems belong to an external partner (e.g. in the case of renting an office building or premises), further measures from module OPS.2.3: Outsourcing are implemented.
Building automation and control systems used in an operational technology environment are subject to measures from the IND module group (e.g. IND.2.3 Sensors and actuators and IND.2.7 Safety automation).
General measures of network security are described in module NET.1.1 Network architecture and solution, the security of network components is discussed in module group NET.3 Network components.
Measures for the secure remote maintenance of the components of a building automation and control system are described in modules OPS.1.2.5: Remote maintenance and IND.3.2 Remote maintenance of operational technology components.
If the data of a BACS is processed in a cloud, further measures are applied from module OPS.2.2 Using cloud services.

2 Threats

2.1 Insufficient design of a building automation and control system

Any mistakes made in the designing of a building automation and control system may result in material and financial damage. Damage may arise from the BACS not functioning as expected (e.g. failing to register an alarm message sent).

2.2 Errors made in interfacing utility systems with the building automation and control system

The alarms or automatic notifications generated by utility systems may activate operations in other utility systems. If errors have been made in interfacing critical utility systems (e.g. safety automation systems, automatic fire alarm systems) with other systems or if there are failures in the interfaces, the lives or health of the people in the building may be at risk.

2.3 Using insecure system components or communication protocols

The components of the utility systems controlled by the building automation and control system may be depreciated or no longer equipped with software updates due to the expiry of manufacturer support. Security vulnerabilities make open the system to attacks. As granting access rights to utility systems cannot be managed centrally, there is a risk of unauthorised persons gaining access to the system. The protocols used in the data communication between system components which have not been updated are often outdated and may also include security vulnerabilities.

2.4 Improper configuration of the building automation and control system

A building automation system which has been configured incorrectly or without considering all potential situations may cause failures or interruptions in business processes, result in direct material damage, or put to risk the health of those in the building.

2.5 Manipulation of the interfaces between the components of the building automation and control system

Manipulation of the data connection between the components of the building automation and control system or the generation of false messages may cause erroneous processes in the building automation and control system. For example, an alarm from a manipulated fire alarm system may

cause the automatic opening of all doors, which will allow unauthorised persons to enter the building undetected.

2.6 Insufficient security of the access to the building automation and control system

If granting access rights to the utility systems is not centrally managed or controlled, the risk of access of unauthorised individuals to the building automation and control system increases.

2.7 Insufficiently secured control panels

If the switches or control panels used for controlling the building automation and control system are not located in a physically protected location, it is possible to physically take over the control of the utility system. For example, by breaking into the room of the person manning the gates, doors or the vehicle access gate can be opened.

2.8 Insufficiently secured remote accesses

The building automation and control system is often equipped with remote access which is used by the manufacturer or a partner organisation providing product support for providing quick access or for the remote monitoring of the system. If such a permanently open remote access is not sufficiently secured, an attacker may use it to access the building automation and control system and, through this, also the IT systems of the organisation.

3 Measures

3.1 Life cycle

Planning

INF.14.M1	Designing a building automation and control system
INF.14.M7	Security rules of a building automation and control system
INF.14.M8	Technical specifications of the requirements for a building automation and control system
INF.14.M9	Concept of a building automation and control system

Implementation

INF.14.M2	Secure deployment of a building automation and control system
INF.14.M3	Secure interfacing of utility systems with the building automation and control system

INF.14.M4	Peculiarities of interfacing threat identification systems with the building automation and control system
INF.14.M10	Reducing the internal dependencies of a building automation and control system
INF.14.M13	Segmentation of a building automation and control system
INF.14.M19	Allocation of address ranges to a building automation and control system

Operation

INF.14.M5	Documentation of a building automation and control system
INF.14.M6	Separation of the network of the building automation and control system
INF.14.M11	Protection of open accesses and ports
INF.14.M12	Use of secure network protocols
INF.14.M14	Regulating access to a building automation and control system
INF.14.M15	Security of specific networks of a building automation and control system
INF.14.M16	Protection of wireless data communication in the network of a building automation and control system
INF.14.M17	Protection of mobile communication in the network of a building automation and control system
INF.14.M18	Secure information exchange with external building automation and control systems
INF.14.M20	Minimising broadcasting in the network of the building automation and control system
INF.14.M21	Verifying the authenticity of information in building automation and control systems
INF.14.M23	Using sustainable system components
INF.14.M24	Synchronising the clocks of the components of a building automation and control system
INF.14.M25	Monitoring a building automation and control system
INF.14.M26	Logging a building automation and control system

Emergency response

INF.14.M22	Ensuring the autonomous operation of a building automation and control system and utility systems
INF.14.M27	Emergency management of building automation and control systems

Additional advanced measures

INF.14.M28	Physical separation of building automation networks
INF.14.M29	Separation of business-critical utility systems
INF.14.M30	Independent time server of a building automation and control system

3.2 Key measures

INF.14.M1 Designing a building automation and control system [architect]

a. The building automation and control system (BACS) is designed before or concurrently with planning the construction works related to the building (new construction works, extensions or renovation of the building).
b. Designing the BACS involves identifying all utility systems which will be interfaced with the building automation and control system or automated. In addition to the utility systems, the composition of a building automation and control system may also include further sensors and data sources (e.g. an information interface for receiving weather forecasts).
c. At least the following aspects are taken into consideration in the design of a building automation and control system:

- the intended purpose of the building and the requirements arising therefrom;
- segmentation of the building into separate controllable areas;
- organisational requirements and regulations;
- construction-related and technical specifications of the building;
- the utility systems included in the composition of the BACS;
- the environmental conditions affecting the utility systems;
- the BACS technology and architecture used;
- the components of the BACS;
- the communication networks required;
- the network architecture of the building automation and control system;
- interfaces with other systems;
- the data communication interfaces and protocols used;
- the need for regular and uninterruptible power supply (UPS);
- the use of cloud services;
- the requirements for the storage and back-up of data;
- the security measures required;
- the roles required for managing access rights.

d. The BACS is designed so that the number of different technologies, data communication interfaces, and protocols to be deployed is as low and the compatibility of the systems as high as possible.
e. Only secure and standardised protocols and data communication interfaces are used in the building automation and control system.

INF.14.M2 Secure deployment of a building automation and control system

a. A detailed plan is drawn up before the deployment of a building automation and control system for the coordinated interfacing of all utility systems involved with the building automation and control system.
b. It is agreed how and through which data communication interfaces the communication between the administrators of the building automation and control system and the utility systems and the partner organisations providing technical support to the related infrastructure will be taking place.
c. The data communication interfaces of the building automation and control system are documented.
d. In the case of planning internal changes to the BACS system, the documentation of the BACS is updated and all internal and external parties concerned are notified of the upcoming change.

INF.14.M3 Secure interfacing of utility systems with the building automation and control system

a. For all building automation and control systems, utility systems, and the related components, the operations which can be activated by any individual system component and the effect of the activation on other components are defined.
b. Parameter ranges have been set for the critical processes of the utility systems (e.g. the minimum and maximum temperatures of a heating device) which may not be exceeded by the BACS.
c. If the data of a utility system is required for the functioning of the building automation and control system, but the utility system cannot be integrated with the BACS, an alternative solution is found for supplying the data to the building automation and control system.
d. If several building automation and control systems are used in one building, it is defined whether and how information is exchanged between the systems.
e. The peculiarities arising from using different technologies are taken into consideration in interfacing utility systems with the building automation and control system. Utility systems can function autonomously in emergency situations.
f. The functioning of the processes and the data exchange between the system components have been tested thoroughly. Any errors detected in the course of testing are fixed before the deployment of the BACS in the production environment.
g. The interfacing of the utility systems and the building automation and control system is fully documented (see INF.14.M5 Documentation of a building automation and control system).

INF.14.M4 Peculiarities of interfacing threat identification systems with the building automation and control system [architect]

a. The threat identification systems (e.g. the surveillance and fire alarm systems) are interfaced with the building automation and control system so that the functioning or non-functioning of the BACS will not affect the functioning of the threat identification systems. The BACS may use the information received from a threat identification system, but not vice versa.
b. Those threat identification systems which use a network connection or wireless data communication are placed in a physically separated network segment. Only the data communication required for the functioning of the threat identification systems and for the communication of alarms is permitted in the network segment.
c. The threat identification systems function even if a higher-level network connection (e.g. the Internet connection) has been interrupted.

INF.14.M5 Documentation of a building automation and control system

a. The use of, access to, interdependencies, and data interfaces of the components of the building automation and control system used (incl. utility systems and infrastructure components) are documented.
b. There is also documentation about those physical interfaces, data communication interfaces, protocols, and access possibilities of the BACS which have been deactivated.
c. The documentation of the building automation and control system is coordinated with all parties involved and accessible for the authorised employees.
d. The relevance and timeliness of the documentation and the alignment of the actual situation with the documentation are checked regularly. If any differences are found, the cause of the difference is identified and the necessary changes are made.

INF.14.M6 Separation of the network of the building automation and control system [architect, IT department]

a. The network of the building automation and control system is at least logically separated from the office network and from other networks of the organisation.
b. The entire data communication and transfers between the BACS and other IT systems are verified and protected by a firewall. For remote access and external data exchange, it is advisable to create a DMZ (demilitarized zone) of the building automation and control system.

c. If the BACS includes different buildings or campuses, secure wide area network (WAN) connections are used for data communication, for example by using a virtual local area network (VLAN). In a public network, the data connection of the BACS is protected by a virtual private network (VPN).
d. The access of external persons to the components of the BACS is regulated based on the module OPS.1.2.5: Remote maintenance.

3.3 Standard measures

INF.14.M7 Security rules of a building automation and control system

a. The security rules of the building automation and control system are drawn up based on the general security policy and the security requirements for the technical management of buildings (INF.13.M4 Security rules of technical building management).
b. The security rules of the building automation and control system include at least the following security requirements:

- secure interfacing of utility systems with the building automation and control system;
- the required security specifications of the components of the BACS;
- handling of non-compliant components;
- security of the access to the BACS;
- roles of the BACS and secure authentication of users;
- security of the data communication of BACS, incl. requirements for the protocols;
- logging and monitoring of the BACS;
- requirements for the development and testing of the BACS.

c. All employees of the field of building automations have familiarised themselves with the security rules of the building automation and control system and observe the rules in their work.
d. Compliance with the security rules of the building automation and control system is checked regularly and the rules are updated as and when needed.

INF.14.M8 Technical specifications of the requirements for a building automation and control system

a. Specifications of the requirements are drawn up for each building automation and control system based on the security rules of the building automation and control system (see INF.14 M7 Security rules of a building automation and control system). The special requirements arising from the

architecture of the building and the business processes of the organisation are also taken into consideration in drawing up the specifications of the requirements.
b. The specifications of the requirements of the building automation and control system are used in the designing and procurement of the BACS, as well as in the planning and designing of new buildings.
c. The specifications of the requirements for the building automation and control system have been documented. The specifications of the requirements are updated in connection with the development of the hardware and software of the BACS and the overall development of technology.
d. The architecture, structure, and components of the building automation and control system used are compliant with the specifications of the requirements. Compliance is checked regularly.

INF.14.M9 Concept of a building automation and control system

a. The organisation has developed a general concept of the building automation and control system based on the security rules of the building automation and control system and the specifications of the requirements.
b. The concept of the building automation and control system includes all aspects described under the measure INF.14.M1 Designing a building automation and control system and the inclusion thereof is documented. In addition to the technical requirements, organisational requirements are also taken into consideration in the concept of the building automation and control system.
c. The concept describes all utility systems integrated and interfaced with the building automation and control system and the communication links required for interfacing the systems.

INF.14.M10 Reducing the internal dependencies of a building automation and control system [architect]

a. The building automation system is designed so that the functionalities of each area of the BACS would operate as independently as possible from other areas of building automation.
b. The impact of a failure of one of the functions on the BACS on other areas of building automation is minimal.
c. The building automation and control systems of the buildings included in the same campus can be controlled separately.

INF.14.M11 Protection of open accesses and ports [architect]

a. The access to the components of the building automation and control system through USB and network ports and other open interfaces is protected by technical security measures.
b. Connection of any unauthorised or unknown components to the building automation and control system is restricted (see INF.14.M13 Segmentation of a building automation and control system).
c. All connection attempts and successful connections are recorded in the event log of the building's automation and control system.
d. Access to the network is regulated by security mechanisms which are based on the IEEE 802.1X standard or by equivalent security mechanisms. Unauthorised network components cannot be added to the network segments of the building automation and control system.
e. Dongles or locked equipment cabinets are used to restrict unauthorised access to the local interfaces or console ports of the BACS system component.
f. The accesses necessary for the maintenance of the components of the building automation and control system are only opened temporarily, for the duration of maintenance operations.

INF.14.M12 Use of secure network protocols

a. Only secure protocols are used for controlling and maintaining the components of the building automation and control system outside the secured network elements (e.g. HTTPS or FTPS protocols encrypted with an updated TLS version).
b. Ethernet-based data communication outside of secured network elements is encrypted by reliable encryption mechanisms (see NET.3.3 Virtual private network (VPN)).
c. Any data communication interfaces which use insecure protocols have been deactivated.

INF.14.M13 Segmentation of a building automation and control system [architect]

a. The network of the building automation and control system is divided into separated network segments which include individual components of the building automation and control system or the utility system based on the protection requirement.
b. Rules have been drawn up for data communication between the segments. The transfers are at least protected by dynamic stateful packet filtering.
c. Network segmentation is documented in detail.

INF.14.M14 Regulating access to a building automation and control system

a. Administration of access of the building automation and control system is implemented based on the module ORP.4 Administration of identity and rights.
b. The central authentication solution of the building automation and control system administers the access to all important components of the BACS.
c. The system of roles and authorisations of the building automation enables to create users with different access rights based on the needs of the employees of the organisation and the external providers of technical support.
d. All components of the building automation and control system used enable to restrict the unauthorised use of the components.
e. It is prohibited to use any components of the BACS which do not have any access restrictions or the default password of the manufacturer of which cannot be changed.

INF.14.M15 Security of specific networks of a building automation and control system

a. In the case of specific networks of the building automation and control system (e.g. BACnet, KNX, M-Bus), security measures are applied which ensure a security level equivalent to the security level of the network segment (e.g. in the case of BACnet, sufficient security is currently ensured by BACnetSC and TLS 1.3).
b. The gateways of the specific networks of the building automation and control system are configured to only let through the required data communication and use a fixed access control list (ACL).
c. If the building automation and control system includes integrated security mechanisms (e.g. for authentication or encryption of data), those security mechanisms are deployed.
d. Any building automation and control systems with insufficient security mechanisms are replaced as soon as possible from the technical perspective. Until then, they are placed in a network segment separated by a firewall.

INF.14.M16 Protection of wireless data communication in the network of a building automation and control system [architect]

a. Appropriate authentication and encryption mechanisms are applied to protect the data communication of the BACS networks using wireless data communication (e.g. BLE, BACnet Zigbee, EnOcean).
b. The transitions to a cable-based network are executed by using BACS components which are equipped with the firewall functionality.

c. Any wireless data connection networks and the frequency ranges used by such networks are registered. Network devices are configured so that the functioning of other wireless data connection networks is disturbed as little as possible (especially in the 2.4 GHz band).
d. Interference with the propagation of radio waves arising from physical obstacles (e.g. glass surfaces with a metal coating, reinforced concrete walls) are taken into consideration in designing the BACS network.

INF.14.M17 Protection of mobile communication in the network of a building automation and control system [architect]

a. If the BACS uses a public mobile communication network as a data communication channel (e.g. the LTE or 5G mobile communication technology), the communication is limited to authorised parties and designated IP addresses.
b. If it is not possible to separate the BACS networks in a public mobile communication network in any other manner, application level gateways (ALGs) are used to separate the networks.
c. The BACS components only use a public mobile communication network if it is vital for the functioning thereof; mobile communication of BACS components is restricted under normal settings. Instead of a permanent data communication connection, temporary data communication sessions initiated by the BACS components are used.
d. If possible, a mobile communication infrastructure allocated by the mobile communication operator for the data communication of the BACS or a virtual network area which is only designed for automatic devices is used.
e. In the event of using a private mobile communication network which uses autonomous mobile communication technologies (such as the 5G network of a university campus) as the BACS data communication network, the BACS network is separated from other networks and all transitions between the mobile communication network and the network using another technology are protected by a firewall.

INF.14.M18 Secure information exchange with external building automation and control systems

a. Data communication of the building automation and control system with an external BACS system is only possible through specific information exchange interfaces. All interfaces and data communication channels used are documented and approved for use.
b. The parties of the information exchange transaction are authenticated; the data communication is

encrypted.
c. Interfaces with external BACS systems are limited to the minimum extent required.

INF.14.M19 Allocation of address ranges to a building automation and control system [architect]

a. The range of IP addresses allocated for the components of the building automation and control system is sufficient for all BACS components of the organisation.
b. The range of addresses allocated is clearly distinguishable from the IP addresses of the devices of the office network and other IT networks. The address range can be divided into subnetworks, if necessary.
c. The IP addresses of the components of the building automation and control system which use static IP addresses are documented.
d. If the system configurations of the building automation and control system are duplicated, the systems are placed in different network segments to prevent potential conflicts of addresses. Application level gateways (ALGs) or network address translation (NAT) are used for information exchange between systems.

INF.14.M20 Minimising broadcasting in the network of the building automation and control system [architect]

a. In order to reduce the load on the network, measures have been taken in BACS networks to minimise OSI Layer 2 and OSI Layer 3 level broadcasting in the IPx4 network.
b. If broadcasting is necessary from the technical perspective, it should only be directed to the necessary subnetworks. Network segmentation is used to reduce the number of addressees of broadcasting. The senders and recipients of broadcasting are separated from those BACS components which may be disturbed by the broadcasting.
c. Multicast or Unicast routing of data packages is used in the IPx6 network of the building automation and control system.

INF.14.M21 Verifying the authenticity of information in building automation and control systems

a. Input data is constantly validated in the BACS system (whether or not the time, place, value, status, or event displayed is aligned with what was expected).

b. Any data with simulated or 'frozen' values is identified and a respective warning is issued. The further process depends on whether or not the BACS system is critical and on the protection requirement.

INF.14.M22 Ensuring the autonomous operation of a building automation and control system and utility systems [architect]

a. The building automation and control systems must be configured so that the functioning thereof would not depend on any other utility systems or building automation and control systems (e.g. the heating system must continue to operate even if no new information is received from the temperature sensors).
b. If there are, however, some interdependencies between different components of the BACS, measures have been applied to reduce the effects of the interdependence.
c. The utility systems which are integrated with the BACS continue to operate in the event of a BACS failure and continue to fulfil their functions within the parameter ranges established even after a prolonged interruption in the data connection with the BACS system.
d. If the components related to the building automation and control system (e.g. certain IoT components) require uninterrupted Internet connection for functioning, changing or replacing the system should be considered.

INF.14.M23 Using sustainable system components

a. The components of the building automation and control system are designed with a persistence reserve, which means that the system can function for a long time in environmental conditions which are more difficult than the normal conditions.
b. The physical structure of the components of the building automation and control system is durable. If the durability is questionable, further measures are taken to protect the BACS component (e.g. the component is placed in an additional protective box).
c. The BACS components are equipped with assurances given by the manufacturers or certificates issued by independent organisations which prove that the component is compliant with the requirements for physical durability.

INF.14.M24 Synchronising the clocks of the components of a building automation and control system

a. In order to ensure automatic measuring, control, and adjustment, the clocks of the components and utility systems connected to the building automation and control system are synchronised (see OPS.1.2.6 Synchronising clocks with the NTP server).
b. Mutually interfaced building automation and control systems use the same time servers to synchronise their clocks. If the building automation and control system is extended to a campus or several registered immovables, synchronisation of clocks is ensured in all of the buildings involved.
c. All components of the building automation and control system interpret the time in the same uniform standard format (taking into consideration time zones and daylight savings).
d. The building automation and control system is equipped with a local time server which continues to provide time information to the BACS components in the event of an interruption in the connection with the central or higher-level NTP server.
e. SNTP (Simple Network Time Protocol) is not used in the building automation and control system, as this simplified protocol reduces the accuracy of the synchronisation of clocks.
f. In the event of the building automation and control system exchanging time information in real time with utility systems which require high temporal accuracy, using the PTP (precision time protocol) instead of NTP should be considered.

INF.14.M25 Monitoring a building automation and control system

a. All significant components of the BACS are included in the monitoring system. Regular checks are performed to make sure that building automation and control systems are available and that the status parameters remain within the range of the threshold values defined.
b. The monitoring system sends any error messages and departures from the threshold values defined to the managers of the building automation and control system.
c. In the case of any pre-defined events, an automatic alarm message is immediately sent to the responsible person (by a text message, for example). Such events include the following, among others:

- loss of a vital functionality of the building automation and control system;
- failure of a BACS component;
- critical status of the power source (e.g. fluctuating voltage);
- interruption of the network connection.

d. The monitoring data and the BACS status information are only sent via secure data communication channels.

INF.14.M26 Logging a building automation and control system

a. The measures described in the module OPS.1.1.5 Logging are used in the logging of the building automation and control system.
b. The status changes and security events of vital BACS components are also logged.
c. All manual or automatic changes in the configuration of the building automation and control system and the components thereof are logged.
d. It has been defined whether and how the log data of the building automation and control system is sent to the central log server and/or the SIEM (Security Information and Event Management) system.
e. The log data is only sent via secure data communication channels.

INF.14.M27 Emergency management of building automation and control systems

a. The organisation has analysed the impact of an emergency of the building automation and control system on the business processes and the planning of organisation-wide emergency response.
b. The effects of a failure of a single component of the building automation and control system or the outcome of an attack on a single component to all other utility systems and the components of the BACS have been taken to the lowest possible level.
c. An emergency management action plan of the building automation and control system has been drawn up to regulate action in the event of an emergency of the building automation and control system (see DER.4 Emergency management).
d. The emergency management action plan specifies the employees responsible for the functioning of the building automation and control system and the utility systems concerned, as well as the contact details for contacting those individuals.
e. The emergency management action plan describes the measures for ensuring the emergency operation of vital utility systems in the event of an emergency of the building automation and control system.
f. Recovery plans have been drawn up to restore the operation of the vital components of the building automation and control system after an emergency.
g. The reboot sequence including the entire BACS and all utility systems has been defined for recovery after an emergency. The reboot sequence is also documented in the recovery and reboot plans of the system components.

3.4 Advanced measures

INF.14.M28 Physical separation of building automation networks [architect] (C-I)

a. In the case of a higher protection requirement, the networks of the building automation and control systems are executed as physically separate zones (see NET.1.1 Network architecture and solution).
b. Any data exchange between the protected building automation network and the network with a lower protection requirement is restricted to the minimum required level. Access to the Internet from the protected building automation network is blocked.
c. The access of the manufacturer of the building automation and control system or an external maintenance partner to the protected building automation network is strictly regulated.
d. Creating a specialised security operation centre for organising the monitoring and management of network failures or incidents of the isolated building automation network has been considered.

INF.14.M29 Separation of business-critical utility systems (C-I)

a. Business-critical utility systems (with a higher need for protection) are installed in a separate network segment.
b. The data communication of business-critical utility systems is regulated by a Layer 2 firewall installed in front of the network segment.

INF.14.M30 Independent time server of a building automation and control system (I-A)

a. An independent time server which is directly connected to an atomic or radio clock (Stratum layer 0) is used in the network of the building automation and control system.
b. Further time servers of the building automation and control system synchronise their clocks with the central time server of the building automation and control system.

NET: NETWORKS AND COMMUNICATION

NET.1 Networks and communication

NET.1.1 Network architecture and solution

1 Description

1.1 Purpose

To present the information security measures for network architecture and network solutions.

1.2 Responsibility

The architect is responsible for compliance with the network architecture and solution measures.
Additional responsible persons: Information security manager, IT department.

1.3 Limitations

Topics related to network management are discussed in the module NET.1.2 Network management.
The security of the network components is covered in the module group NET.3 Network components.
The measures for network solutions (such as wireless local area networks and storage area networks) are presented in specific modules (e.g. the security measures for the wireless local area network in the module group NET.2 Wireless networks and storage area network measures in the module SYS.1.8 Storage systems).
The measures for private clouds and hybrid clouds are presented in the module OPS.2.2 Using cloud services. The measures for the infrastructure of communication devices are described in the module NET.4.2 IP phone (VoIP).

2 Threats

2.1 Malfunction or inadequate performance of the communication links

An insufficient bandwidth of communication channels or a technical malfunction of communication links could seriously hinder business processes because the use of supporting cloud services would be interrupted. A distributed denial-of-service attack (DDoS attack) that takes advantage of the vulnerabilities of the communication links could make a service that depends on the communication links completely unavailable.

2.2 Inadequate security of the access to the intranet

When the connection between the intranet and the internet is not secure enough (for example, when there is no firewall or it has been configured incorrectly), the attackers might gain access to the sensitive data of the organisation or steal or manipulate it.

2.3 Incompetent design of the network

Network architecture with an insecure design and incompetent expansion of the network help an attacker in gathering information about the network and identifying vulnerabilities. A chaotic topology or rash configuration of the network make the detection of an attacker who has penetrated the network complicated. An attacker could monitor the traffic in the organisation's network while staying invisible inside the network and steal and manipulate data.

3 Measures

3.1 Life cycle

Planning

NET.1.1.M1	Network security policy
NET.1.1.M3	Specification of the technical requirements of the network
NET.1.1.M13	Network design plan
NET.1.1.M16	Documenting the network architecture
NET.1.1.M17	Specification of network solutions
NET.1.1.M22	Guidelines for segmentation
NET.1.1.M25	Detailed plan of the network architecture and solution
NET.1.1.M26	Operating guidelines of the network
NET.1.1.M27	Consideration of the network architecture in the emergency response

Implementation

NET.1.1.M2	Documentation of the network design
NET.1.1.M4	Network zoning
NET.1.1.M14	Construction of the network according to plan
NET.1.1.M10	Demilitarised zone (DMZ)
NET.1.1.M18	Use of the P-A-P structure (packet filter - application level gateway - packet filter) of an internet connection
NET.1.1.M21	Partitioning administrative networks
NET.1.1.M23	Partitioning network segments

Operation

NET.1.1.M5	Partitioning the network segments of clients and servers
NET.1.1.M6	Endpoint segments in the intranet
NET.1.1.M7	Security of sensitive information in the network
NET.1.1.M8	Basic security of internet access

NET.1.1.M9	Secure data exchange with untrustworthy networks
NET.1.1.M11	Security of incoming data traffic
NET.1.1.M12	Security of outgoing data traffic
NET.1.1.M15	Network compliance procedures
NET.1.1.M19	Partitioning infrastructure services
NET.1.1.M20	Subnets IPv4/IPv6 for endpoints
NET.1.1.M24	Logical partitioning of networks with VLAN

Additional advanced measures

NET.1.1.M28	High-availability network and security components
NET.1.1.M29	High-availability implementation of network connections
NET.1.1.M30	Prevention of distributed denial-of-service attacks
NET.1.1.M31	Physical partitioning of network segments
NET.1.1.M32	Physical partitioning of administrative network segments
NET.1.1.M33	Network sub-segments
NET.1.1.M34	Network-based means of encryption
NET.1.1.M35	Implementation of data leak prevention based on the network
NET.1.1.M36	Prohibition of separating a virtual local area network in case of a very high protection requirement

3.2 Key measures

NET.1.1.M1 Network security policy [IT department, information security manager]

a. The network security policy has been established pursuant to the general information security policy. The network security policy presents requirements and guidelines for the secure design and maintenance of the network.

b. The network security policy determines:

- the conditions for segmenting the network and for separating the groups of users and IT systems from each other logically and physically;
- which data connection channels and network and implementation protocols are allowed in specific instances;
- the manner of separating the network management and monitoring from the rest of traffic;
- under which conditions and how the data traffic is encrypted;
- how data exchange is organised with other organisations.

c. Employees responsible for the network management and security are familiar with the network security policy and comply with it.
d. The proposals for amending the network security policy and deviations from the security policy are documented and the information security manager is informed thereof.
e. The compliant application of the network security policy is checked regularly. The results of the inspection are documented.

NET.1.1.M2 Documentation of the network design [IT department]

a. Network design is documented and, as a minimum, includes the following:
a network map that presents the logical structure of the network;
- description of the subnets, zones, and segments;
- changes in the network.

b. The documentation of the network design (including the network map) is kept up to date.

NET.1.1.M3 Specification of the technical requirements of the network

a. The requirements for the network have been developed based on the security policy of the network (see also NET.1.1.M1 Network security policy).
b. When the security policy or business requirements change, the technical requirements specification of the network is updated.
c. When choosing the network architecture and components and implementing the network design, the technical requirements for the network are taken into account.

NET.1.1.M4 Network zoning

a. The network is divided into physically separate zones (constructed of separate devices):
- intranet;
- demilitarised zone (if necessary; see also NET.1.1.M10 Demilitarised zone (DMZ));
- external connections with the internet and untrustworthy networks.

b. The transitions between the zones are protected with firewalls which allow only certain types of data traffic.
c. Untrustworthy networks (such as internet) and trustworthy networks (such as intranet) are partitioned with firewalls that use dynamic packet filters and whitelisting.

d. If the security policy or the specification of network requirements stipulate a special firewall architecture for zoning, then the architecture is implemented accordingly.

NET.1.1.M5 Partitioning the network segments of clients and servers [IT department]

a. Clients (functional units receiving services from a server) and servers are located in different network segments.
b. Data connection between these segments is regulated with a dynamic packet filter. Exceptions specific to applications and systems that allow positioning the clients and servers in a shared network segment are documented.

NET.1.1.M6 Endpoint segments in the intranet

a. A single network segment only contains endpoints with similar security requirements and functionality.
b. Network segments with external access are located in separate zones if the security measures of their endpoints are not sufficient.

NET.1.1.M7 Security of sensitive information in the network

a. Current and secure network protocols or trustworthy and secure communication channels are used for forwarding sensitive data (see also NET.3.3 Virtual private network (VPN)).

NET.1.1.M8 Basic security of internet access

a. Network zones are separated from the internet with a firewall.
b. Internet traffic is directed through the firewall filtering the traffic based on the firewall rules that restrict protocols and network connections.

NET.1.1.M9 Secure data exchange with untrustworthy networks

a. A level of trustworthiness is assigned to each network with which data is exchanged.
b. An unreliable network is considered to be of the same level of trustworthiness as the internet.

NET.1.1.M11 Security of incoming data traffic

a. Access from external IP addresses to the intranet is directed through a secure communication channel and only granted for trustworthy IT systems and users (see also NET.3.3 Virtual private network (VPN)).
b. VPN gateways for incoming traffic are in a separate address room (an external demilitarised zone (DMZ) is recommended).
c. Authenticated access to the intranet through a VPN gateway is granted through the internal firewall.
d. External IT systems cannot gain access to the intranet straight from the internet or the external demilitarised zone.

NET.1.1.M12 Security of outgoing data traffic

a. Data connection from the intranet to the internet is directed through a security proxy located outside the intranet or a central firewall with the necessary capability.
b. When using the P-A-P structure (packet filter - application level gateway - packet filter), the outgoing data connection is directed through the P-A-P security proxies.

NET.1.1.M13 Network design plan

a. A network design plan has been prepared, which is based on the network security policy and the specification of requirements.
b. As a minimum, the network design plan takes into account the following:

- connection with the internet and trusted partner networks;
- the topology of the network, network zones, and its segments;
- dimensioning and duplicating the network and security components, forwarding routes, and external connections;
- the used protocols and their basic configuration (primarily in case of IPv4/IPv6 subnets);
- management and monitoring (see also NET.1.2 Network management).

NET.1.1.M14 Construction of the network according to plan

a. The network has been constructed competently in accordance with the design plan.
b. When accepting the network, its compliance with the design plan is verified.

NET.1.1.M15 Network compliance procedures [information security manager]

a. The compliance of the network with the security policy and the specifications of the network requirements are checked regularly.
b. The responsibility for the compliance checks is assigned and the criteria for the checks are established.

3.3 Standard measures

NET.1.1.M10 Demilitarised zone (DMZ)

a. The organisation has created a physical and/or logical subnet to separate a trusted network from an untrustworthy one, which contains proxies to enable the mutual availability of the servers (a demilitarised zone (DMZ)).
b. The organisation has established the procedure for using demilitarised zones according to the protection requirement of the IT systems and data.
c. The services and applications that are accessible from the internet are located in the demilitarised zone and are protected with the firewall of the demilitarised zone.
d. There could be more than one segment of the demilitarised zone depending on the protection requirement of the IT systems.

NET.1.1.M16 Documenting the network architecture

a. The documentation of the architecture presents all essential components of the network architecture, including:

- the architecture of the intranet, incl. the virtualisation solution;
- the components with the redundancy of the intranet;
- the architecture of external interfaces, including the firewall and the demilitarised zone;
- components of the wide area network and the wireless network;
- the locations and security functions of the security devices (firewalls, systems for intrusion detection and prevention);
- network connection requirements of specific IT systems;
- the architecture of virtualised hosts, including NVO (network virtualisation overlay);
- connections with a private cloud;
- connections with cloud services (see also OPS.2.2 Using cloud services and OPS.3.1 Information security of the service provider);

• the architecture of the components used for the management of IT infrastructure and monitoring.

b. The documentation of the architecture is updated regularly.

NET.1.1.M17 Specification of network solutions

a. The technical design plan of the network is prepared based on the network architecture, which presents the details of the elements of the architecture:

• zoning plan;

• components of the network virtualisation overlay, including virtualised network components;

• security of the wide area network and the wireless network;

• the endpoint connections with the network devices; connections between network elements; communication protocols;

• the redundancy mechanisms of all network elements;

• the principles for addressing, patching, and routing IPv4 and IPv6;

• the security of virtualised hosts;

• the security of private cloud components;

• the statements of the secure management of IT infrastructure and the implementation of monitoring;

NET.1.1.M18 Use of the P-A-P structure (packet filter - application level gateway - packet filter) of an internet connection

a. A two-level firewall system is implemented. An application level gateway based on a proxy or security proxies is used between the firewalls which are connected to the external and internal firewalls by a redundant transition network.

b. The transition network does not contain any other devices besides the application level gateways based on the proxy and the respective security proxies. Any data traffic has been disconnected from the external network by an application level gateway or a security proxy.

c. Direct connection with the application layer firewall (to be configured with the transmission network) has been blocked. The internal firewall has been configured to reduce the internal attacks of the application level gateways and security proxies.

d. The authenticated and trustworthy network accesses from the VPN gateway to the intranet do not pass the application level gateway or the security proxies of the P-A-P structure.

NET.1.1.M19 Partitioning infrastructure services

a. The servers providing basic services for the IT infrastructure are located in a partitioned network segment.
b. The data connection of servers providing services for the IT infrastructure is protected with a dynamic packet filter.

NET.1.1.M20 Subnets IPv4/IPv6 for endpoints

a. The endpoints are distributed into subnets based on whether the devices use IPv4, IPv6, or both protocols.

NET.1.1.M21 Partitioning administrative networks

a. In order to manage the network infrastructure, a communication channel separated from the general data connection (out-of-band management) is used.
b. Administrative workstations used for the management of the network infrastructure are located in a separate network segment.
c. The connection between the administrative workstations and management areas is protected with a dynamic packet filter.
d. The outgoing and incoming data traffic of the administrative network has been restricted with the network management measures to only include the necessary destinations.
e. As a minimum, the administrative networks include the following network segments:
- the segment of IT systems handling rights and the authentication of management connections;
- management of the IT systems;
- network monitoring;
- central logging;
- the IT systems of the main services of the administrative network;
- managed IT systems.
- The management interfaces of the IT systems are protected with a dynamic packet filter.
- The management interfaces of the IT systems are protected with firewalls if the IT systems:
- can be accessed from the internet;
- are only meant to be used in the intranet;
- are themselves a security component between the IT systems accessible from the internet and the intranet.

f. A network cannot be segmented or segments bridged through the management interface of the IT system.

NET.1.1.M22 Guidelines for segmentation

a. Network segmentation guidelines are prepared before the segmentation, which take into account the planned architecture and network design (including the virtualised networks).
b. As a minimum, the segmenting guidelines describe the following:

- the planned network segments, the creation of new network segments, and placing the endpoints in the network segments;
- the segments of development and testing environments;
- the regulation of access to the network from the network segment of client computers;
- wireless connections and specialised communication channels;
- virtualisation hosts and virtual machines;
- the integration of devices servicing several network segments (such as a load balancer);
- security functions of the coupling components between the network segments (such as a firewall with a dynamic packet filter);
- the technical implementation of the network segments.

NET.1.1.M23 Partitioning network segments

a. IT systems with varying protection requirements are located in network segments with differing security levels.
b. When placing IT systems in the same network segment, the security level is determined by the IT system with the highest level of security.
c. The segments are divided into sub-segments based on the parameters established by the segmenting guidelines.
d. Network segments and zones cannot be bridged.
e. If the virtual local area networks (virtual LAN, VLAN) linked to the switch belong to different organisations, then these are partitioned completely or the entire network traffic is encrypted to prevent unauthorised access to the data.

NET.1.1.M24 Logical partitioning of networks with VLAN

a. VLAN cannot be used for connecting with a zone in front of an application level gateway or P-A-P security proxies or the intranet behind them.
b. Bridging to network zones from the VLAN is prohibited.
c. All connections between VLANs go through a firewall.

NET.1.1.M25 Detailed plan of the network architecture and solution

a. A detailed implementation plan is prepared for the network architecture and solution.

NET.1.1.M26 Operating guidelines of the network [IT department]

a. The management procedures for the network are documented in the operating guidelines of the network.
b. The operating guidelines of the network take into consideration the possible peculiarities of the network segments and zones when establishing the IT management procedures.

NET.1.1.M27 Consideration of the network architecture in the emergency response [IT department]

a. When designing a network or prior to important changes in the architecture, the effect of the network architecture on the emergency preparedness of the IT systems is analysed.

3.4 Advanced measures

NET.1.1.M28 High-availability network and security components (A)

a. The essential network and security components of the intranet have a failover capability and are implemented with redundancy.

NET.1.1.M29 High-availability implementation of network connections (A)

a. Network connections (including internet connection) are planned with redundancy.
b. When implementing the redundancy of the data connections of the service provider, the needs and network technology guaranteeing performance that is similar to the data connections are taken into account.
c. When designing network connections, possible threats and unfavourable environmental conditions are taken into account.
d. When using two independent internet service providers (ISPs), it is made sure that both connections would not use the same physical forwarding medium.

NET.1.1.M30 Prevention of distributed denial-of-service attacks (A)

a. In order to reduce the effect of distributed denial-of-service attacks (DDoS attacks), the bandwidth of the network is divided between different users and protocols.
b. For the mitigation of large-scale denial-of-service attacks, the internet service provider (ISP) has been contracted to provide a service for preventing DoS attacks.

NET.1.1.M31 Physical partitioning of network segments (C-I-A)

a. Network segments with different levels of security have been physically separated from each other with switches and/or routers; using only logical partitioning is prohibited.

NET.1.1.M32 Physical partitioning of administrative network segments (C-I-A)

a. The administrative network segments have been physically separated from the main network with switches and/or routers; using only logical partitioning is prohibited.

NET.1.1.M33 Network sub-segments (C-I-A)

a. For the prevention of attacks on endpoints, the network is divided into small sub-segments with a similar requirement profile and comparable security.

NET.1.1.M34 Network-based means of encryption (C-I)

a. The security segments in the intranet, partner network, and demilitarised zone have been established with the means of encryption on the network level, such as VPN technology or technology that is compliant with the security standard IEEE 802.1AE.
b. When data is exchanged in the intranet, a partner network, or a demilitarised zone through an insecure communication channel, the entire data connection is encrypted.

NET.1.1.M35 Implementation of data leak prevention based on the network [information security manager] (C-I)

a. In order to reduce the risk of data leaks, data leakage prevention (DLP) systems are implemented on the network level.

NET.1.1.M36 Prohibition of separating a virtual local area network in case of a very high protection requirement (C-I-A)

a. In the case of a network segment with a very high protection requirement, the use of a virtual private network (VLAN) is prohibited.

NET.1.2 Network management

1 Description

1.1 Purpose

To present the measures for establishing and operating secure network management and guaranteeing a secure data connection.

1.2 Responsibility

The IT department is responsible for compliance with the network management measures.
Additional responsible persons: Architect, director.

1.3 Limitations

The module presents the general measures for network management. The security measures for network components are presented in greater detail in the module groups NET.2 Wireless networks and NET.3 Network components. The management of the network infrastructure is handled in the module layer INF. Access rights management is covered in the module ORP.4 Administration of identity and rights. The logging and archiving of network events (including administrative operations) are described in the modules OPS.1.1.5 Logging and CON.3 Data backup concept.

2 Threats

2.1 Unauthorised access to central network management components

If an attacker gains access to the network management system due to the inadequate partitioning of the network or unpatched vulnerabilities, they can interfere with the functioning of the network by unauthorised reconfiguration (e.g. by redirecting network traffic).

2.2 Unauthorised access to network components

If an attacker manages to gain access to a network component through the network, then they can control and manipulate that component. The attacker can interfere with the data traffic passing the component in question. In addition, the attacker can prepare future attacks.

2.3 Unauthorised interruption of the network management communication

By eavesdropping on and manipulating the network management data connection, the configuration of network components can be changed, and through that, controlled. This could damage the availability of the network. In addition, the attacker can view and save the forwarded information.

2.4 Inadequate synchronisation of the system time of the network components

In case of inadequate synchronisation of the system time of the network components, the log data might not correlate with each other or erroneous event messages might be issued because the time stamps of various events have no common basis. For this reason, it is difficult to react fast to events and rectify problems in time. Security incidents, such as data leaks, might remain undetected.

3 Measures

3.1 Life cycle

Planning

NET.1.2.M1	Planning network management
NET.1.2.M2	Specification of network management requirements
NET.1.2.M11	Guidelines for network management
NET.1.2.M13	Concept of network management
NET.1.2.M14	Implementation plan of network management
NET.1.2.M15	Procedure for the secure use of network management infrastructure
NET.1.2.M16	Secure configuration of network management solutions
NET.1.2.M27	Emergency response of network management

Emergency response

NET.1.2.M6	Regular data backup

Operation

NET.1.2.M7	Event logs
NET.1.2.M8	Synchronising time

NET.1.2.M10	Restricting SNMP communication
NET.1.2.M17	Regular review of network management
NET.1.2.M24	Central configuration management of network components
NET.1.2.M25	Monitoring network components
NET.1.2.M26	Event notifications, alarms, and logging

Implementation

NET.1.2.M9	Security of network management communication
NET.1.2.M12	Network management documentation
NET.1.2.M18	Network management training
NET.1.2.M21	Separation of the network management communication
NET.1.2.M22	Limiting management functions
NET.1.2.M28	Secure location of management workstations in the case of in-band management
NET.1.2.M29	Virtual local area networks (VLAN) in the management zone

Additional advanced measures

NET.1.2.M30	High availability of the management solution
NET.1.2.M31	Secure protocols
NET.1.2.M32	Physical partitioning of management networks
NET.1.2.M33	Physical partitioning of management segments
NET.1.2.M35	Security of evidence
NET.1.2.M36	Interfacing network management logs with security information and event management (SIEM)
NET.1.2.M37	Synchronisation of time covering all locations
NET.1.2.M38	Replacement solutions for network management infrastructure

3.2 Key measures

NET.1.2.M1 Planning network management

a. Network management plans are based on the information security policy, specification of requirements (see also NET.1.2.M2 Specification of network management requirements), the work tasks of network management, and the necessary access rights for the completion of work tasks.
b. As a minimum, the following is covered when planning network management:

- network areas separated for network management;
- access to the management server;

- data connection for management;
- data connection protocols (such as IPv4 and IPv6);
- interfaces for sending event and alarm messages;
- logging, including interfaces for the central logging solution;
- reporting and its interfaces.

NET.1.2.M2 Specification of network management requirements

a. When planning network management, the requirements established for the network management infrastructure and for processes are documented.
b. The requirements for the network management include the requirements for management tools, important network components, and the stages of the network management process.

NET.1.2.M6 Regular data backup

a. The following data is regularly backed up in the network management solutions:
- system data for the managed objects;
- event and network messages;
- logs;
- configuration of the central network management solution.

NET.1.2.M7 Event logs

a. As a minimum, the following events are logged in the network management solution:
- unauthorised or unsuccessful access attempts;
- changes in configuration;
- fluctuations in the network capacity and availability;
- error messages of automatic processes (e.g. when the configuration is propagated);
- availability malfunctions of the network components.

NET.1.2.M8 Synchronising time

a. All network management components and their related network components have their time synchronised and the same time zone is implemented.
b. In all locations of the local area network, the time is synchronised with an NTP service.

c. A separate NTP server is recommended to be included in the management network in case of a separate management network.

NET.1.2.M9 Security of network management communication

a. When the main network infrastructure is used for the data connection of network management, data exchange only takes place using secure protocols.
b. When a special management network is used for data connection, the measures of the module NET.1.1 Network architecture and solution are implemented.

NET.1.2.M10 Restricting SNMP communication

a. Secure versions of SNMPs (simple network management protocols) are used for network management (SNMPv3 in 2020).
b. In the case of insecure SNMP versions that are not protected with a VPN or a TLS, a partitioned management network is used.
c. Access to the data of the SNMP protocol is only allowed to the necessary management servers.
d. When the SNMP protocol is not used for network management, the SNMP is blocked.

NET.1.2.M11 Guidelines for network management

a. Written guidelines have been established for network management; the guidelines are updated if necessary.
b. The network management guidelines stipulate:
- used network services and network management tools;
- network management activities (including all centrally conducted and automated operations);
- security measures for logging, data connection, and regulating access.

c. The employees responsible for the network management comply with the network management guidelines. Compliance with the guidelines is checked regularly.

3.3 Standard measures

NET.1.2.M12 Network management documentation

a. The network management documents describe:
- the managed network components;

- network management means, terminals, and workstations;
- databases and management data related to network management;
- interfaces with external applications and services.

b. The documentation of network management complies with the network infrastructure documentation (see also NET.1.1 Network architecture and solution).

c. The architecture of the network management infrastructure is complete and timely.

NET.1.2.M13 Concept of network management

a. A concept of network management is developed, which determines the following in addition to the contents of the network management guidelines (see also NET.1.2.M11 Guidelines for network management):

- methods and technologies of network management;
- security of data access and data connection;
- network segmentation;
- the location of network management components in security zones;
- the monitoring and operation logs of the network components;
- organisation of alarms;
- automation of network management;
- organisation of malfunction and security incident notifications;
- emergency response for network management.

NET.1.2.M14 Implementation plan of network management

a. A detailed implementation plan of network management is prepared based on the network management concept and network management guidelines.

NET.1.2.M15 Procedure for the secure use of network management infrastructure

a. The secure use procedure of the network management infrastructure is developed based on the network security policy, network management guidelines, and the network management concept.

NET.1.2.M16 Secure configuration of network management solutions

a. The configuration of the network management solution is based on the established requirements (see also NET.1.2.M2 Specification of network management requirements) and network

management concept (see also NET.1.2.M13 Concept of network management).
b. Network management is configured and implemented in a secure manner.

NET.1.2.M17 Regular review of network management

a. The compliance with the requirements for the network management is checked regularly.
b. During the review, the up-to-dateness of the network management documentation, its suitability for the current situation, and actual procedures are checked.
c. In the course of the review, the security and sustainability of the existing network management infrastructure is evaluated.

NET.1.2.M18 Network management training [director]

a. The network management training programme includes configuration management and capacity management and takes into account the peculiarities of the specific network management solution.
b. The network management training programme includes instructions for coping with typical failures and security incidents.
c. Trainings take place regularly. Trainings are organised after any significant technical or organisational changes in the network solutions.

NET.1.2.M21 Separation of the network management communication

a. If possible, granting management access from an external network to the network components is avoided.
b. If access to the network components from the external network without a central management tool is necessary, a separate data connection channel is used.
c. The respective jump servers are a part of the management network and are installed in a separate access segment.

NET.1.2.M22 Limiting management functions

a. Only the necessary management functions are activated; all other functions are blocked.

NET.1.2.M24 Central configuration management of network components

a. The software, firmware, and configuration data of the network components of the management network are shared and installed centrally, automatically, and without causing any noticeable

interruptions.
b. The configurations are stored securely; they are available to the authorised employees if necessary.
c. Configuration management is in line with the processes of version management and backup.
d. The functioning of central configuration management is checked regularly.

NET.1.2.M25 Monitoring network components

a. The availability and performance parameters of essential network components are monitored regularly.
b. In order to evaluate the monitoring results, the threshold values for availability and performance parameters have been established (network baselining).

NET.1.2.M26 Event notifications, alarms, and logging

a. Significant events related to the network components and network management tools are logged in the central management system.
b. Significant events related to the network components and network management tools are automatically reported to the responsible IT staff immediately after the event.
c. As a minimum, the following is logged:
- failure or availability malfunction of network and management components;
- dysfunction of hardware;
- unsuccessful login attempts;
- workload nearing the limit or overload of IT systems.

NET.1.2.M27 Emergency response of network management

a. The emergency response of network management is a part of the general emergency response concept of the organisation.
b. The configurations of the network management tools and network components are backed up and their recovery is added to the recovery plans.

NET.1.2.M28 Secure location of management workstations in the case of in-band management

a. Specialised management workstations are used for managing IT systems in an in-band management network.

b. If an organisation uses systems that can be accessible from the internet as well as the intranet, separate management workstations are customised for their management.

NET.1.2.M29 Virtual local area networks (VLAN) in the management zone

a. When virtual management networks are used, an external packet filter and devices connected to it are located in a separate network segment.
b. The entire traffic passes through an application level gateway.

3.4 Advanced measures

NET.1.2.M30 High availability of the management solution (A)

a. The central management solutions and the network components supporting them are implemented with high availability.
b. The redundancy of important management solution components is guaranteed through the duplication of components, for example.

NET.1.2.M31 Secure protocols (C-I-A)

a. Only secure network management protocols are used.
b. All of the security functions of the network management protocols are in use.

NET.1.2.M32 Physical partitioning of management networks [architect] (C-I-A)

a. The management network is physically partitioned from the rest of the intranet.

NET.1.2.M33 Physical partitioning of management segments [architect] (C-I-A)

a. The management network is divided into management segments with separate network devices.
b. The components of local area networks, the security components, and the components of external connections are managed from different management segments that are physically partitioned with network devices.

NET.1.2.M35 Security of evidence (C-I-A)

a. Due to computer forensics needs, a procedure has been established for archiving the evidence on the network management in compliance with legal provisions and in a manipulation-proof manner (see also DER.2.2 Enabling computer forensics).

NET.1.2.M36 Interfacing network management logs with security information and event management (SIEM) (C-I-A)

a. Logging the network management is linked to the security information and event management (SIEM) solution.
b. The requirements to the network management solutions (see also NET.1.2.M2 Specification of network management requirements) are supplemented by the interfaces and means of transmission of SIEM solutions.

NET.1.2.M37 Synchronisation of time covering all locations (C-I)

a. The synchronicity of device time is guaranteed in all of the locations of the organisation with a common basic time (e.g. according to a higher-level NTP server).

NET.1.2.M38 Replacement solutions for network management infrastructure (A)

a. Efficient alternative solutions exist for the installation and the restoration of the software and firmware configuration of the network components.

NET.2 Wireless networks

NET.2.1 Operating wireless local area networks

1 Description

1.1 Purpose

To present guidelines for the construction and secure operation of wireless local area networks (WLAN).

1.2 Responsibility

The IT department is responsible for complying with the measures for operating wireless local area networks.
Additional responsible persons: Architect, technical department.

1.3 Limitations

The secure use of wireless local area networks is described in the module NET.2.2 Using wireless local area networks. When using the authentication services of wireless local area networks (such as RADIUS), measures from the modules NET.1.1 Network architecture and solution and SYS.1.1 Server in general are also implemented. Measures from the module DER.2.1 Handling of security incidents are implemented for the incident handling of a wireless local area network.

2 Threats

2.1 Failure or malfunction of the wireless local area network connection

The connection of a wireless local area network (WLAN) could be interrupted by other sources of electromagnetic emissions of the same frequency (other devices of the wireless local area network, Bluetooth devices, microwave ovens, other wireless local area networks). Signals with the same frequency can be transmitted to launch a denial-of-service attack, interfering with the use of the wireless local area networks.

2.2 Design errors of wireless local area networks

Errors made when designing a wireless local area network could cause significant vulnerabilities. When local area network standards are used that have known vulnerabilities (for example, a cryptographic key can be easily cracked when using the WEP security algorithm), an attacker could infiltrate the network, eavesdrop on the network traffic, and copy confidential data.

2.3 Absence of the procedure for using a wireless local area network

Without the central management of the wireless local area network infrastructure, it is difficult to guarantee secure configuration in all wireless access points. The default configuration of network devices mostly has deficient security mechanisms and easily identifiable passwords.

2.4 Insecure authentication procedures

Absent or insufficient authentication procedures and mechanisms of the wireless local area network could cause vulnerabilities. For example, some methods of the Extended Authentication Protocol (EAP) described in the standard IEEE 802.1x include known vulnerabilities (for example, the EAP-MD5 is defenceless against man-in-the-middle attacks and dictionary attacks). This means that it is possible to guess user passwords and eavesdrop on the data connections when using EAP-MD5.

2.5 Configuration errors of the wireless local area network infrastructure

The wireless access points and other components of the wireless local area networks (such as wireless LAN controllers) have numerous configuration options, which also include security functions. In case of incorrect configuration, the access point cannot be used for data communication or the access point has a security level that is too low.

2.6 Absent or insufficient security mechanisms of the wireless local area network

The components of the wireless local area network are often pre-configured without activated security mechanisms or the security mechanisms are only partially implemented. Even today, wireless local area network components are used that only support insufficient security mechanisms (such as WEP). Generally, firmware updates improving the security are not available for older devices. An attacker can use a device with a known vulnerability for eavesdropping on the data communication and accessing confidential data.

2.7 Eavesdropping on the wireless local area network communication

The wireless transmission environment cannot be controlled (a shared medium); it can be used by many users at the same time. For this reason, the data forwarded through the wireless local area network can be monitored and saved. If the transmitted data is not encrypted or an insecure encryption mechanism is used, the data can be read. As the area of the wireless network often exceeds the required limits, the owner of the network cannot control or secure the entire network area.

2.8 Simulation of a real access point (rogue access point)

An attacker can pretend to be a part of the wireless local area network infrastructure if they have installed an access point with a suitable network name in the vicinity of the user. Such an access point is called a rogue access point. If a rogue access point sends stronger signals than the actual

access point and mutual authentication is not required, the client's device is going to use the rogue access point as a base station. The user logs into the network which they consider to be the desired network, but the attacker can eavesdrop and record the user's data communication. Often, this method is used for attacking public Wi-Fi networks.

2.9 Unprotected access from an access point to the local area network

When the access points are installed in such a way that they are visible to everyone and have no physical protection, an attacker could add their own device between the access points and switches for eavesdropping on the network traffic. Even using WPA2 encryption for the data communication is insufficient because this method only protects the wireless interface and does not consider Ethernet connections.

2.10 Hardware damage

The functioning of a wireless local area network could be hindered by hardware malfunctions. The wireless network devices that are located outside the security perimeter of the organisation can be intentionally damaged by an attacker. In addition, these devices are vulnerable to the threats arising from the location (such as excess moisture or damage from lighting).

2.11 Theft of an access point

Installing wireless access points to easily accessible or crowded areas (such as on the ceiling above access routes) increase the danger of theft of the devices. An attacker can use the stolen devices to access the shared secret key of the RADIUS server or another key (such as WPA2 Personal) that is saved in the access point which can be used for gaining unauthorised access to the wireless local area network.

3 Measures

3.1 Life cycle

Planning

NET.2.1.M1	Planning wireless local area networks
NET.2.1.M2	Suitable wireless local area network standard
NET.2.1.M3	Secure encryption mechanism

NET.2.1.M10	Security guidelines for the wireless local area network

Implementation

NET.2.1.M4	Secure installation of access points
NET.2.1.M5	Secure configuration of access points
NET.2.1.M6	Secure configuration of the wireless local area network infrastructure
NET.2.1.M7	Secure wireless local area network architecture
NET.2.1.M9	Secure connection of the wireless local area network with a cable network

Emergency response

NET.2.1.M8	Incident handling procedure for the wireless local area network

Acquisition

NET.2.1.M11	Suitable components of the wireless local area network

Operation

NET.2.1.M12	Suitable management of the wireless local area network
NET.2.1.M13	Regular security checks of the wireless local area network
NET.2.1.M14	Regular review of the wireless local area network components

Additional advanced measures

NET.2.1.M15	Protecting the wireless local area network with a virtual private network (VPN)
NET.2.1.M16	Additional security for the connection between the wireless local area network and a cable network
NET.2.1.M17	Security of the access point connections
NET.2.1.M18	The tools for intrusion detection and prevention in the wireless local area network

3.2 Key measures

NET.2.1.M1 Planning wireless local area networks

a. A plan for the implementation of a wireless local area network (WLAN) has been established in the organisation, stipulating:

- the purpose of the wireless local area network and the business processes where it is implemented as well as the additional value of the network;
- the locations of the implementation of the wireless local area network;
- which functions and applications are supported by the wireless local area network;
- which type of data may not be sent via the wireless local area network;

• which security requirements are taken into consideration when operating the wireless local area network.

b. When designing a wireless local area network, the persons responsible for the management of the wireless local area network infrastructure are assigned, the reporting routes are established, and management procedures are developed.

NET.2.1.M2 Suitable wireless local area network standard [architect]

a. In order to avoid failures of the wireless local area network, the number of devices in the planned wireless local area network frequencies (2.4 GHz and 5 GHz) and the wireless channels they use are determined. Other sources of disturbances (Bluetooth transmitters, high-voltage cables, DECT phones) are removed if possible.

b. The most secure standards are selected for the wireless local area network that is supported by devices. The acceptable standards are IEEE 802.11i-2004 (encryption mechanism WPA2) or a more recent version (WPA3). Using WEP and WPA is blocked. The reasons for selecting the standards are documented.

c. When planning a wireless local area network, devices which only support insecure authentication and encryption mechanisms are excluded.

NET.2.1.M3 Secure encryption mechanism [architect]

a. The data traffic of the wireless local area network is protected cryptographically.

b. The use of easily cracked encryption protocols (such as TKIP used with WEP) is blocked. Instead, WPA2 encryption protocols CCMP (used by the AES encryption algorithm) or EAP (extensible authentication protocol) are used.

c. When the WPA2-Personal authentication mechanism is used (WPA2-PSK, Pre Shared Key), a complex key that contains at least 20 characters is used as a password. The key is changed regularly.

d. Authentication mechanism WPA2-Enterprise guarantees better security; in this case, the authentication takes place with a username and password along with the authentication protocol 802.1X and a centrally managed RADIUS server.

NET.2.1.M4 Secure installation of access points [technical department]

a. Wireless access points are not easily accessible for unauthorised persons. If necessary, protective covers and means for preventing theft are used.

b. Measures to prevent the spread of the radio waves outside the required area (such as directional antennas or metal shielding) are used.
c. Antennas and access points in external conditions are protected from the effects of the weather (such as rain or lightning) and electrical interferences. If possible, the use of access points outside the building should be avoided.

NET.2.1.M5 Secure configuration of access points

a. Configuration made by the manufacturer (including network names, passwords, and cryptographic keys) are changed before adding the access point to the network.
b. The network name (SSID) of the wireless local area network meant for internal use does not allow drawing conclusions about the hardware, organisation, service provider, or the purpose of use.
c. Unnecessary protocols, ports, services, and management accesses (such as Telnet or HTTP) are closed or deactivated.
d. When using a DHCP server, means for the detection and prevention of ARP spoofing have been implemented (such as Dynamic ARP Inspection, DAI).
e. Firmware updates and security updates have been installed for the entire wireless local area network infrastructure. The updates are tested before the installation.
f. The access rights to the user account of an administrator are granted based on the principle of least privilege. A local user account has been activated in the access point for emergency response.
g. The communication for the management of access points is encrypted.

NET.2.1.M6 Secure configuration of the wireless local area network infrastructure

a. Measures from the modules SYS.2.1 Client computer in general and NET.2.2 Using wireless local area networks are implemented for the secure configuration of wireless local area network clients.
b. Client devices in separate security zones cannot be connected through the wireless local area network.

NET.2.1.M7 Secure wireless local area network architecture [architect]

a. Access points are linked to the network infrastructure with cables to ensure high availability.
b. The network segments of a wireless local area network are separated from a local area network physically or by dividing the network logically into virtual local area networks (VLANs).

NET.2.1.M8 Incident handling procedure for the wireless local area network

a. A procedure is established for the incident handling of the wireless local area network (see also DER.2.1 Security incident handling).
b. In case of a wireless local area network attack, the access points and the wireless connection can be blocked in the pre-determined extent.
c. An action plan is established for the prevention of network intrusion with the help of a stolen access point (if using WPA2-PSK, the key is changed; in case of a RADIUS server, the stolen access point is blocked in the server).
d. The client's certificates are blocked in the case of certificate-based authentication in the stolen access point.
e. If necessary, the configuration of the access points can be restored with a backup copy.

3.3 Standard measures

NET.2.1.M9 Secure connection of the wireless local area network with a cable network [architect]

a. Connection points of the wireless local area network with a cable-based local area network are secure (e.g. using a packet filter).
b. A separate virtual local area network is implemented for every network name (SSID).
c. Access to the local area network from the wireless local area network is handled and secured similarly to access from the internet. Access is permitted only through a firewall.
d. Only wireless access points compliant with the established organisational requirements are connected to the wireless local area network.
e. The measure NET.2.1.M7 Secure wireless local area network architecture is complied with when connecting access points.

NET.2.1.M10 Security guidelines for the wireless local area network

a. Security guidelines for the wireless local area network are documented, established, and communicated to all users based on the general security policy of the organisation.
b. Among all else, the security guidelines for the wireless local area network establish:

- who can install, configure, and use the components of the wireless local area network;
- the security measures and standard configuration of the wireless local area network components;
- the manner of managing the wireless local area network components;
- the manner of logging and monitoring activities in the wireless local area network;

• the manner of reporting security issues and the person to whom they are reported (see also DER.2.1 Security incident handling).

c. Compliance with the security guidelines for the wireless local area network is checked regularly. The results are documented.

NET.2.1.M11 Suitable components of the wireless local area network

a. A specification of requirements for the selection of the wireless local area network components is prepared based on the results of designing the wireless local area network infrastructure (see also NET.2.1.M1 Planning wireless local area networks).

b. All wireless local area network components are compatible with the network, security, authentication, monitoring, and log infrastructures. Compatibility requirements are taken into consideration when acquiring wireless local area network components.

c. The clients, access points, network management systems, and authentication servers of the wireless local area network support secure authentication methods.

NET.2.1.M12 Suitable management of the wireless local area network

a. The wireless local area network is managed with the central means of management.

b. As a minimum, the management of the wireless local area network entails the following:

• updating and documenting the firmware versions of client devices of the access points and the wireless local area network;

• configuration changes and documenting such changes;

• analysis and assessment of alarm messages;

• troubleshooting;

• action in case of a suspicion of an incident;

• logging and analysis of log data.

c. The management solution complies with the requirements of the security guidelines for the wireless local area network.

NET.2.1.M13 Regular security checks of the wireless local area network

a. The wireless local area network is regularly checked for known vulnerabilities.

b. Unauthorised access points that have been installed in the wireless local area network are searched for in the course of the inspection.

c. The service quality of the network is measured periodically, including:

- bandwidth;
- latency;
- packet loss.

d. Periodic security testing of the wireless local area network is conducted for the detection of the vulnerabilities of the network.

e. The results of the security checks are documented and the reasons for deviations are analysed.

NET.2.1.M14 Regular review of the wireless local area network components

a. The implementation of the security measures covering the components of the wireless local area network (access points, distribution system, management solution of the wireless local area network, etc.) is checked regularly.

b. The correctness of the configuration of the wireless local area network components is checked regularly.

c. Random checks are conducted to determine whether there have been any opening or manipulation attempts in access points that are in easily accessible locations.

d. The results of the reviews are documented and the reasons for deviations are analysed.

3.4 Advanced measures

NET.2.1.M15 Protecting the wireless local area network with a virtual private network (VPN) (C-I)

a. A virtual private network (VPN) is used to protect the data communication of the wireless local area network (WLAN) infrastructure.

b. The measures of the module NET.3.3 Virtual private network (VPN) are implemented when using a VPN.

NET.2.1.M16 Additional security for the connection between the wireless local area network and a cable network (C-I-A)

a. Additional measures and tools are used for the upgraded security of the connection between the wireless local area network and a cable network, such as an intrusion detection system (IDS) and/or intrusion prevention system (IPS).

NET.2.1.M17 Security of the access point connections (C)

a. The communication between the access points is encrypted to guarantee the confidentiality of the data (see also NET.2.1.M3 Selecting secure cryptographic mechanisms).
b. Data communication between the wireless access points and the management system of the wireless local area network is secured with the IPSec, TLS v1.2 or TLS v1.3 protocols. A certificate is required for authentication.
c. None of the elements of the management of access points and the wireless local area network are positioned in a cloud.
d. The infrastructure of the wireless local area network has no direct communication between access points; data communication is encrypted and goes through the central controller of the wireless local area network.

NET.2.1.M18 The tools for intrusion detection and prevention in the wireless local area network (C-I-A)

a. Wireless intrusion detection system (WIDS) and/or wireless intrusion prevention system (WIPS) meant for wireless local area networks are used in the wireless network for the detection of vulnerabilities and security events.

NET.2.2 Using wireless local area networks

1 Description

1.1 Purpose

To present the measures for the secure use of wireless local area networks (WLAN).

1.2 Responsibility

The user is responsible for the implementation of the measures in this module.
Additional responsible persons: IT department, director.

1.3 Limitations

The module contains measures for the secure management of wireless local area networks. The measures for the secure implementation and operation of a wireless local area network are described in the module NET.2.1 Operating wireless local area networks. The general security principles for the client computer are discussed in the module SYS.2.1 Client computer in general. Measures from the modules ORP.3 Increasing awareness of information security and training and DER.2.1 Handling of security incidents are also implemented for the users of the wireless local area network.

2 Threats

2.1 Ignorance of the guidelines

If a user does not comply with the guidelines for the secure use of a wireless local area network (e.g. connects to an unknown network), an attacker has the opportunity to eavesdrop on the network traffic. The attacker would gain access to the data transmitted through the network, such as webpages that have been visited, session cookies, and passwords.

2.2 Failure to comply with the security measures

If the established security measures are ignored (e.g. the client of the wireless local area network is used in ad hoc mode), then another client device could gain unauthorised access to the confidential documents of the user if the client resources have been distributed.

2.3 Eavesdropping on the data communication of the wireless network

Data that is not encrypted or has been encrypted insufficiently can be copied during the data exchange and it is possible to eavesdrop on the communication. An organisation does not have full control of all locations where the receipt of the data is technically possible.

2.4 Analysis of the data communication

The MAC address of a WLAN interface can be used for compiling a profile of the mobile user; for example, it is possible to discover which wireless access points the user utilises.

2.5 Spoofing a real access point (rogue access point)

An attacker could present devices under their control as parts of the infrastructure of the wireless local area network by establishing a rogue access point in the vicinity of the client with a suitably

selected network name (SSID). A user logs into the network that only appears to be the network desired by the user. This way, the attacker can eavesdrop on the data communication. The use of rogue access points is particularly widespread in the wireless local area networks for public use.

3 Measures

3.1 Life cycle

Planning

NET.2.2.M1 Guidelines for the use of a wireless local area network

Implementation

NET.2.2.M2 Raising the awareness of and training the users of the wireless local area network

Operation

NET.2.2.M3 Use of a wireless local area network in public wireless local area networks

Emergency response

NET.2.2.M4 Procedure for security events in the wireless local area network

3.2 Key measures

NET.2.2.M1 Guidelines for the use of a wireless local area network [IT department]

- a) Guidelines for the use of the wireless local area network (WLAN) are established based on the general security policy of the organisation.
- b) As a minimum, the guidelines for the use of the wireless local area network stipulate:
- the types of intranets and external networks that the client of the wireless local area network can connect to;
- the type of information that cannot be exchanged through the wireless local area network;
- the implementation of the security tools of the client devices;
- sufficient strength requirement for passwords;
- prohibition of the ad hoc network mode;
- prohibition of changing the configuration;
- the conditions for the permissibility of directories and services;
- prohibition of connecting wireless access points with the local area network of the organisation;
- deactivation of the WLAN interface after a longer period of inactivity;

• action in case of a security incident.
• c) Compliance with the guidelines is checked regularly and the results are documented.

NET.2.2.M2 Raising the awareness of and training the users of the wireless local area network [director, IT department]

• a) The users of the wireless local area network are trained in the threats and security of the wireless local area networks. The training includes examples based on the specific organisation.
• b) Important security settings of the wireless local area network and the threats related to avoiding or deactivating these settings are explained to the users.
• c) Users are familiar with the guidelines for the use of the wireless local area network and comply with them.

NET.2.2.M3 Use of a wireless local area network in public wireless local area networks [IT department]

• a) The users know whether the use of a public access point is permitted and under what conditions (see also NET.2.2.M2 Raising the awareness of and training the users of the wireless local area network).
• b) Rarely used wireless local area networks are deleted from the history of the client device.
• c) If possible, a user account with limited rights is used in insecure conditions. A user with administrative rights is prohibited from entering insecure external wireless local area networks from their computer.
• d) Sensitive data is forwarded only in an encrypted format using secure protocols in insecure wireless local area networks.
• e) A user can access the internal resources of the organisation from a foreign wireless local area network only through a virtual private network (VPN) (see also NET.3.3 Virtual private network (VPN)).

3.3 Standard measures

NET.2.2.M4 Procedure for security events in the wireless local area network

• a) The user is obligated to back up their work results, exit the wireless local area network, and deactivate the WLAN interface in the client device in the case of a suspicion of an incident or a failure in the wireless local area network.

• b) The user documents the error messages and anomalies, including the activities that they were involved in before or during the security incident.

• c) In case of a failure or a suspicion of an incident in a WLAN network, the user reports the security event to the IT department immediately through the agreed point of contact (such as the IT user support).

• The module has no advanced measures.

3.4 Advanced measures

There are no advanced measures in this module.

NET.3 Network components

NET.3.1 Routers and switches

1 Description

1.1 Purpose

To present the measures for the secure operation of routers and switches.

1.2 Responsibility

The IT department is responsible for the implementation of the measures for routers and switches.
Additional responsible persons: Information security manager.

1.3 Limitations

The module does not describe the product-specific measures of individual manufacturers.
As nowadays, the originally different functions of a router and a switch are often combined into a single device, most of the measures of this module can be used for both routers and switches.
Measures from the module NET.3.2 Firewall should be complied with when implementing the firewall functions of routers and switches.
The module does not handle the security measures of virtual routers and switches or the routing functions that can be activated in the operating systems of computers.

The module does not cover the security aspects of the infrastructure (e.g. the suitable installation, power supply, or cables of the devices); these are presented in the INF Infrastructure modules. The measures for the establishment and management of networks are presented in the modules NET.1.1 Network architecture and solution and NET.1.2 Network management.

2 Threats

2.1 Distributed denial-of-service attack (DDoS)

A distributed denial-or-service attack could be launched through a SYN flood or a UDP flood. A large amount of SYN packets or datagrams are sent to the device selected as the victim and the recipient is overloaded by responding to them. The functioning of the routers is interrupted as a result of the denial-of-service attack. As a result, the availability of the local area network service decreases and the local area network might become unavailable.

2.2 Manipulation

If an attacker manages to gain unauthorised access to a router or a switch, they can manipulate the devices (e.g. activate additional services in the devices). Services, client devices, or entire network segments can be blocked by changing the configuration of the router or the switch.

2.3 Configuration errors of a router or a switch

The original standard configuration of routers and switches can have unnecessary and insecure services that are activated. If the routers and switches are commissioned with insecure default settings, unauthorised access to the devices, manipulating the devices, and/or interrupting services is easier. This might make network services unavailable to the users.

2.4 Inadequate planning

When planning to commission routers and switches, mistakes can be made in specifying the number of ports or the capacity of the device. This often happens when the main decision criterion is the cost of the device.

2.5 Incompatible active network components

If active network components are added to the existing networks, compatibility problems could easily arise between the devices. When using the devices of several manufacturers together, the quality of network services might suffer (e.g. bandwidth). Even using different firmware or software versions for the same device models in a single network could create compatibility problems. This results in complicated failures and interferences in the functioning of the network.

2.6 MAC flooding

In the case of MAC flooding, the attacker forwards a large amount of forged queries with MAC source addresses to the switch. As soon as the switch achieves the limit of the MAC addresses, it will send queries to all IT devices in the network. This way, the attacker can map the network traffic and create an unnecessary load in the network.

2.7 Attacks against the STP protocol

In case of a spanning tree protocol (STP) attack, the attacker forwards the bridge protocol data units (BPDUs) so that the switches would start to use the malicious switch that is connected to the local area network as a root bridge. Network traffic is directed through the malicious switch, enabling the attacker to save information that is forwarded through it. An attacker can initiate distributed denial-of-service attacks and force the network to establish a new spanning tree topology with the help of the forged bridge protocol data unit, thus causing a network failure.

2.8 GARP attacks

In case of a gratuitous ARP attack (GARP attack), the attacker sends packets in the format of an ARP (address resolution protocol) response to the selected victims or all the IT devices in the same subnet. The attacker replaces someone else's IP address with the MAC address of their own device in the forged ARP request answers, forcing the device that is being attacked to change its ARP table. As a result, the network traffic is directed to the attacker instead of the actual intended address. This way, the attacker can save or manipulate the data exchange between the victims.

3 Measures

3.1 Life cycle

Implementation

NET.3.1.M1	Secure baseline configuration of a router or switch
NET.3.1.M4	Security of the administrative interfaces of routers or switches
NET.3.1.M9	Operational documentation of routers or switches
NET.3.1.M10	Security guidelines for routers and switches
NET.3.1.M18	Access control lists

Operation

NET.3.1.M5	Protection from fragmentation attacks on IP packets
NET.3.1.M6	Emergency access to routers or switches
NET.3.1.M7	Router and switch logs
NET.3.1.M12	Checklist of the configuration
NET.3.1.M13	Out-of-band management network
NET.3.1.M14	Protecting ICMP messages from improper use
NET.3.1.M15	Prevention of forged packets and spoofing
NET.3.1.M16	Prevention of IPv6 'routing header type 0' attacks
NET.3.1.M17	Prevention of denial-of-service attacks
NET.3.1.M19	Security of switch ports
NET.3.1.M20	Secure routing protocols
NET.3.1.M23	Reviews and penetration testing

Emergency response

NET.3.1.M8	Regular data backup
NET.3.1.M22	Emergency response of routers and switches

Acquisition

NET.3.1.M11	Choosing a router or switch

Planning

NET.3.1.M21	Management of access rights and identity in the network infrastructure

Additional advanced measures

NET.3.1.M24	Regulation of network access
NET.3.1.M25	Extended protection of the integrity of configuration files
NET.3.1.M26	Guaranteeing high availability
NET.3.1.M27	Management of the performance of business-critical applications
NET.3.1.M28	Certified products

3.2 Key measures

NET.3.1.M1 Secure baseline configuration of a router or switch

a. Before taking a router or a switch into use, secure baseline configuration is installed on it.
b. The standard user accounts and passwords are changed. The passwords are stored in an encrypted manner (e.g. in a password storage). Unnecessary user accounts are deactivated.
c. Access to the configuration files is limited and their integrity is ensured with suitable measures.
d. The unnecessary services, protocols, and function solutions in the baseline configuration of the routers and switches are deactivated or uninstalled.
e. The unnecessary network interfaces and ports of the routers and switches are blocked.
f. Upgrading the functionality of the routers and switches is well-grounded and complies with the security policy of the organisation.

NET.3.1.M4 Security of the administrative interfaces of routers or switches

a. Access for managing the routers or switches is only possible from a predetermined IP address or a range of IP addresses.
b. Management interfaces cannot be accessed from untrustworthy networks.
c. Secure and encrypted protocols are used for the protection of routers and switches. In the case of unencrypted management communication, a partitioned management network is used (out-of-band management).
d. Suitable time limits are set for the use of the management interfaces.
e. All unnecessary services of the management interface are deactivated.
f. Unauthorised access (including physical access) to the specialised hardware interface of the network device is restricted.

NET.3.1.M5 Protection from fragmentation attacks on IP packets

a. Security mechanisms are activated in the router and layer 3 switch for the prevention of IPv4 and IPv6 fragmentation attacks.

NET.3.1.M6 Emergency access to routers or switches

a. When the network is down, the administrators can manage the routers and switches through a local direct access.

NET.3.1.M7 Router and switch logs

a. As a minimum, the following router and switch events are logged (if possible, automatically):

- changes in the configuration;
- restarts;
- system failures;
- changes in the status of interfaces, system, and network segments;
- unsuccessful login attempts.

NET.3.1.M8 Regular data backup

a. The router and switch configuration files are backed up regularly.
b. Backup copies are stored in a secure manner. Backup copies are available in case of an emergency.

NET.3.1.M9 Operational documentation of routers or switches

a. All important operations of the router and switch (including everything related to changes in security) are added to the operational documentation.
b. The configurations of the router and the switch and changes thereto are documented.
c. Operational documentation is protected against unauthorised access.

3.3 Standard measures

NET.3.1.M10 Security guidelines for routers and switches [information security manager]

a. Security guidelines for routers and switches are established based on the general security policy of the organisation, which present the specification and instructions for the secure operation of the devices.
b. The device managers are familiar with the security guidelines for routers and switches and comply with them.
c. Any deviations from the security guidelines and amendments to the security guidelines are approved by the information security manager and documented.
d. Compliance with the security guidelines is checked regularly.

NET.3.1.M11 Choosing a router or switch

a. A specification of requirements is established for the procurement of routers or switches.
b. The acquired device complies with the information security policy and corresponds to the protection requirement of the network.

NET.3.1.M12 Checklist of the configuration

a. A configuration checklist is prepared for the inspection of the essential security settings according to the purpose of using the routers and switches.

NET.3.1.M13 Out-of-band management network

a. Routers and switches are managed through a partitioned management network (out-of-band management).
b. The management interfaces and connections are protected with a separate firewall.
c. The management interfaces that connect to the main network are deactivated.
d. All security mechanisms for the authentication and encryption of management protocols and ensuring their integrity are activated. All insecure management protocols are deactivated (see also NET.1.2 Network management).

NET.3.1.M14 Protecting ICMP messages from improper use

a. The messages of the ICMP (internet control message protocol) and ICMPv6 protocols are filtered for the prevention of improper use.

NET.3.1.M15 Prevention of forged packets and spoofing

a. Bogon filtering is used to block access to routers and switches from unspecified IP addresses.

NET.3.1.M16 Prevention of IPv6 'routing header type 0' attacks

a. When using the IPv6 protocol, security mechanisms are implemented which detect and avoid routing header type 0 attacks.

NET.3.1.M17 Prevention of denial-of-service attacks

a. In order to prevent denial-of-service attacks, security mechanisms are applied which detect and prevent attacks related to a large number of messages (denial-of-service attacks) and TCP state-exhaustion attacks.

NET.3.1.M18 Access control lists

a. Access to routers and switches is limited by an access control list (ACL), which determines the types of IT systems and/or networks that can access the routers and switches.
b. In the absence of specific requirements, the access control list is prepared based on the whitelisting principle.

NET.3.1.M19 Security of switch ports

a. Switch ports are protected from unauthorised physical access.

NET.3.1.M20 Secure routing protocols

a. When forwarding the changes in the routing data and updates to the routing table, the routers are authenticated. All used routing protocols support the authentication of the routers.
b. Dynamic routing protocols are used only in secure networks. Static routing protocols based on the routing table are used in the demilitarised zones (DMZ).

NET.3.1.M21 Management of access rights and identity in the network infrastructure

a. The access management of routers and switches is part of the central administration of identity and rights (see also ORP.4 Administration of identity and rights).

NET.3.1.M22 Emergency response of routers and switches

a. A guideline for handling typical failures is prepared for diagnostics and troubleshooting, which is regularly updated.
b. The emergency preparation of routers and switches is a part of the general concept of emergency preparation (see also DER.4 Emergency management).
c. The documentation and guidelines for emergency response are available on paper as well.
d. Emergency procedures are practised regularly.

NET.3.1.M23 Reviews and penetration testing

a. Routers and switches are regularly tested and inspected for known security issues.
b. The compliance of the devices to secure baseline configuration is checked in the course of regular reviews.
c. The results of the reviews and penetration testing are documented and the identified shortcomings are rectified at the earliest opportunity.

3.4 Advanced measures

NET.3.1.M24 Regulation of network access (I-A)

a. Access to the network is regulated with port-based authentication methods EAP-TLS (extensible authentication protocol - transport layer security) that comply with the standard IEEE 802.1x.
b. The aforementioned method cannot be used with the standard's insecure versions IEEE 802.1x-2001 or IEEE 802.1x-2004.

NET.3.1.M25 Extended protection of the integrity of configuration files (I)

a. In the case of an emergency recovery or restart of the router or the switch, only the latest correct configuration and the access control list with the latest update are used.

NET.3.1.M26 Guaranteeing high availability (A)

a. The routers and switches are planned with redundancy.
b. The mechanisms for guaranteeing high availability correspond to the security policy of the organisation, do not hinder the work of the router or switch, and do not decrease the security level.

NET.3.1.M27 Management of the performance of business-critical applications (A)

a. The routers and switches prioritise server applications and network services and distribute resources based on need to guarantee the sufficient capacity of the business-critical applications.

NET.3.1.M28 Certified products (C-I)

a. As a minimum, the router or the switch is certified at the level EAL4 of the Common Criteria (CC) or other comparable security assessment criteria.

NET.3.2 Firewall

1 Description

1.1 Purpose

To present the measures for the secure procurement, construction, configuration, and operation of a firewall or a firewall system.

1.2 Responsibility

The IT department is responsible for complying with the security measures for firewalls.
Additional responsible persons: Information security manager.

1.3 Limitations

This module supplements the module NET.1.1 Network architecture and solution with security measures specifically for firewalls. Measures from the module NET.3.1 Routers and switches are also implemented for protecting the functioning of the router or switch used in the firewall.
The module does not handle additional security aspects of devices with an added functionality (such as the next-generation firewall); these are presented in the modules NET.3.3 Virtual private network (VPN) and OPS.1.1.4 Protection against malware. This module does not cover the specific security options of the external server service (e.g. a reverse proxy or a web firewall).
The security aspects of the infrastructure (such as suitable installation or power supply) are explained in the module group INF Infrastructure. General security measures from the modules ORP.4 Administration of identity and rights, OPS.1.1.2 IT management, and OPS.1.1.3 Patch and change management are also applied for firewalls.

2 Threats

2.1 Distributed denial-of-service attack (DDoS)

In case of a distributed denial-of-service attack (DDoS), a large number of packets or messages that must be processed create failures in the functioning of the firewall. A distributed denial-of-service attack can also be launched with a TCP SYN flood or UDP flood, for example. The availability of the network services deteriorates due to a denial-of-service attack.

2.2 Manipulation

When an attacker manages to gain access to the firewall or the management interface of the firewall, they can deliberately manipulate its settings. The attacker can change the configuration (for example, allow access to the intranet from the internet by changing the firewall rules), initiate additional services, or install malware. In addition, they can eavesdrop on the data communication in the manipulated system or launch a denial-of-service attack.

2.3 Bypassing the limitation of the firewall rules

In order to access network sections that are protected with a firewall or penetrate the security mechanisms of the firewall, an attacker can launch a fragmentation attack or take advantage of the vulnerabilities in the network protocols.

2.4 Configuration and maintenance errors of the firewall

The configuration and management of the firewall is essential in ensuring the security of the IT systems and business processes. Incorrectly configured firewall rules could block the network access of the IT system and create availability problems. The incorrect configuration of the firewall might leave the intranet completely defenceless against an external attacker. In the worst case, an attacker might gain access to the resources of the intranet.

3 Measures

3.1 Life cycle

Planning

NET.3.2.M1 Security guidelines for firewalls

Operation

NET.3.2.M2 Firewall rules

NET.3.2.M3 Suitable filtering rules for packet filters

NET.3.2.M6 Security of the management interfaces of the firewall

NET.3.2.M9 Firewall logs

NET.3.2.M10 Preventing fragmentation attacks in a packet filter

NET.3.2.M22 Synchronising the firewall time

NET.3.2.M16	Secure P-A-P structure (packet filter - application level gateway - packet filter)
NET.3.2.M17	Deactivation of IPv4 or IPv6
NET.3.2.M18	Partitioning the management network of the firewall
NET.3.2.M19	Preventing UDP floods, TCP SYN floods, and serial number guessing in the packet filter
NET.3.2.M23	Monitoring the firewall and the analysis of the monitoring results
NET.3.2.M24	Reviews and penetration testing

Implementation

NET.3.2.M4	Secure configuration of the firewall
NET.3.2.M8	Prohibition of dynamic routing
NET.3.2.M14	Operational documentation of a firewall

Emergency response

NET.3.2.M7	Firewall emergency access
NET.3.2.M32	Firewall emergency response

Acquisition

NET.3.2.M15	Procedure for acquiring firewalls

Additional advanced measures

NET.3.2.M20	Security of the basic internet protocols
NET.3.2.M21	Temporary encryption of data traffic
NET.3.2.M25	Integrity-protected configuration files
NET.3.2.M26	Outsourcing function extensions
NET.3.2.M27	Various operating systems and firewall products in the architecture of a multi-layer firewall
NET.3.2.M28	Central filtering of active content
NET.3.2.M29	Means of guaranteeing high availability
NET.3.2.M30	Management of the performance of business-critical applications
NET.3.2.M31	Certified products

3.2 Key measures

NET.3.2.M1 Security guidelines for firewalls [information security manager]

a. Security guidelines for firewalls are established based on the general security policy of the organisation, which present the requirements for the secure operation of the firewalls.
b. All persons responsible for the firewalls are familiar and comply with the security guidelines for

the firewalls.
c. Any deviations from the security guidelines and amendments to the security guidelines are approved by the information security manager and documented.
d. Compliance with the security guidelines for the firewalls is checked regularly.

NET.3.2.M2 Firewall rules

a. The entire outgoing data traffic of the intranet is directed through a firewall. Unauthorised connections cannot be established outside the network and are blocked.
b. Unauthorised connection attempts from an outside network to the protected network are blocked. None of the external IT systems can access the intranet directly through the firewall (see also NET.1.1 Network architecture and solution).
c. Clear rules have been established for the protection of the firewalls, determining the types of the authorised intranet traffic and connections from the intranet to an external network (with various service servers, for example). All network connection requests in the firewall are authorised based on the whitelisting principle.
d. All exceptions to and changes in the firewall rules are documented along with the reasons. Exceptions and changes are approved before implementing the firewall rules.
e. The organisation has appointed persons who can change the firewall rules and a person responsible for approving the changes to the firewall rules.
f. The vulnerabilities resulting from the exceptions to the firewall rules are compensated with the security measures specific to certain applications or IT systems.

NET.3.2.M3 Suitable filtering rules for packet filters

a. The filtering rules for packet filters are established and implemented based on the measure NET.3.2.M2 Firewall rules.
b. A packet filter prevents all faulty TCP flag combinations.
c. The firewall implements the rules for filtering TCP data flow, UDP datagrams, and ICMP messages with dynamic packet filtering (stateful packet inspection).

NET.3.2.M4 Secure configuration of the firewall

a. Before commissioning, the firewall is configured to be secure; only the necessary services are allowed.

b. All changes in the configuration are documented (see also NET.3.2.M14 Operational documentation).
c. Measures to ensure the integrity of the configuration files are applied.
d. Access passwords of the firewall are carefully protected; for example, cryptographic means are used for security (see also CON.1 Cryptography concept).
e. Unnecessary services and additional functions of the firewall are deactivated or uninstalled. The implementation of the additional functions of the firewall takes place based on legitimate needs and the respective decisions are documented.
f. The configuration data and documentation of the settings of the firewall are protected from access by outsiders.

NET.3.2.M6 Security of the management interfaces of the firewall

a. Accessing the firewall for management is only possible from the given IP address or a range of IP addresses.
b. Untrustworthy networks do not have access to the management interfaces of the firewall.
c. The in-band management protocols of the firewall are secure. As an alternative, out-of-band management can be used for management purposes.
d. Suitable time limits are set for the use of the management interfaces.

NET.3.2.M7 Firewall emergency access

a. When the network is not functioning, the operators can manage the firewall through local direct access.

NET.3.2.M8 Prohibition of dynamic routing

a. The dynamic routing of the firewall is deactivated (except when the packet filter is used as a router according to the module NET.3.1 Routers and switches).

NET.3.2.M9 Firewall logs

a. As a minimum, the following security events are logged in the firewall:
- logins to the management interface of the firewall;
- configuration changes of the firewall;
- blocked requests for network connection (source and destination IP addresses, source and

destination ports or the type of ICMP/ICMPv6, date, and time);

• unsuccessful access attempts to system resources (due to authentication errors or the lack of rights);

• error messages of firewall services;

• general error messages of the firewall.

b. The operations conducted in the firewall are logged automatically if possible.

c. As a minimum, the failed authentication attempts of the protocol or access control list are logged when using security proxies, including the service, the source and destination IP addresses, the source and destination ports, date, and time.

NET.3.2.M10 Preventing fragmentation attacks in a packet filter

a. Security mechanisms are applied in the packet filter to prevent fragmentation attacks against the IPv4 and IPv6 protocols.

NET.3.2.M14 Operational documentation of a firewall

a. All operations affecting the security of a firewall (including firewall rules and changes in configuration and system services) are included in operational documentation.

b. All changes in firewall rules are documented along with the reasons for the changes.

c. The documentation is protected against unauthorised access.

NET.3.2.M15 Procedure for acquiring firewalls

a. A specification of requirements has been prepared for assessing the suitability of a firewall before the acquisition.

b. When selecting the firewall, the requirements of the information security policy and the protection requirements are taken into account.

c. When using the IPv6 protocol, the packet filter allows for checking the IPv6 extension headers and the IPv6 configuration to the IPv4 protocol.

NET.3.2.M22 Synchronising the firewall time

a. The firewall time is synchronised with a secure NTP server.

b. The synchronisation of time with other external sources is blocked in the firewall.

3.3 Standard measures

NET.3.2.M16 Secure P-A-P structure (packet filter - application level gateway - packet filter)

a. The P-A-P structure (packet filter - application level gateway - packet filter) is constructed of compatible hardware and software components.
b. The basic protocols use an OSI application level security proxy. As a minimum, a generic proxy is used in case of TCP and UDP.

NET.3.2.M17 Deactivation of IPv4 or IPv6

a. When the IPv4 or IPv6 protocols are not used in a network segment, the respective protocol is deactivated in the firewall interface.

NET.3.2.M18 Partitioning the management network of the firewall

a. Firewalls are managed only by out-of-band management (using an additional channel). The in-band management interfaces of the firewall are deactivated.
b. The management protocol and the given source and destination addresses limit the administrative data communication in the firewall. All insecure management protocols are deactivated (see also NET.1.2 Network management).
c. The security mechanisms for the authentication of the users, ensuring the integrity of the data, and encryption of the administrative connections are activated in the firewall.

NET.3.2.M19 Preventing UDP floods, TCP SYN floods, and serial number guessing in the packet filter

a. The server services that can be accessed from an untrustworthy network are protected from an attempted semi-open and open handshake flood with a packet filter that limits the UDP data flows.
b. The generation of the initial sequence number (ISN) of the TCP protocol is activated for the outgoing connections in the packet filter (except when they go through a security proxy).

NET.3.2.M23 Monitoring the firewall and the analysis of the monitoring results

a. The concept of monitoring the IT systems of the organisation includes monitoring the firewalls.
b. It is specified which types of logs are analysed and whether it is done on a regular, random, or case-by-case basis.

c. The managers of the firewall are informed automatically in the following instances:

- when the previously determined limits are exceeded;
- when errors and failures occur;
- when previously determined events take place.

d. The log data and status messages of the firewall are only forwarded through secure communication routes.

NET.3.2.M24 Reviews and penetration testing

a. The firewall (or the firewall system) is tested regularly regarding the known vulnerabilities.
b. The security review of the firewall is conducted regularly and the results of the review are documented.

NET.3.2.M32 Firewall emergency response

a. The emergency response of the firewall is a part of the general emergency response concept of the organisation (see also DER.4 Emergency management).
b. The configurations of the firewall are backed up and their recovery is part of the recovery plans.
c. The documentation and guidelines for emergency response are available on paper as well.
d. The firewall emergency procedures are practised regularly.

3.4 Advanced measures

NET.3.2.M20 Security of the basic internet protocols

a. The data traffic of the HTTP, SMTP, and DNS protocols and their encrypted versions is routed through the security proxies that are specific to protocols.

NET.3.2.M21 Temporary encryption of data traffic (C-I)

a. The encrypted connections with untrustworthy networks are decrypted temporarily to verify the protocol and check the forwarded data for malware.
b. Legal framework conditions are complied with when using the decrypted data.
c. The component that decrypts the data traffic temporarily stops the outdated and/or insecure encryption technologies (such as SSL) and outdated and/or insecure encryption algorithms (such as DES MD5, SHA1).

d. A TLS proxy checks the trustworthiness of the certificates. If the used certificate is not trustworthy, the connection is blocked.

NET.3.2.M25 Integrity-protected configuration files (C-I)

a. After the recovery or restart of a firewall following an emergency, only the last correct configuration and the latest updated access control list are used.
b. The aforementioned requirements also apply when the firewall has been restarted by an attacker.

NET.3.2.M26 Outsourcing function extensions (C-I-A)

a. The function extensions of the firewall are outsourced only as specialised hardware and software.

NET.3.2.M27 Various operating systems and firewall products in the architecture of a multi-layer firewall (C-I)

a. Various operating systems and firewall products are used by the external and internal firewalls in the case of a multi-layer firewall to reduce the effect of a potential vulnerability in an individual product.

NET.3.2.M28 Central filtering of active content (C-I)

a. The active content of web traffic is filtered centrally, the data needed for checking the encrypted data traffic is temporarily decrypted.
b. The security proxies enable the filtration of active content.

NET.3.2.M29 Means of guaranteeing high availability (A)

a. Packet filters, application level gateways, routers, and other active components (such as switches) are designed with sufficient redundancy.
b. Two independent solutions are used for external network connections (such as the solutions of various internet service providers).
c. After a failover, the firewall retains the compliance with the requirements of the security guidelines.
d. The availability is monitored based on more than one parameter and criterion. The log data and warning messages are checked regularly.

NET.3.2.M30 Management of the performance of business-critical applications (A)

a. Packet filters capable of performance management are used in the transition between the network gateways and network segments.

NET.3.2.M31 Certified products (C-I)

a. The firewalls are certified based on at least the EAL4 level of Common Criteria or other comparable security assessment criteria.

NET.3.3 Virtual private network (VPN)

1 Description

1.1 Purpose

To present the measures for the secure design, implementation, and operation of a virtual private network (VPN).

1.2 Responsibility

The IT department is responsible for compliance with the measures for virtual private networks (VPNs).
Additional responsible persons: Information security manager.

1.3 Limitations

The module only discusses the virtual private network systems based on the OSI model layers 2 (data link layer) to 4 (transport layer).
The module NET.1.1 Network architecture and solution describes the creation of a secure network. The processes related to the operation of a virtual private network are covered in the modules OPS.1.1.3 Patch and change management, ORP.3 Increasing awareness of information security and training, CON.1 Cryptography concept, CON.3 Data backup concept, DER.4 Emergency management, and OPS.1.2.5: Remote maintenance.

The secure configuration of the operating systems of VPN endpoints is presented in the modules SYS.1.1 Server in general or SYS.2.1 Client computer in general.

2 Threats

2.1 Absence or inadequacy of an application plan for the virtual local area network

A carelessly planned, constructed, or configured virtual private network could contain vulnerabilities. An attacker could take advantage of the vulnerabilities to access the confidential data of the organisation.

2.2 Insecure service provider of the virtual local area network

When an organisation uses a service provider for the VPN solution, it is possible that an attacker attacking the IT systems of the service provider gains access to the intranet of the client devices of the service provider and uses the access to deliberately steal the data in the client devices.

2.3 Insecure configuration of the VPN client applications

If the VPN client application is not configured securely, its security mechanisms might be implemented insufficiently or not at all. If a user can change the configuration of the VPN client application or use software they have selected as a VPN solution, then it makes the connection insecure.

2.4 Insecure standard configuration of the VPN components

The standard configuration of the VPN components might not correspond to the protection requirement of the data. When the convenience of use and the ease of the installation of the solution is paramount (e.g. the default passwords of the manufacturer are not changed), the standard configuration might include vulnerabilities that an attacker can easily exploit. An attacker might have an opportunity to access the local area network of an organisation.

3 Measures

3.1 Life cycle

Planning

NET.3.3.M1 Implementation plan for a virtual private network

NET.3.3.M6 Analysis of the requirements for a virtual private network

NET.3.3.M7 Technical design plan of the virtual private network

NET.3.3.M8 Guidelines for the secure use of the virtual private network

Acquisition

NET.3.3.M2 Selection of a service provider of the virtual private network

NET.3.3.M9 Procedure for selecting products for the virtual private network

Implementation

NET.3.3.M3 Secure installation of the virtual private network devices

NET.3.3.M4 Secure configuration of the virtual private network

NET.3.3.M10 Secure operation of the virtual private network

Operation

NET.3.3.M5 Preventing unnecessary access to the virtual private network

NET.3.3.M11 Secure connection to an external network

NET.3.3.M12 Access management of the users of the virtual private network

Additional advanced measures

NET.3.3.M13 The integration of the VPN components with the firewall

3.2 Key measures

NET.3.3.M1 Implementation plan for a virtual private network

a. The organisation assesses the need for a virtual private network prior to the commissioning of a virtual private network (VPN).

b. Before the commissioning of a virtual private network, the following has been decided:

- the responsibilities of the employees operating the virtual private network;
- the user groups of the VPN and their rights;
- the procedure for granting, changing, and revoking access rights.

NET.3.3.M2 Selection of a service provider of the virtual private network [information security manager]

a. Service level agreements (SLA) have been concluded with the service provider of the virtual private network; the agreements are documented.

b. The performance of the service level agreement with the VPN service provider is monitored regularly.

NET.3.3.M3 Secure installation of the virtual private network devices

a. When special VPN devices are used, the devices have a valid maintenance agreement.
b. Only employees with the necessary qualification install the VPN components.
c. The process of installing the VPN components and any deviations from the installation manual are documented.
d. The functions of the virtual private network and of the security mechanisms are tested before the commissioning of the virtual local area network.

NET.3.3.M4 Secure configuration of the virtual private network

a. A secure configuration has been specified and documented for all client devices, servers, and connections of the virtual private network.
b. The manager of the virtual private network regularly checks the security of the VPN settings in the IT systems. The VPN configuration is changed if necessary.

NET.3.3.M5 Preventing unnecessary access to the virtual private network

a. Regular checks are conducted to determine whether only authorised IT systems and users have access to the virtual local area network.
b. Unnecessary access to the virtual local area network is deactivated as quickly as possible.
c. Access to the virtual local area network is only granted for the allocated duration of use.

3.3 Standard measures

NET.3.3.M6 Analysis of the requirements for a virtual private network

a. An analysis of the requirements to the hardware and software components of the private network is conducted based on the assessment of the need for a virtual private network (see also NET.3.3.M1 Implementation plan for a virtual private network).
b. The analysis of the requirements for a virtual private network takes into consideration:

- the business processes that are included;
- access channels;

- procedures for identification and authentication;
- users and user rights;
- responsibilities and obligations;
- notification routes.

NET.3.3.M7 Technical design plan of the virtual private network

a. A technical design for the virtual private network is prepared, determining:
- the topology of the network;
- VPN access points;
- encryption methods and means;
- allowed access protocols;
- services and resources.

b. Subnets have been determined which can be accessed through the VPN.

NET.3.3.M8 Guidelines for the secure use of the virtual private network [information security manager]

a. Guidelines for the secure use of the virtual private network are prepared for the users of the virtual private network.
b. The users are trained in the secure use of the virtual private network.
c. When a VPN access is created for an employee, they are trained to use the VPN.
d. All users of the virtual private network are obligated to comply with the guidelines for the secure use of the virtual private network.

NET.3.3.M9 Procedure for selecting products for the virtual private network

a. When selecting the products for the virtual private network, the needs of the organisation in its various locations and subunits, including the needs of the mobile users and remote workers, are taken into account.

NET.3.3.M10 Secure operation of the virtual private network

a. The principles for the secure operation of the virtual private network are documented, stipulating its:
- quality management;

- supervision;
- maintenance;
- training;
- administration of rights.

NET.3.3.M11 Secure connection to an external network

a. Sufficiently secure authentication is used when establishing a VPN connection. If possible, multi-factor authentication is used.
b. A VPN connection can only be created between the designated IT systems and services.
c. The data exchange protocols of the VPN connection are suitable and secure.

NET.3.3.M12 Access management of the users of the virtual private network

a. The access management of the users of the virtual private network is centralised and consistent.
b. The servers of the access rights management are managed securely and protected from unauthorised access.

3.4 Advanced measures

NET.3.3.M13 The integration of the VPN components with the firewall (C-I)

a. The data traffic of the virtual private network can be controlled and filtered.
b. The integration of the VPN components with a firewall is documented.

NET.3.4 Network access control (NAC)

1 Description

1.1 Purpose

To present measures for network access control, secure planning, implementation, and utilisation of client devices.
NAC enables access to network through secure authentication and authorisation. For this purpose,

authentication based on standard IEEE 802.1X (central authentication server or a RADIUS server) or MAC addresses is used.

1.2 Responsibility

The IT department is responsible for the implementation of network access control (NAC) measures.
Additional responsible persons: The management of the organisation.

1.3 Limitations

The module describes the general measures for the configuration, authentication, authorisation, and management of a NAC solution. When a measure focuses on a specific IT component (such as a RADIUS server), the component is specifically mentioned in the measure.
Measures from modules APP.2.1 Directory service in general and NET.1.1 Network architecture and solution complement this module. Devices in a wireless local area network (WLAN) are discussed in modules NET.2.1 Operating wireless local area networks and NET.2.2 Using wireless local area networks.
The module does not cover the following:

- general aspects of network components and security of network ports (see NET.3.1 Routers and switches);
- NAC special solutions of the IEEE 802.1X protocol that are not in use;
- implementation of RADIUS in network components (switches, WLAN access points, or WLAN controllers);
- security of endpoints (see module groups SYS.2 Client computers, SYS.3 Mobile devices, and SYS.4 Other systems);
- general security of servers (see SYS.1.1 Server in general) and virtualisation (see SYS.1.5 Virtualisation system);
- general aspects of the administration of identity and rights (see ORP.4 Administration of identity and rights).

2 Threats

2.1 Inadequate planning of NAC solutions

Without an overview of devices that are connected to a network, devices that require a network connection might be left without it or directed to the incorrect network segment. Due to inadequate

planning, the switches in use might not support the requirements of the NAC solution. Due to the inadequate performance of a RADIUS server, the server cannot serve a sufficient number of endpoints simultaneously.

2.2 Adding endpoints to a NAC solution without coordination

The absence of suitable orchestration tools, procedural guidelines, and incomplete lists of devices make the integration of endpoints with a NAC solution complicated.

2.3 Use of insecure protocols

In the absence of EAP (Extensible Authentication Protocol) support, insecure authentication protocols are used, such as EAP-MD5 or MAC authentication. Endpoints with weak authentication protocols that do not restrict devices that are allowed to be connected and protocols that may be used for this purpose, facilitate counterfeit, replay, or man-in-the-middle attacks.

2.4 Incorrect configuration of NAC solutions

Errors may occur when configuring a NAC solution in endpoints and switches or when configuring NAC rules for a RADIUS server. A human error may be caused by an inadequate process guideline, ignorance of an employee, or lack of time. The error may cause disturbances in the functioning of NAC solutions, for example, prevent endpoints from accessing necessary resources or cause endpoints to be unable to access the network.

2.5 Insufficient validation of changes in configuration

Where changes in configuration are not verified or validated when making the changes, errors in configuration may occur. For example, an endpoint may have access to excessive resources or, on the contrary, have no access to the required resources.

2.6 Unprotected network access

Disabling NAC functions temporarily or permanently in switch ports may affect the security of network access. Unauthorised persons or IT systems may be granted excessive rights, be able to access confidential information without permission, and to manipulate or delete it.

2.7 Malfunction of a component of a central NAC solution

Faulty NAC components, incorrect network configuration, lack of processes or denial-of-service attacks cause component failures in central NAC solutions. An endpoint may become inaccessible. In the case of a RADIUS server malfunction, the switch configuration determines whether an endpoint can then access the network without any restrictions or have no network access at all.

2.8 Insufficient protection of personal data

Insufficient protection of personal data (such as setting excessive data retention periods or lack of approval by a data protection specialist) may facilitate the improper use of personal data. For example, employees who use endpoints can be categorised into different user profiles or their activities might be monitored over a longer period.

3 Measures

3.1 Life cycle

Planning

NET.3.4.M1	Decision to implement NAC
NET.3.4.M2	Planning the deployment of NAC
NET.3.4.M3	List of requirements for NAC solutions
NET.3.4.M4	Implementation plan for NAC solutions

Operation

NET.3.4.M5	Adapting the management of endpoints with NAC solutions
NET.3.4.M7	Use of secure authentication in endpoints
NET.3.4.M10	Identity management of NAC solutions
NET.3.4.M11	Secure configuration of NAC solutions
NET.3.4.M12	Monitoring NAC solutions
NET.3.4.M13	Validating the configuration of a NAC solution
NET.3.4.M14	Additional measures for authentication based on the MAC address of a device
NET.3.4.M15	Integrating anti-malware with NAC solutions
NET.3.4.M16	Logging events in the components of a NAC solution
NET.3.4.M17	Secure location of a RADIUS server in the network
NET.3.4.M18	Detailed documentation of a NAC solution
NET.3.4.M19	Secure identity management in NAC

Emergency response

NET.3.4.M6 Emergency response for NAC solutions

Implementation

NET.3.4.M8 Defining NAC-specific roles and privileges in a RADIUS server

NET.3.4.M9 Rules for granting NAC authorisations

Additional advanced measures

NET.3.4.M20 Utilisation of MACsec

NET.3.4.M21 Compliance check of endpoints

NET.3.4.M22 Using NAC when granting authorisation

NET.3.4.M23 Utilisation of autonomous RADIUS servers

NET.3.4.M24 Exclusive use of secure data connection protocols

NET.3.4.M25 Integrating NAC solutions with security monitoring

NET.3.4.M26 Ensuring the high availability of the central components of a NAC solution

NET.3.4.M27 Avoiding authentication based on a MAC address

3.2 Key measures

NET.3.4.M1 Decision to implement NAC [management of the organisation]

a. The organisation has made a justified decision on whether NAC is implemented in the organisation and regarding the scope of implementation.

b. Before deciding, the following has been taken into account:

- network segments and network components where NAC is applied;
- endpoints within and outside of the network that use NAC;
- impact of NAC on the operation of IT systems.

3.3 Standard measures

NET.3.4.M2 Planning the deployment of NAC

a. At least the following aspects have been taken into consideration when planning the implementation of NAC:

- requirements for endpoints, switches, and RADIUS servers;
- updating and supplementing device lists;
- deciding the processes for the acquisition, operation, and incident management of NAC

components;

• allowing the devices to be relocated and replaced;

• monitoring and logging NAC solutions;

• interfacing with external security components (such as firewalls, anti-malware applications, vulnerability scanners, central systems for identifying and reporting security events);

• the need for additional security functions (such as profile analysis, compliance checks of endpoints, MACsec encryption).

NET.3.4.M3 List of requirements for NAC solutions

a. Functional requirements for the components of a NAC solution are collated into a single list of NAC requirements.
b. NAC requirements have been approved by all parties concerned. When acquiring, testing, and approving for commissioning any NAC components, the established requirements are taken into consideration.
c. The list of NAC requirements is regularly reviewed and updated as required.

NET.3.4.M4 Implementation plan for NAC solutions

a. The implementation plan for NAC solutions describes the operating procedures and technical specifications of NAC components that meet the requirements for described solutions.
b. The implementation plan for NAC solutions complies with the principles of network segmentation (see NET.1.1 Network architecture and solution).
c. The implementation plan for NAC solutions determines:

• network segments where NAC is used;

• specifications for affected endpoints, switches, wireless access points, and WLAN controller settings;

• implementation of RADIUS, NAC rules;

• integration with directory services in use;

• authentication and authorisation of users;

• interfacing with external security components (such as firewalls, anti-malware applications, vulnerability scanners, central systems for the identification and reporting of security events);

• the use of additional functions.

NET.3.4.M5 Adapting the management of endpoints with NAC solutions

a. Processes for the commissioning, replacement, changes, and failure management of endpoints take into account limitations caused by the implementation of NAC solutions.
b. The central management process of endpoints includes the installation and management of software, configuration changes, and authentication certificates (such as certificates) required for the functioning of NAC solutions.

NET.3.4.M6 Emergency response for NAC solutions

a. NAC security mechanisms can be temporarily deactivated to the desired extent when necessary.
b. In the event of a failure of a RADIUS server, emergency response scenarios are prepared and measures are planned for the mitigation of any negative impacts.
c. The following options have been considered to prepare for NAC emergency response:
- active network connections are maintained (such as by the temporary suspension of multifactor authentication) but all new login attempts are rejected;
- dynamic network login is halted. Instead, fixed connections between network segments are used to the extent of less critical needs, realised through predefined switch configurations.
- NAC is deactivated either on all network devices or on single switch ports so that network connectivity would be able to continue without restrictions.

d. Emergency scenarios for RADIUS comply with the security policy of the organisation.

NET.3.4.M7 Use of secure authentication in endpoints

a. Endpoints use secure and up-to-date authentication measures (for example, endpoints are authenticated automatically based on certificates or access permissions).
b. Insecure authentication measures are used only under exceptional circumstances when it is justified. The respective decision is documented.

NET.3.4.M8 Defining NAC-specific roles and privileges in a RADIUS server

a. When granting access rights to a RADIUS server, the needs of user groups required for the management of the RADIUS server are taken into account.
b. NAC-specific access to a RADIUS server is only granted to the following user groups:
- users who manage switches in their network area (RADIUS clients);
- users who are responsible for the management of endpoints and who manage device identities (such as MAC addresses);

• primary level support unit that analyses invalid RADIUS requests and makes the necessary corrections.

NET.3.4.M9 Rules for granting NAC authorisations

a. Rules for allowing endpoints to enter a network have been prepared for the NAC solution.
b. Regarding each endpoint or endpoint group, the following has been decided:
• whether unrestricted network access is allowed;
• whether network access is prohibited;
• whether the device can only access limited network segments.
c. The NAC rules determine the authentication measures in use, the conditions of successful authentication, and the manner of performing access control.

NET.3.4.M10 Identity management of NAC solutions

a. Individual identities are used for NAC authentication. Identities created for more than one endpoint are allowed only under exceptional circumstances with justification.
b. NAC authentication details are protected from unauthorised access.

NET.3.4.M11 Secure configuration of NAC solutions

a. Secure standard configurations and procedural guidelines have been prepared for the secure configuration of the components of a NAC solution.
b. The components of a NAC solution are regularly inspected to make sure that they are up to date and appropriate.
c. The authorisations of the users of endpoints are restricted to the extent that they are unable to manipulate or deactivate a supplicant, i.e. to change the configuration of a device requesting a connection, to deactivate it, or to read the keys or passwords of NAC.
d. NAC authentication is deactivated on switches or single ports of switches only in justified and predetermined exceptional cases.

NET.3.4.M12 Monitoring NAC solutions

a. The central RADIUS server, all switches in an authenticator role, and other central services required by a NAC solution are integrated into a central monitoring solution.
b. The following is added to a monitoring solution:

• all parameters specific to NAC, ensuring the functionality of the NAC solution or the corresponding services;

• monitoring the usage of the RADIUS protocol (for example, generating RADIUS requests for monitoring the entire NAC chain, including external directory services);

• monitoring the status of switches to identify the deactivation of NAC.

c. Authorised members of IT management staff are notified of any deviations from the defined states and limits.

NET.3.4.M13 Validating the configuration of a NAC solution

a. Validation objectives are prepared to verify the correctness of a NAC solution configuration. The validation objectives take into consideration the functionality and specifications of various components of the NAC solution.

b. The actual configuration of the components of the NAC solution is regularly compared to the desired configuration.

NET.3.4.M14 Additional measures for authentication based on the MAC address of a device

a. Endpoints where secure EAP authentication is impossible and that are identified by their MAC address are not classified as trustworthy endpoints. The network access of such devices is limited to the least necessary settings.

b. Where possible, additional measures are implemented to protect the data, such as limiting data communication in the endpoints or preparing device profiles.

NET.3.4.M15 Integrating anti-malware with NAC solutions

a. All endpoints are checked to identify malware before connecting the devices to the network of the organisation and allowing them to access IT systems.

b. A suitable anti-malware solution is linked to NAC authentication. Whenever malware is discovered, measures to prevent the spread of malware are implemented in the NAC solution.

NET.3.4.M16 Logging events in the components of a NAC solution

a. In NAC solutions, changes in the statuses of NAC components and other significant events from the point of view of security are logged.

b. In addition, changes in the configuration of central NAC components are logged.

c. The level of detail of the compiled logs and the logs to be stored in a central log infrastructure are determined.
d. Log data is forwarded through secure communication channels.
e. Security-critical events (such as RADIUS disruptions or an unusual number of RADIUS requests) trigger automatic alarms.

NET.3.4.M17 Secure location of a RADIUS server in the network

a. A RADIUS server is located in a protected network segment (see NET.1.1 Network architecture and solution).
b. Requests to a RADIUS server are only allowed from trustworthy sources.
c. A RADIUS server does not communicate with endpoints directly, but only through a switch authenticator. Switch requests are accepted only from a specified management network segment.

NET.3.4.M18 Detailed documentation of a NAC solution

a. A NAC solution along with all the components belonging to the solution are documented appropriately.
b. The documentation describes the configurations of NAC solution components and endpoints as well as interdependencies between the components. The documentation has been suitably subdivided for the purposes of clarity.
c. The documentation contains a simplified description of the integrated authentication rules of the NAC solution.
d. The documentation is kept updated and is updated after every change.
e. The documentation is regularly reviewed to make sure that it is up to date.

NET.3.4.M19 Secure identity management in NAC

a. A suitable identity management solution is implemented to protect network accesses through NAC.
b. As a minimum, the following is performed in the course of identity management:
- handling and protection of certificates;
- terminating and deleting identities;
- describing the process of terminating an identity and the interfaces used.

3.4 Advanced measures

NET.3.4.M20 Utilisation of MACsec (C-I)

a. In order to ensure data integrity and confidentiality, a MACsec (Media Access Control Security) solution based on the IEEE 802.1AE network standard is used on network level.
b. Switches and endpoints not supporting MACsec or where MACsec should not be used are registered. Regular checks are conducted to make sure that the exclusion is justified.

NET.3.4.M21 Compliance check of endpoints (C)

a. Before connecting an endpoint to the network of the organisation and granting access to IT systems, the compliance of the endpoint with the security requirements of the organisation must be verified.
b. Specifications have been prepared for each type of endpoint and endpoints must comply with them. Non-compliant devices have restricted network access.
c. A NAC solution is integrated with a tool for compliance checks, automatically evaluating the compliance of endpoints. Based on the results, the NAC solution decides whether to allow an endpoint to access the network and the scope of access.

NET.3.4.M22 Using NAC when granting authorisation (C)

a. A NAC solution divides endpoints into separate network segments based on the device profile and protection requirements.
b. The organisation has considered the option of letting NAC perform the microsegmentation of endpoints.

NET.3.4.M23 Utilisation of autonomous RADIUS servers (A)

a. Special and autonomous RADIUS servers are used for the implementation of NAC. A RADIUS server does not provide any other services aside from NAC functions, such as the regulation of VPN access.
b. Individual RADIUS servers are used for different networks. The need to implement separate RADIUS servers for office and production networks or to add separate RADIUS servers to LAN and WLAN has been considered.
c. Using autonomous RADIUS servers in separate network segments has been discussed.

NET.3.4.M24 Exclusive use of secure data connection protocols (C)

a. Only secure protocols are used for data communication between central components of a NAC solution and communication between a RADIUS server and a directory service.
b. An analysis has been completed regarding the possibility to use only secure protocols in data communication between a RADIUS server and switches.

NET.3.4.M25 Integrating NAC solutions with security monitoring (A)

a. Central components of a NAC solution and central services used by the NAC solution are integrated with security monitoring solutions.
b. Security events specific to NAC (such as frequent rejection of connection requests or repeated use of an identity) trigger an automatic notification.
c. Where an organisation uses automated systems for the detection of the characteristics of an intrusion and to send respective alerts (an intrusion detection system, or IDS), components of the NAC solution are integrated with them.

NET.3.4.M26 Ensuring the high availability of the central components of a NAC solution (A)

a. Central components of a NAC solution are installed with redundancy. Other central services essential for the functioning of the NAC solution are also highly available.
b. Important parameters for high availability are integrated with monitoring and logging systems. Whenever the status of important parameters changes, an automatic notification is sent.
c. Emergency scenarios prepared for instances of a RADIUS server failure do not decrease the security level of the network.

NET.3.4.M27 Avoiding authentication based on a MAC address (I)

a. Authentication based on a MAC address is only used when it is unavoidable for technical reasons, making an exception is justified and necessary, and the security policy of the network allows this.

NET.4 Communications

NET.4.1 Telephone exchange

1 Description

1.1 Purpose

To present the measures for the secure use of communication systems with the help of a private branch exchange (PBX) that is connected to an external network and the related client devices (landline phones). A telephone exchange can be used for connecting the phones of the organisation with the internal and external subscribers (e.g. through an analogue telephone network).

1.2 Responsibility

The responsible specialist is responsible for compliance with the measures for the telephone exchange.
Additional responsible persons: IT department, director.

1.3 Limitations

The security aspects of IP phone components and calls made from IP phones are explained in greater detail in the module NET.4.2 IP phone (VoIP).
In addition, the modules ORP.4 Administration of identity and rights, OPS.1.2.5: Remote maintenance, CON.3 Data backup concept, and OPS.1.1.5 Logging are taken into account for telecommunication systems.

2 Threats

2.1 Surveillance of the communication system

2.1 Surveillance of the communication system

If the phone calls are forwarded without encryption, an attacker might eavesdrop on the calls. The telephone exchange has a function which enables listening to the phone calls undetected. Activating functions which are normally blocked requires a more detailed knowledge of the system, but due to the freely available online instructions, this is not complicated.

2.2 Surveillance of the premises through the communication system

Everything taking place on the premises can be listened to through the microphones of the communication devices.

2.3 Communication service theft

The purpose of communication service theft is to transfer the expenses of the phone calls or data transmission to third persons. The existing functions of the communication system can be abused for improper use of the system. Remote programmable call forwarding or dialup options can be used for this, for example.

2.4 Improper use of phone connections

If the organisation has phones that are in locations accessible to visitors or are not linked to a specific user, there is a danger of the phones being improperly used for causing damage or for personal gain. Malicious users can call paid service numbers from the landlines of the organisation. An attacker can also organise calls to paid numbers that they own for direct financial gain.

3 Measures

3.1 Life cycle

Planning

NET.4.1.M1 Implementation plan for a telephone exchange

NET.4.1.M6 Security guidelines for a telephone exchange

Acquisition

NET.4.1.M2 Selecting a provider of communication services

NET.4.1.M13 Procedure for acquiring a telephone exchange

Operation

NET.4.1.M5 Telephone exchange logs

NET.4.1.M9 Training on the secure use of the communication system

NET.4.1.M10 Documentation and review of the configuration of the telephone exchange

NET.4.1.M12 Backup of configuration files

Emergency response

NET.4.1.M15 Emergency calls in the event of a failure of the telephone exchange

NET.4.1.M14 Emergency response of the telephone exchange

Implementation

NET.4.1.M7 Secure configuration of the telephone exchange

NET.4.1.M8 Limiting and blocking unnecessary or security-critical functions

NET.4.1.M16 Security of the client devices of the communication system

Disposal

NET.4.1.M11 The decommissioning procedure for telephone exchange and communication devices

Additional advanced measures

NET.4.1.M17 Security of the telephone exchange maintenance

NET.4.1.M18 Additional physical security

NET.4.1.M19 Duplication of connections

3.2 Key measures

NET.4.1.M1 Implementation plan for a telephone exchange [IT department]

a. An analysis of the requirements to the communication system is conducted before acquiring or extending a telephone exchange.

b. The purpose of using the telephone exchange and the expected functions are used as a basis for the analysis of the requirements.

c. As a result of the requirement analysis, the following is determined:

- the type and number of client devices;
- extendability;
- connections with a common phone network;
- the number of external lines;
- the concept of rights;
- management and configuration;
- security requirements;
- logging;
- backup;
- emergency response;
- customer support and maintenance agreements.

d. The implementation plan of the telephone exchange is documented and approved by the IT department.

NET.4.1.M2 Selecting a provider of communication services [IT department]

a. A contractual provider of communication services is selected, who connects the subscribers of the telephone exchange into a single phone network so it would be possible to make outgoing calls from the telephone exchange of the organisation.
b. When selecting a communication service provider, the following is taken into account:
- the requirements of the communication system;
- security requirements;
- experience of the provider;
- service quality;
- cost and tariffs.

c. A written contract is concluded with the provider for all communication services that are used.

NET.4.1.M5 Telephone exchange logs

a. As a minimum, the following call data is logged in the telephone exchange:
- time and date of the call or connection;
- source and destination phone number;
- duration of the call.

b. The management operations and changes in access rights of the telephone exchange are logged.
c. The logs of the telephone exchange are analysed regularly.

NET.4.1.M15 Emergency calls in the event of a failure of the telephone exchange

a. In the event of a communication system failure, the option for making external emergency calls is guaranteed (for example, by using a mobile phone).
b. Emergency calls can be made from all rooms.

3.3 Standard measures

NET.4.1.M6 Security guidelines for a telephone exchange [IT department]

a. Security guidelines for the telephone exchange are established based on the security policies of the organisation.
b. All persons related to the acquisition, installation, and operation of the telephone exchange comply with the security guidelines.
c. As a minimum, the security guidelines of the telephone exchange establish the following aspects of secure operation:

- logging of management security and management operations;
- authorised operation and maintenance tools;
- restrictions of access options;
- procedure for granting rights;
- installation of software updates and changes in the configuration;
- data backup and recovery;
- procedure for handling failures and security incidents.

NET.4.1.M7 Secure configuration of the telephone exchange

a. The telephone exchange is located in a room with a security level that complies with the requirements for a server room.
b. In order to ensure the operation of the communication services, the following aspects are taken into account in case of the telephone exchange infrastructure:
- stable power supply/surge protection;
- suitable microclimate;
- protection from water damage;
- fire safety;
- use of security doors and windows;
- connectivity with the alarm system.

c. The devices and device interfaces of the telephone exchange are protected from physical access (for example, locked and sealed).

NET.4.1.M8 Limiting and blocking unnecessary or security-critical functions

a. Only the necessary functions are activated.
b. Unnecessary telephone exchange functions or those enabling improper use are deactivated centrally.
c. The confidential data in client devices is sufficiently secured. If necessary, client devices with special programmable security functions are used.

NET.4.1.M9 Training on the secure use of the communication system [director]

a. The users of the communication system have passed the training on using the communication services and devices.

b. The user manuals of client devices are available to the users of the communication systems.
c. The users know whom to contact in the event of a failure of the communication system or a security event.

NET.4.1.M10 Documentation and review of the configuration of the telephone exchange [IT department]

a. The configuration of the telephone exchange and the list of phone numbers are documented and updated.
b. The configuration of the telephone exchange is checked regularly. During the review, the following is checked:

- whether the phone numbers and users match completely;
- whether unspecified phone numbers are really not in use;
- whether the deactivated functions and communication interfaces are unavailable for use;
- whether the configuration corresponds to the documentation;
- whether the management procedures are sufficient and their results have been documented;
- whether the data protection requirements are complied with.

c. The results of the review are reported to the information security manager, data protection specialist, and the person responsible for this area in the management board in addition to employees who are directly responsible for this issue.

NET.4.1.M11 The decommissioning procedure for telephone exchange and communication devices [IT department]

a. The decommissioning of a telephone exchange or communication devices takes place in accordance with the requirements of the general information security policy.
b. Before the telephone exchange or communication devices are decommissioned, all data is safely deleted.
c. The data that is essential for further work is backed up to an external data carrier or archived.
d. The decommissioned devices do not bear any labels or tags containing sensitive information (explanations to the speed dial buttons, etc.).

NET.4.1.M12 Backup of configuration files

a. A data backup concept has been prepared for communication systems, which is a part of the general data backup concept for servers and network components.
b. The first backup of the telephone exchange configuration and operational data is done immediately after the initial configuration.
c. The data (including the list of subscribers) is backed up regularly or immediately after changes in the configuration and operational data.
d. The recovery of the telephone exchange data with the backup copy is tested regularly.

NET.4.1.M13 Procedure for acquiring a telephone exchange

a. When acquiring a telephone exchange, the results of analysing the design and requirements for the communication system are taken into account (see also NET.4.1.M1 Implementation plan for a telephone exchange).
b. During the acquisition, the existing communication systems of the organisation and their components are considered. In the case of a partial update or addition to the communication system, the compatibility of the old and new devices is observed.
c. When updating the communication system (e.g. when the analogue communication systems are extended or replaced with IP systems and devices), the additional logging and security requirements are taken into account.

NET.4.1.M14 Emergency response of the telephone exchange

a. An emergency response plan for the telephone exchange is prepared, which is a part of the general emergency response concept of the organisation (see also DER.4 Emergency management).
b. Guidelines for acting in typical failure situations are prepared.
c. Spare equipment is ready to replace the critical components of the communication system.
d. The emergency response plan of the telephone exchange is regularly tested based on scenarios; the results of the testing are documented.

NET.4.1.M16 Security of the client devices of the communication system

a. The inactive data exchange interfaces (such as Bluetooth) of client devices and unnecessary functions are deactivated.
b. The functions of the phones in freely accessible rooms are suitably restricted and the configuration of the phones is protected with a password or a PIN.

c. The sensitive data in the client devices is sufficiently secured.
d. The users of the devices are responsible for ensuring the security of the client devices. The users are trained accordingly.

3.4 Advanced measures

NET.4.1.M17 Security of the telephone exchange maintenance (C-I)

a. The tools for telephone exchange maintenance and configuration are password-protected.
b. The telephone exchange can only be accessed from specialised maintenance computers which are located in a separate security zone.
c. If a separate cable is not used for IP-based access, the IP data communication is encrypted.
d. A device that is handed over for repairs does not contain sensitive information.

NET.4.1.M18 Additional physical security (C-I)

a. The telephone exchange is located in a separate and secure room.
b. Entrance to the telephone exchange room is only allowed to a limited group of people.
c. Outsiders can access the telephone exchange only with an appointed chaperone.
d. Any outsiders entering the room are registered (name, company, time).

NET.4.1.M19 Duplication of connections (A)

a. The external connection of the telephone exchange is duplicated.
b. A communication system that is based on IP is additionally and securely connected to the analogue telephone network.

NET.4.2 IP phone (VoIP)

1 Description

1.1 Purpose

To present the measures for ensuring the security of the components of a VoIP-based communication system and the calls made from an IP phone.

1.2 Responsibility

The IT department is responsible for the implementation of IP phone measures.
Additional responsible persons: User, information security manager.

1.3 Limitations

The security measures of a traditional telephone exchange are discussed in the module NET.4.1 Telephone exchange.
The security of the data connection is discussed in the modules NET.1.1 Network architecture and solution, NET.1.2 Network management, and NET.3.2 Firewall.
If an IP phone is used as a software phone located in the client computer, the measures of the module SYS.2.1 Client computer in general and modules related to operating systems are implemented.
If the VoIP-based communication system software is used in a server, the measures of the module SYS.1.1 Server in general are also complied with in addition to the modules related to the operating systems.
In case of a VoIP-based communication system, the modules ORP.4 Administration of identity and rights, OPS.1.1.2 IT management, OPS.1.1.3 Patch and change management, and OPS.1.1.5 Logging are also taken into account.

2 Threats

2.1 Configuration errors of the middleware of a VoIP-based communication system

Usually, several IT systems are used for connecting to an IP phone. If SIP is used as the initialisation protocol, data connection requires such systems as registrars, SIP proxy servers, and location servers. Configuration errors could easily occur when the infrastructure of the VoIP-based communication system is changed (for example, phone numbers might be incorrectly dialled by accident).

2.2 Incorrect configuration of the components of the VoIP-based communication system

Regardless of whether the VoIP-based communication system is built on a system that uses specialised hardware of software, the correct configuration for the compliant operation of the phone system is essential. In addition to the signalling settings, the methods and settings of media transmission and data packing are important. If an unsuitable method is used or the call data is

packed too extensively, the call quality drops. If a method is selected that packs the data too little, the data communication network might be overloaded.

2.3 Surveillance of calls

If the phone calls or data are forwarded without encryption, an attacker can eavesdrop on the calls or record the data. Eavesdropping on phone calls and data transmission is easier in a VoIP-based communication system than in a traditional phone communication system because media streaming with the real-time transport protocol (RTP) is used for the call. An attacker has many different possibilities for attacking the data connection network by using spoofing or sniffing methods.

2.4 Improper use of phone connections

If the organisation has IP phones which are in locations accessible to visitors or are not linked to a specific user, the IP phones can be improperly used for causing damage or for personal gain. An attacker could use the vulnerabilities of the IP phone and install malware when they gain access to the device. In addition, the network connection of the IP phone can be used for connecting to other components of the communication system and access the intranet this way.

3 Measures

3.1 Life cycle

Planning

NET.4.2.M1 Implementation plan of a VoIP-based communication system

NET.4.2.M7 Security guidelines for a VoIP-based communication system

NET.4.2.M8 VoIP communication encryption

Operation

NET.4.2.M3 Secure management of a VoIP-based communication system

Implementation

NET.4.2.M4 Restricting access to the VoIP-based communication system

NET.4.2.M5 Secure configuration of the middleware

NET.4.2.M11 Secure use of IP phones

NET.4.2.M13 Firewall of an IP phone

Acquisition

NET.4.2.M9 Procedure for selecting the components for a VoIP-based communication system

Disposal

NET.4.2.M12 Secure decommissioning of the components of a VoIP-based communication system

Additional advanced measures

NET.4.2.M14 Encryption of signalling

NET.4.2.M15 Security of the SRTP protocol

NET.4.2.M16 Separating the data communication network and VoIP network

3.2 Key measures

NET.4.2.M1 Implementation plan of a VoIP-based communication system

a. Before the commissioning of IP phones, an implementation plan for a VoIP-based communication system is prepared.

b. It determines whether the IP phones are used exclusively or partly and how the VoIP-based communication system is connected to the public (data) communication network.

c. The implementation plan for a VoIP-based communication system establishes:

- the recommended functions;
- requirements for availability, integrity, and confidentiality;
- signalling and transport protocols;
- the presumed number of users;
- the extent of encryption and cryptographic mechanisms;
- the principles for selecting components;
- configuration and management;
- the organisation of logging.

d. The commissioning plan considers the capacity and structure of the existing data communication networks.

NET.4.2.M3 Secure management of a VoIP-based communication system

a. Unnecessary functions of the VoIP-based communication system are deactivated.

b. The configuration of the VoIP-based communication system is protected from unauthorised changes.

c. All security mechanisms of the VoIP-based communication system are activated. The functioning

of security mechanisms is tested before taking the IP phones into use.
d. The implemented security mechanisms and configuration are documented.

NET.4.2.M4 Restricting access to the VoIP-based communication system

a. IT systems cannot establish direct connections from insecure networks with the components of the VoIP-based communication system.
b. If the VoIP-based communication system is used for connecting directly to a public data communication network, all signalling and call data is forwarded only through a concentrator in the demilitarised zone.

NET.4.2.M5 Secure configuration of the middleware

a. The default configuration of the components and middleware of the VoIP-based communication system is adjusted based on the protection requirement of the data exchange before commissioning.
b. All installation and configuration stages are documented in such a way that a competent third person is capable of configuring the middleware purely based on the documentation.
c. The macros for automating the configuration are thoroughly tested and documented.
d. All unnecessary services of the middleware of the VoIP-based communication system are deactivated.

3.3 Standard measures

NET.4.2.M7 Security guidelines for a VoIP-based communication system [information security manager]

a. Guidelines for a VoIP-based communication system are established based on the general security policy of the organisation, presenting the requirements for the operation and use of the components of the VoIP-based communication system.
b. As a minimum, the following is included in the security guidelines for the VoIP-based communication system:

- the potential risks of the use of the VoIP-based communication system;
- requirements for the secure use of IP phones;
- allowed functions, services, protocols, and connections;
- roles, rights, and obligations;
- the organisation of the management, maintenance, and auditing of the VoIP-based

communication system;

- the requirements for the acquisition and updating of components;
- requirements for the documentation of activities.

c. All managers of the VoIP-based communication system comply with the security guidelines for the VoIP-based communication system.

NET.4.2.M8 VoIP communication encryption

a. The instances of obligatory encryption of the VoIP communication are established.
b. The entire outgoing IP phone communication from the secure local area network is encrypted with suitable security mechanisms (SRTP, TLS).
c. If the VoIP communication is not encrypted, the users are aware of it and avoid forwarding any confidential data.

NET.4.2.M9 Procedure for selecting the components for a VoIP-based communication system

a. A specification of requirements for choosing the components of the VoIP-based communication system has been prepared.
b. As a minimum, the specification of the requirements contains the following:

- general requirements (infrastructure, compatibility, support for protocols, capacity);
- logging requirements (level of detail, security, data protection requirements);
- update and patch requirements;
- management requirements (support for protocols, management interface);
- encryption requirements.

c. A procedure for comparing the components of the VoIP-based communication system has been established.

NET.4.2.M11 Secure use of IP phones [user]

a. The users of the IP phones know the main threats and security measures of VoIP communication.
b. An IP phone that is left without supervision is locked. Unlocking requires entering a password with sufficient strength.
c. Calling emergency numbers is possible even with an activated password protection.
d. The users know who must be informed about the security events and how.

NET.4.2.M12 Secure decommissioning of the components of a VoIP-based communication system

a. Before the decommissioning of the components of the VoIP-based communication system, all sensitive data is deleted securely from the devices.
b. After the data is deleted and/or the factory settings of the components are restored, the success of deleting the data is checked.
c. Before decommissioning the IP phones, labels and tags with sensitive information are removed from the devices.

NET.4.2.M13 Firewall of an IP phone

a. When designing a VoIP-based communication system, it is decided whether it is sufficient if the existing firewall is adjusted for the VoIP communication or an additional firewall is acquired and installed.
b. A firewall with the functions similar to an application level gateway is used for filtering the RTP traffic.

3.4 Advanced measures

NET.4.2.M14 Encryption of signalling (C-I)

a. In order to guarantee the integrity and confidentiality of the VoIP-based communication system, the signalling information is forwarded through encrypted VPN channels or with signalling protocols that have their own security mechanisms (SIP, H.225).
b. If the signalling protocol does not have enough security mechanisms, security mechanisms form the levels below the application level (transport or network layer) are implemented.
c. In case of a high protection requirement, the signalling protocol SIP (session initialisation protocol) is used along with the TLS protocol.
d. Encryption is compliant with the module CON.1 Cryptography concept.

NET.4.2.M15 Security of the SRTP protocol (C-I)

a. The transport protocols of the VoIP-based communication system - RTP (real-time transport protocol) and RTCP (RTP control protocol) - are protected with the encrypted versions of the protocols (SRTP and SRTCP).

b. The master key of the encryption and authentication of the SRTP (secure real-time transport protocol) has a size of at least 128 bits and is generated with secure means (such as the MIKEY key management protocol).
c. The authenticity and integrity of the RTP messages is protected by a sufficiently strong hash function (such as HMAC-SHA2).
d. A counter of authentic SRTP packets is used. Recurrent packets are discarded in case of a replay attack.
e. The selection and reasons of the cryptographic mechanisms and parameters and the hash algorithm are documented.

NET.4.2.M16 Separating the data communication network and VoIP network (C-I-A)

a. The VoIP network is separated from the data communication network physically with firewall or at least with a VLAN (virtual local area network).
b. The actions regarding devices which need access to both VoIP and data communication networks have been decided (such as computers with an IP phone client application that is a piece of software).
c. Only IP phone connections are allowed in a port that is connected to an IP phone of a VoIP network switch.
d. Depending on the protection requirement, additional measures are applied to protect the VoIP network (such as authentication compliant with IEEE 802.1X).

SYS: IT SYSTEMS

SYS.1 Server

SYS.1.1 Server in general

1 Description

1.1 Purpose

To provide the measures for the protection of the data processed in the servers and the server services related thereto.

The module is used for server systems irrespective of the operating system of the server. The measures of the module can be used for both separate physical servers and virtual servers.
In this module, server services mean the main background services for the functioning of the local area network as well as the services designed for the user which enable exchanging emails and using a group printer, for example.

1.2 Responsibility

The IT department is responsible for the implementation of the measures of the module 'Server in general'.
Additional responsible persons: The information security manager, the technology department, the procurement department.

1.3 Limitations

The measures in this module are applied to all servers. If a separate E-ITS module has been developed for a server service or an IT system, the specific module is considered first, and only then this module. Where a separate module does not exist for a server service, measures from this module are applied to the server service and an additional risk assessment of the target object is completed.
The secure management of a server is discussed in modules OPS.1.1.2: IT systems management and OPS.1.1.3 Patch and change management. The safe placement of a server in a network is described in module NET.1.1 Network architecture and solution.
The server is also subject to additional measures from the following modules: ORP.4 Administration of identity and rights, DER.4 Emergency management, and OPS.1.1.4 Protection against malware.

2 Threats

2.1 Inadequate planning for commissioning a server

A server is a complex IT system with many functions and configuration options as a rule. The standard configuration of a server might be insufficiently safe. If the configuration of a server is not changed before commissioning, it will be much more complicated to harden the security when the server is in use, so this operation is often neglected. An insufficiently configured server leaves a lot of possibilities for attackers to complete successful attacks.

2.2 Inadequate management of a server

Server software is constantly upgraded and manufacturers add new functions. Therefore, server configurations need constant reviews and adjustments. If the IT department fails to handle this consistently, the security of the server may weaken. Mistakes may also be made as a result of human errors made in the course of configuration. Administration errors may cause failures in the functioning of a server, affecting the security of the system, among other things.

2.3 Unlawful acquisition or abuse of administrative privileges

If an administrator uses an account with administrator privileges (a privileged account) for their daily operations, there is a high risk of an attacker being able to hijack the privileged account. Extensive rights are usually granted to privileged accounts, and thus, abuse of such accounts may have a great impact. For example, extensive damage may be caused by taking over the account of a domain manager. The attacker may also acquire a password required for using an account without guessing the passwords or using a brute-force attack if they manage to gain access to the password hash.

2.4 Data loss

Data saved in central servers must be accessible if necessary. Loss of data may have a significant and long-term impact on the business processes of an organisation, depending on how critical the data is and whether or not back-up copies have been made. Data loss may also cause other damage in addition to the expenses of recovering the lost data, such as losing customers or partners, legal consequences arising from breaking the law, and damage to reputation. Loss of archived data may also result in serious consequences. The direct and indirect damage caused by this may even threaten the survival of the organisation.

2.5 Denial-of-service attacks

In the event of a denial-of-service attack, an attacker attempts to prevent the use of server services by overloading the system or network connection. IT systems are usually interdependent and the lack of resources in one server may have an impact on the functioning of other servers. If no measures to alleviate the impact of a denial-of-service attack have been planned, the resources and services of the server may become inaccessible.

2.6 Useless operating system components and applications

The operating system of a server includes many default applications and services, some of which are not needed. Software components which are actually not necessary may also be added by installing software. Administrators often do not have a clear understanding of which unnecessary applications are needlessly burdening a server.

2.7 Server overload

Overloading a server may interfere with availability, as numerous simultaneous queries burden the system excessively and the server service will thus become temporarily inaccessible. Data may be lost as the memory capacity at the disposal of the server has been exceeded and the database server is unable to perform an operation within an established time frame. If a server is no longer compliant with the needs of an organisation, overloading the server may also result in failures of other servers in the case of a complex IT environment.

3 Measures

3.1 Life cycle

Implementation

SYS.1.1.M1	Restricting access to a server
SYS.1.1.M2	Authentication of users
SYS.1.1.M5	Protection of administrative interfaces
SYS.1.1.M6	Deactivation of unnecessary services
SYS.1.1.M16	Secure installation and baseline configuration of a server

Operation

SYS.1.1.M9	Use of anti-malware applications on the server
SYS.1.1.M10	Server logging
SYS.1.1.M19	Local packet filters
SYS.1.1.M21	Drawing up the operating documentation of the server
SYS.1.1.M23	Monitoring the server system
SYS.1.1.M24	Regular security testing
SYS.1.1.M34	Hard disk encryption
SYS.1.1.M35	Administration of the operating documentation of the server
SYS.1.1.M36	Security of server booting

SYS.1.1.M37 Encapsulation of security-critical applications and components of operating systems

SYS.1.1.M39 Central management of the security settings of a server

Planning

SYS.1.1.M11 Establishing security guidelines for servers

SYS.1.1.M12 Server deployment plan

SYS.1.1.M15 Uninterrupted and stable power supply

Procurement

SYS.1.1.M13 Procurement of a server

Emergency response

SYS.1.1.M22 Integration with emergency response

Disposal

SYS.1.1.M25 Procedure for the decommissioning of the server

Additional advanced measures

SYS.1.1.M27 Host-based intrusion detection

SYS.1.1.M28 Redundancy

SYS.1.1.M30 One service per server

SYS.1.1.M31 Preventing the operation of applications

SYS.1.1.M33 Active root certificate administration

SYS.1.1.M38 Enhanced protection of server system files

3.2 Key measures

SYS.1.1.M1 Restricting access to a server [technical department]

a. Only individuals with access privileges have access to the physical location of a server.
b. Servers are located in a computer centre, in a locked server room, or in a locked equipment cabinet (see INF.5 Technical infrastructure room or cabinet).
c. Only authorised persons have access to virtualised server configuration and resources.
d. A server is not used as a workstation or for performing work tasks that can be completed in a client computer. First and foremost, using a web browser and web applications in a server must be avoided.
e. A computer which is designed to be used as a workstation is not used as a server.

SYS.1.1.M2 Authentication of users

a. If possible, central authentication processes are used for authentication of the server system.
b. The user is only authenticated into the server by using their personalised user account.
c. Authentication of the users depends on the protection requirement of the server. In the case of a high protection requirement, multifactor authentication is used.
d. The administrative rights to the server are restricted based on needs. For daily work, the administrators use user accounts with restricted rights.

SYS.1.1.M5 Protection of administrative interfaces

a. The external devices and data media of the server are only used for the maintenance of the server.
b. Server booting from a CD/DVD device or a removable storage device is deactivated in the BIOS.
c. A special administrative network separated from the rest of the network is created for remote administration. If there is no such network, only secure protocols (SHH, HTTPS) are used for remote administration).
d. Any useless interfaces in the server have been deactivated.

SYS.1.1.M6 Deactivation of unnecessary services

a. Any useless services (especially network services) and applications have been deactivated or uninstalled from the server.
b. All useless server component firmware functions are deactivated.
c. The storage space allocated to the user and application in the server is limited by a disk quota.
d. The configuration of the software, services, and accounts of the server is documented.

SYS.1.1.M9 Use of anti-malware applications on the server

a. The necessity and feasibility of the anti-malware application of the server are determined based on the operating system of the server, the server services, and the security mechanisms of the server.
b. The anti-malware application used in the server is also capable of scanning packed data for malware, in addition to real-time scanning and scanning on demand.

SYS.1.1.M10 Server logging

a. The events logged in the server, the persons having access to the log data, and the terms and conditions of such access have been specified and documented.
b. A decision has been made on whether to store the log data in the server or use a central log server.

c. All events significant from the perspective of information security are logged, incl. at least the following:

- system activation and booting;
- logins and login attempts into the operating system and applications;
- attempts to exceed the limits of rights;
- attempts to breach access lists or firewall rules;
- creation or alteration of users, user groups, and rights;
- security-related failure messages (e.g. power cuts, hardware failures, exceeding of capacities);
- warning messages of security mechanisms (e.g. messages from the anti-malware application).

3.3 Standard measures

SYS.1.1.M11 Establishing security guidelines for servers

a. Security guidelines for a server have been documented and enforced based on the general security policy of the organisation. The differing protection requirements of servers are taken into consideration in security guidelines.
b. All employees involved in the procurement, administration, or operation of the server comply with security guidelines.
c. As a minimum, the security guidelines of a server cover the following:

- regulation of physical access;
- virtualisation (see SYS.1.5 Virtualisation system);
- the organisation of administration and auditing;
- installation and baseline configuration;
- encryption of files;
- documentation;
- requirements for secure handling;
- password requirements;
- security of communication and network services;
- logging.

d. Compliance with the requirements of the guidelines is checked regularly and the results are documented.

SYS.1.1.M12 Server deployment plan

a. The following is taken into consideration in planning the deployment of a server:

- the hardware platform, operating system, and application software;
- the suitability of the hardware parameters (performance, memory, capacity, etc.);
- the space requirement and structure type;
- the energy consumption and heat emission;
- the type and number of communication interfaces;
- organisation of administration (see SYS.1.1.M5 Protection of administrative interfaces):
- the access rights of the users;
- logging (see SYS.1.1.M10 Logging);
- monitoring;
- updating the IT components of the server;
- integration with the existing network management, data backup, and information security (e.g. anti-malware software, anti-intrusion system) solutions.

b. The decisions made in the course of planning the deployment of a server are documented.

SYS.1.1.M13 Procurement of a server [procurement department]

a. For the procurement of a server, the technical specifications of the requirements are drafted and the criteria for comparing products are defined:

- physical parameters (dimensions, fitting into the server cabinet);
- functionality requirements (the hardware interfaces required, compatibility);
- reliability and administrator-friendliness (reliable information from an independent source);
- administration (manufacturer's support and maintenance contract);
- total cost (acquisition and fixed costs).

b. The following requirements have been established from the perspective of information security:

- sufficient availability and integrity of the data;
- secure protocols for data management;
- compatibility with the administration of rights and the organisation-wide security concept.

SYS.1.1.M15 Uninterrupted and stable power supply [technical department]

a. All servers are connected to an uninterruptible power supply (UPS) with a sufficient capacity and battery life.

b. The management of the uninterrupted power supplies is compliant with the measure INF.2.M3 Uninterruptible power supply (UPS).

SYS.1.1.M16 Secure installation and baseline configuration of a server

a. The system and application software for a server is only purchased from authentic and reliable sources.
b. The installation and configuration of a server is conducted in an installation environment that is separated from the production environment.
c. The configuration of a server is based on the recommendations of its manufacturer and the recommended configuration, presuming that it is sufficiently secure and does not contradict the needs and requirements of the organisation.
d. The basic configuration of a server is documented even if the default settings of the manufacturer are used.
e. The basic configuration of a server complies with the requirements of the security guidelines. Security settings are checked before the deployment of a server and each time after making changes in the server.
f. Only services which are required for fulfilling the purpose of a server are installed.
g. If an internet connection is required for operating a server, the server is connected to the internet after installation and configuration are completed.

SYS.1.1.M19 Local packet filters

a. Servers with a high protection requirement are protected with a local (operating system level) packet filter.
b. Upon adding the server to the network, the packet filter is activated with the baseline configuration (all connection attempts are rejected).
c. The local packet filter of the server only accepts data communication sessions with the predefined communication partners. Any unnecessary protocols, ports, and interfaces are blocked.
d. The ICMP protocol messages are filtered selectively, as full blocking of the ICMP may cause network failures which are difficult to diagnose.
e. The configuration of a packet filter is checked regularly and adjusted, if necessary.

SYS.1.1.M21 Drawing up the operating documentation of the server

a. The operations, individuals performing the operations, and outcomes of the operations are documented comprehensibly in the operational documentation of the server.
b. All configuration changes can be traced based on the documentation.

c. All safety-related operations are documented.
d. All activities concerned with the operation of the server which can be documented automatically are logged automatically.

SYS.1.1.M22 Integration with emergency response

a. The business continuity concept of the organisation includes the backup and recovery of the servers. (see DER.4 Emergency management).
b. A server data recovery plan has been developed for the servers.
c. An emergency recovery plan has been documented and enforced for recovering and restarting the server services which affect business continuity.
d. The recovery plan establishes the procedure for the secure use and storage of the passwords and encryption keys needed for recovery.
e. The implementation of the recovery plan is regularly practised.

SYS.1.1.M23 Monitoring the server system

a. The status of the server systems, the servers, and the services operated in the servers are monitored by constant monitoring tools.
b. Any occurrences of exceeding established thresholds and all failures are immediately reported to the administrators of the server.

SYS.1.1.M24 Regular security testing

a. In order to detect and prevent network attacks, the security of the servers with external interfaces is tested at least once a month.
b. Compliance of the intranet servers to the security policy is checked regularly.
c. At least the following is checked in the course of security testing:
- compliance with the password policy;
- user accounts which remain passive for prolonged periods of time;
- compliance of the rights with the system established;
- configuration of the system programs;
- network services and the configuration thereof;
- the functioning of automatic monitoring.

d. If possible, automated tools (testing tools and scripts) are used to conduct server security checks.
e. The results of the checks are documented and deviations are handled as soon as possible.

SYS.1.1.M25 Procedure for the decommissioning of the server

a. Users of a server (physical server or virtual server) are notified of the decommissioning of the server well in advance.
b. A checklist of operations has been drawn up for the disposal of a server which covers at least the aspects of backing up the data, transfer of the services, and the secure deletion of the data.
c. An overview of the data in the server and the intended new locations is drawn up before disposal of a server.
d. Important data is backed up before the decommissioning of a server.
e. It is ensured that the services provided by the server are taken over by another server, if necessary. The migration of a heavily used server is first tested in the testing environment.
f. Upon the decommissioning of a server, it is ensured that no sensitive data remains on the data media.

SYS.1.1.M34 Hard disk encryption

a. The data media of the server (e.g. hard disks) are encrypted by reliable means.
b. The data media containing virtual machines (data arrays or hard disks) are encrypted.
c. The encryption keys and passwords are sufficiently strong and protected. In addition to the TPM (Trusted Platform Module), other measures are also used to protect the encryption key.
d. The disk script recovery password is stored in a secure location (e.g. password repository).

SYS.1.1.M35 Administration of the operating documentation of the server

a. The operating documentation of the server is drawn up for all standard servers. The documentation includes the information security requirements and the requirements arising from legislation.
b. The operating documentation of a server is protected from unauthorised access. In an emergency situation, authorised persons have access to the operation documentation.
c. The operating documentation of a server is updated regularly.

SYS.1.1.M36 Security of server booting

a. Only administrators can change server booting settings. Access to the configuration interface of the firmware is at least password-protected.
b. The server operating systems supporting UEFI SB (Secure Boot) are used.
c. UEFI Secureboot is activated. The bootloader and kernel of the operating system are signed with a key which enables SecureBoot integrity checks during booting.
d. Useless keys are removed from the server.

SYS.1.1.M37 Encapsulation of security-critical applications and components of operating systems

a. The security-critical data of applications and operating systems (e.g. authentication and certificate data) is encapsulated to prevent the access of other application or operating system components or isolated into a separate execution environment.
b. Those applications which process data originating from unreliable sources (e.g. web browsers) are activated in an execution environment which is separated from the operating system.

SYS.1.1.M39 Central management of the security settings of a server

a. Server configuration is stored in a central management system (see OPS. 1.1.7 Systems management).
b. The security settings of a server comply with the established security policies and guidelines. Exceptions are documented along with justifications.

3.4 Advanced measures

SYS.1.1.M27 Host-based intrusion detection (I-A)

a. Host-based intrusion detection systems (HIDS) and/or host-based intrusion prevention systems (HIPS) are used for the detection of anomalies and attacks. If enough log information is available in the SIEM (security information and event management) solution, the SIEM solution may be used instead of the host-based intrusion detection systems.
b. In order to detect anomalies, the following is checked regularly (e.g. every night):
- the integrity of the configuration of the server system;
- potential changes in the file system;
- permissibility of the processes processed in the main memory.

c. The intrusion response / intrusion prevention mechanisms used are appropriately configured and

thoroughly tested.
d. A procedure has been established for reporting anomalies and handling anomalies.
e. The resources of the operating system of the server are also used to detect any changes in the system files or configuration settings (e.g. in the Windows registry file).

SYS.1.1.M28 Redundancy (A)

a. High availability of the server system is ensured by adding redundancy.
b. The server system maintenance contracts concluded with external suppliers and service providers are based on heightened requirements for availability.
c. One of the following options is used to ensure server system redundancy:
- cold standby;
- manual switchover or hot standby;
- load balancing cluster;
- failover cluster.

d. The cost-efficiency of the architecture is kept in mind in creating an architecture which ensures redundancy.
e. In the event of a very high availability requirement, a cluster of servers in different physical locations which enables emergency switching is used.

SYS.1.1.M30 One service per server (C-I-A)

a. As a general rule, each physical or virtual server only enables the use of one server service.
b. In exceptional cases, the reasons are documented.
c. No other services but the virtualisation software and the immediately related services (the administration service of virtualisation, etc.) are operated in the virtualisation server.

SYS.1.1.M31 Preventing the operation of applications (C-I)

a. Only allowed programs and scripts can be operated in a server. The list of allowed programs is as limited as possible.
b. The list of allowed programs is based on the verification of certificates, comparison of hashes and/or allowed directory paths.

SYS.1.1.M33 Active root certificate administration (C-I)

a. The list of the root certificates required for the functioning of the server is documented.
b. Only those root certificates which are required for the functioning of the server and have been documented in advance are installed in the server.
c. The instructions from the source of the software product are taken into use in the administration of root certificates. The appropriateness of the root certificates is checked regularly.

SYS.1.1.M38 Enhanced protection of server system files (I)

a. Only read-only access is granted to server system files to ensure integrity.

SYS.1.2 Windows Server

SYS.1.2.2 Windows Server 2012

1 Description

1.1 Purpose

To present the measures for the safe implementation of the Windows Server 2012 and Windows Server 2012 R2 operating systems and for the protection of the data processed in the server system and the processes.

1.2 Responsibility

The IT department is responsible for implementation of the measures of the module 'Windows Server 2012'.

1.3 Limitations

The module complements the module SYS.1.1 Server in general with the specificities and specifications characteristic of Windows Server 2012. The measures described under the module are not based on the exact use of the servers.
If both versions are kept in mind, Windows Server 2012 is referred to. Attention is drawn separately to the differences of the R2 version. The periods of the extended manufacturer's support of both operating systems will expire on 10 October 2023 (the expiry of the service life of the product). The

module can also be used with newer Windows server operating systems, to a limited extent.
The module presumes the integration of the server with Active Directory, the security of which is described in the module APP.2.2 Active Directory.
The server roles related to the Microsoft Server 2012 are described under other modules (e.g. APP.3.3 File server, APP.3.2 Web server, APP.5.2 Microsoft Exchange and Outlook, SYS.1.5 Virtualisation system).

2 Threats

2.1 Insufficient planning of the implementation of Windows Server 2012

Windows Server 2012 is a complex operating system with numerous functions and configuration options. Each function added increases the likelihood of vulnerabilities and configuration errors. Even though the default settings of the modern Windows versions have become more secure, the standard configuration still includes many security vulnerabilities. If the level of security of the baseline configuration of Windows Server 2012 is not increased before the deployment of the server, it will be much more difficult to increase the security when the server is in used and it is often foregone. Insufficiently configured Windows Server 2012 leaves a lot of possibilities for attackers to complete successful attacks.

2.2 Thoughtless use of cloud services

Windows Server 2012 may use cloud services (e.g. Microsoft Azure Online Backup) without specific software. Cloud services may provide certain advantages (such as availability), but pose a threat to confidentiality in the case of thoughtless use and come with dependence on the service providers. Persons with malicious intent may gain access to the data via the cloud service.

2.3 Insufficient management of a Windows server

Compared to the previous versions of Windows Server, Windows Server 2012 has many new security functions. If the managers have not received a training on the secure implementation of Windows Server 2012, configuration errors may occur. Mistakes may also be made as a result of human errors made in the course of configuration. Administration errors may cause failures in the functioning of the server, affecting the security of the system, among other things.

2.4 Insufficient implementation of group policy

Group policy is a useful and efficient tool for configuring many (security) aspects of Windows Server 2012. If a domain includes many servers and workstations for different purposes, the rules established by the group policy may easily become conflicting or incompatible. This may cause malfunctioning, as well as security vulnerabilities of the server or the clients, in the worst case.

2.5 Loss of integrity of the information or a process which requires protection

If the integrity protection functions of Windows Server 2012 have not been applied due to a configuration error or to ensure user convenience, malicious employees or external attackers may falsify the data in the server and then erase traces of manipulation. Specific malware may be used to gain remote access.

2.6 Unlawful acquisition or abuse of administration rights

If the manager uses an account with administrator's rights (a privileged account) for their daily operations, there is a high risk of an attacker being able to hijack the privileged account. Extensive rights are usually granted to the privileged accounts and therefore, abuse of such account may have a great impact. Extensive damage can be caused by taking over the account of the manager of the domain. The attacker may also acquire the password required for using the account without guessing the passwords or using a brute-force attack, if the man age to gain access to the password hash.

2.7 Intrusion via remote access

An attacker may gain remote access to a server if insecure protocols are used (unprotected RDP) or due to weaknesses of the authentication method (weak passwords), and such remote access can be used to attack the server and other systems connected to the server.

3 Measures

3.1 Life cycle

Planning

SYS.1.2.2.M1 Windows Server 2012 deployment plan

Implementation

SYS.1.2.2.M2 Secure installation of Windows Server 2012

SYS.1.2.2.M4 Secure configuration of Windows Server 2012

SYS.1.2.2.M8 Protection of the integrity of the system

Operation

SYS.1.2.2.M3 Secure administration of Windows Server 2012

SYS.1.2.2.M5 Anti-malware

SYS.1.2.2.M6 Secure administration of rights and secure authentication of Windows Server 2012

Additional advanced measures

SYS.1.2.2.M11 Intrusion detection

SYS.1.2.2.M12 Redundancy and tools of advanced availability

SYS.1.2.2.M14 Switching off an encrypted server and virtual machine securely

3.2 Key measures

SYS.1.2.2.M1 Windows Server 2012 deployment plan

a. A deployment plan has been drafted for the implementation of the server operating systems (incl. Windows Server 2012).

b. The Windows Server 2012 deployment plan determines:

- the purpose of the implementation;
- the requirements for the hardware;
- integration with Active Directory;
- the organisation of backup.

c. A decision has been made on whether Windows Server 2012's cloud services integrated with the operating system must be blocked before the deployment of Windows Server 2012.

SYS.1.2.2.M2 Secure installation of Windows Server 2012

a. Only the required server-related roles and role-related functions and attributes are installed.

b. If the needs are limited, the minimum version, Server Core, is installed. There are written justifications for adding other functions.

c. Appropriate Windows Server 2012 updates and security patches are installed immediately after downloading the operating system from the installation medium.

d. If cloud accounts are not needed, the Microsoft cloud accounts of the users are blocked.

SYS.1.2.2.M3 Secure administration of Windows Server 2012

a. The password of the local administrator account is unique and secure.
b. The administrators of the server system are familiar with the server security aspects and have passed a Windows Server 2012 or R2 training.
c. The training for system administrators includes the following topics:

- regulation and control of access to resources;
- administration of the Active Directory certificate services;
- analysis and administration of the server processes and performance;
- administration of user accounts;
- administration of cryptography tools;
- transfer and deletion of files;
- analysis and administration of server policies;
- the diagnostics, planning, and ensuring the security of the systems.

d. The browsers in the server are not used for surfing (especially on the Internet).

3.3 Standard measures

SYS.1.2.2.M4 Secure configuration of Windows Server 2012

a. Each server usually only performs one function or server role. The roles are appropriately divided between different servers.
b. Before adding to the operation environment, the server is thoroughly hardened. System-specific templates for configuring security parameters are used for this purpose.
c. Internet Explorer is only used with the ESC (Enhanced Security Configuration) and EPM (Enhanced Protected Mode) settings in the server.

SYS.1.2.2.M5 Anti-malware

a. The anti-malware application is installed on the server before making the first network connection. Until the implementation of the designed anti-malware solution, Windows Defender is activated in the server.
b. In exceptional cases, autonomous windows Server 2012 servers without a network connection and with no removable media may be used without an anti-malware program.
c. The operating drives of the server are scanned regularly to detect malware.
d. The anti-malware application automatically reports any malware detected to the designated persons.

SYS.1.2.2.M6 Secure administration of rights and secure authentication of Windows Server 2012

a. All users of the Windows Server 2012 R2 are included in the 'Protected Users' (PU) security group.
b. The service accounts of Windows Server 2012 are included in the 'Managed Service Accounts' (MSA) group. Service and computer accounts are not in the 'Protected User' group.
c. The PPL protection of the local security centre LSA (Local Security Authority) is activated.
d. DAC (Dynamic Access Control) is used for the dynamic management of the access rules of resources.
e. A workstation with restricted rights is used for the administration works of Windows Server 2012.

SYS.1.2.2.M8 Protection of the integrity of the system

a. In order to regulate the use of applications, the AppLocker is configured as restrictively as possible and activated. If there is no AppLocker support, the SRP (Software Restriction Policies) feature is used.
b. Regulation of the use of applications is reinforced through group policy objects (GPO).

3.4 Advanced measures

SYS.1.2.2.M11 Intrusion detection (C-I-A)

a. The security events of Windows Server 2012 are collected and analysed centrally.
b. At least the following is logged and analysed in the case of the servers with the Windows Server 2012 operating system:

- deletion of security logs;
- changes in the administrators and other important user groups;
- adding and removal of local server users;
- adding new services.

c. Encrypted sections are locked after a certain number of decryption attempts.

SYS.1.2.2.M12 Redundancy and tools of advanced availability (A)

a. Depending on the protection requirement, the following high availability measures supported by the operating system are applied:

- DFS (Distributed File System);
- ReFS (Resilient File System);
- failover cluster;
- load balancing;
- network card groups (NIC-Teaming, LBFO).

b. The BranchCache added functionality is activated in remote locations.

SYS.1.2.2.M14 Switching off an encrypted server and virtual machine securely (C-I)

a. Any physical or virtual servers which are not currently in use are switched off. The hibernate mode of the server may not ensure sufficient protection.
b. In order to activate the server (and decrypt the data), the manager must enter their password and the operation is registered in the security log.

SYS.1.2.3 Windows Server

1 Description

1.1 Purpose

To present the measures for the secure implementation of the server operating systems Windows Server 2016, Windows Server 2019, and Windows Server 2022 (hereinafter 'Windows Server') which are based on Microsoft Windows 10 code, and for the protection of data processed in the server system and its processes.

1.2 Responsibility

IT department is responsible for the implementation of the measures of the module Windows Server.

1.3 Limitations

This module complements module SYS.1.1 Server in general with specifics and clarifications about Windows Server 2016, Windows Server 2019, and Windows Server 2022.
The measures described in the module are not based on the specific use of the servers. Depending on the role of a server, the necessary measures are covered in other modules (such as APP.3.2 Web

server, APP.3.3 File server, SYS.1.5 Virtualisation system).
The module presumes the integration of the server with Active Directory, the security of which is described in module APP.2.2 Active Directory Domain Services.
Module OPS.2.2 Using cloud services is implemented to cloud services integrated with server operating systems (such as an interface with the Microsoft Azure cloud platform).

2 Threats

2.1 Thoughtless use of cloud services

Windows Server may use cloud services (e.g. Microsoft Azure Online Backup or storing BitLocker recovery keys) without specific software. Cloud services may provide certain advantages (such as availability), but pose a threat to confidentiality when used thoughtlessly and increase dependence on service providers. Persons with malicious intent main gain access to the data via a cloud service.

2.2 Intrusion via remote access

An attacker may gain remote access to a server where insecure protocols are used (such as unprotected RDP or WinRM) or due to weaknesses in the authentication method (weak passwords), and such remote access can be used to attack the server and systems connected to the server.

2.3 Uncontrolled distribution of telemetry data

Windows Server issues so-called diagnostic data to Microsoft in its default configuration. The manufacturer may also gain access through a telemetry service that is integrated with the operating system, thus having access to crash dumps stored whenever a failure has occurred and to server log data. Potentially sensitive information might end up in the hands of unauthorised persons.

2.4 Impairing computer forensics when using VSM (Virtual Secure Mode)

When using VSM, usable computer forensics methods are limited. In the case of an IT incident, it will not be possible to analyse processes and memory dumps which are protected by the means of Secure Kernel or Isolated User Mode (IUM).

3 Measures

3.1 Life cycle

Planning

SYS.1.2.3.M1 Windows Server deployment plan

Implementation

SYS.1.2.3.M2 Secure installation of Windows Server

Operation

SYS.1.2.3.M3 Restricting the distribution of telemetry and diagnostic data

SYS.1.2.3.M4 Preventing the exploitation of vulnerabilities

SYS.1.2.3.M5 Secure privilege management in Windows Server

SYS.1.2.3.M6 Secure remote access to RDP

Additional advanced measures

SYS.1.2.3.M7 Secure use of Windows PowerShell

SYS.1.2.3.M8 Using VSM (Virtual Secure Mode)

3.2 Key measures

SYS.1.2.3.M1 Windows Server deployment plan

a. The Windows Server version that is implemented is chosen based on justified and documented selection criteria.
b. The manner of integrating the new server with Active Directory has been determined.
c. In the case of each cloud service integrated with an operating system, it has been decided whether it is blocked prior to implementation or not, as well as the configuration of the cloud service for utilisation.
d. Unless required otherwise, adding Microsoft accounts is blocked in Windows Server.

SYS.1.2.3.M2 Secure installation of Windows Server

a. If the current functions are sufficient, a minimum version of Server Core is installed. Written justifications are prepared for adding other functions.

SYS.1.2.3.M3 Restricting the distribution of telemetry and diagnostic data

a. In order to limit diagnostic and utilisation data that is sent to Microsoft, the telemetry level of the Windows Server (parameter AllowTelemetry) is set to the selective value 0 (Security).

b. If the telemetry settings of a server cannot be limited, other measures are used for preventing the data from being sent to the manufacturer, such as restricting data traffic on network level.

3.3 Standard measures

SYS.1.2.3.M4 Preventing the exploitation of vulnerabilities

a. Measures to prevent the exploitation of known vulnerabilities are implemented in Windows Server and server services (see Chapter 4 Additional information).

SYS.1.2.3.M5 Secure privilege management in Windows Server

a. All users of the Windows Server are included in the Protected Users (PU) security group.
b. The service accounts of Windows Server are included in the Managed Service Accounts (MSA) group. Service and computer accounts are not in the Protected User group.

SYS.1.2.3.M6 Secure remote access to RDP

a. When planning remote access, local firewall settings are taken into account.
b. The RDP (Remote Desktop Protocol) user group (including necessary service accounts) only consists of authorised users.
c. Implementing the mechanisms of operating systems (such as Remote Credential Guard or RestrictedAdmin) has been considered when establishing a connection to protect remote access credentials.
d. The RDP target system is only accessible in a network infrastructure with higher protection requirements through an RDP gateway.
e. When using the RDP, the following convenience functions must comply with the security requirements of the target system:

- using a clipboard;
- making removable media and network drives available;
- utilisation of internal file storage space and other resources of the server (such as a smart card reader).

f. When establishing remote access, cryptographic protocols and algorithms that are used comply with the cryptography concept of the organisation.
g. When there are no plans to use remote access during a certain period, the remote access option is completely deactivated.

3.4 Advanced measures

SYS.1.2.3.M7 Secure use of Windows PowerShell (C-I-A)

a. The execution of orders given in PowerShell is logged centrally and the logs thus created are analysed.
b. In order to prevent the activation of unsigned scripts, the activation of the PowerShell scripts is restricted by the Set-ExecutionPolicy AllSigned command.
c. The use of older Windows PowerShell versions is blocked.
d. PowerShell commands are restricted with the setting Constrained Language Mode.
e. Just Enough Administration (JEA) tool is used for managing the users of Windows Server Powershell.

SYS.1.2.3.M8 Using VSM (Virtual Secure Mode) (C-A)

a. VSM has been activated in the server to protect the data processed in the server.
b. The fact that the utilisation of VSM hinders computer forensics has been taken into account.

SYS.1.3 Linux and Unix server

1 Description

1.1 Purpose

To present the measures applied to ensure the availability, integrity, and confidentiality of the servers using Linux (e.g. Debian, Red Hat Enterprise Linux/CentOS, SUSE Linux Enterprise/openSUSE) or Unix (e.g. OpenBDS, Solaris, AIX) operating systems and of the data processed in those servers. The measures describe the configuration and operation of the operating system irrespective of the specific intended use of the server. The module specifies and complements the peculiarities of the Linux and Unix systems in the aspects covered in the module SYS.1.1 Server in general.

1.2 Responsibility

The IT department is responsible for the compliance with the measures applicable to a Linux or Unix server.

1.3 Limitations

The module does not cover the special requirements for the different roles related to the server (e.g. the web server is described in the module APP.3.2 Web server and groupware in the module APP.5.3 Email server and client in general).
The security measures of virtualised servers are covered in the module SYS.1.5 Virtualisation system.

2 Threats

2.1 System and user information intelligence

Unix includes several programs which enable inquiring the data stored by the IT system about users. Such data includes the activity profiles of the users, information about users that have logged on, as well as technical information about the installation and configuration of the operating system.

2.2 Exploitation of the script environment

Scripts written in the scripting language and activated from the command line are used in the Unix operating systems to facilitate the work of the administrator and prevent human errors. An attacker may manipulate and exploit the scripts to achieve their goals.

2.3 Dynamic downloading of libraries

With the help of the 'LD_PRELOAD' variable, the dynamic library indicated (dynamically linked shared object library) is downloaded before other standard libraries which are needed in the application. This enables overwriting specific functions of the standard libraries with personal functions. An attacker may, for example, manipulate the operating system so that a malicious program is activated upon launching certain applications.

2.4 Software from sources which have not been validated

In the Unix-like operating systems, the users download packages instead of installing the ready-made applications and the program is compiled locally. Software packages are often downloaded from sources which have not been validated. If the manufacturer's reliable package repository is not used, there is a risk of unintentionally downloading and installing an incorrect or incompatible software package or software which contains malicious functions.

3 Measures

3.1 Life cycle

Implementation

SYS.1.3.M2	Proper definition of indicators
SYS.1.3.M3	Avoiding automatic connection of removable devices to the file system
SYS.1.3.M4	Protection of applications

Operation

SYS.1.3.M5	Secure installation of software packages
SYS.1.3.M6	Administration of users and groups
SYS.1.3.M8	SSH-encrypted data exchange
SYS.1.3.M10	Prevention of the unauthorised expansion of rights

Additional advanced measures

SYS.1.3.M14	Prevention of system and user information intelligence
SYS.1.3.M16	Additional prevention of the unauthorised expansion of rights
SYS.1.3.M17	Additional kernel security

3.2 Key measures

SYS.1.3.M2 Proper definition of indicators

a. All user names, user identifiers (UID), and group identifiers (GID) are unique. The arrangement of the indicators applies to all servers of the organisation.
b. Each user is included in at least one group.
c. All group identifiers found in the '/etc/passwd' file are defined in the file entitled '/etc/group'.
d. All groups only contain necessary users.
e. The same system of allocating user and group names and user and group identifiers applies to all servers of the organisation.

SYS.1.3.M3 Avoiding automatic connection of removable devices to the file system

a. Removable device and removable media (e.g. flash drives or CD/DVD disks) cannot be automatically mounted on the file system by connecting.

SYS.1.3.M4 Protection of applications

a. In order to make the exploitation of the vulnerabilities of an application more difficult, applications use the ASLR and DEP/NX mechanisms activated in the kernel.
b. The security functions of the kernel and standard libraries are activated.

SYS.1.3.M5 Secure installation of software packages

a. Before installation, the integrity and authenticity of the software packages to be installed are checked.
b. In the event of software compilation from a source code, the unpacking, configuration, and compilation of the software are completed under unprivileged account rights.
c. In the case of compilation of software from a source code, all selections made are documented so that the compilation could be repeated with the same parameters.
d. Software is not installed in the root file system of the server.
e. All installation steps are documented so that the configuration can be restored quickly, if necessary.

3.3 Standard measures

SYS.1.3.M6 Administration of users and groups

a. Appropriate administration tools are used for the administration of users and groups.
b. The '/etc/password', '/etc/shadow', '/etc/group', and '/etc/sudoers' configuration files are not edited by using a standard text editor.

SYS.1.3.M8 SSH-encrypted data exchange

a. Data exchange is encrypted with the SSH (Secure Shell) protocol.
b. All insecure data exchange protocols are deactivated.
c. User certificates are preferred to user passwords for authentication.

SYS.1.3.M10 Prevention of the unauthorised expansion of rights

a. Services and applications are protected by a kernel security module (e.g. AppArmor or SELinux).
b. In addition, chroot environments and LXC or Docker containers are taken into consideration.
c. All standard profiles and rules of the rights are activated.

3.4 Advanced measures

SYS.1.3.M14 Prevention of system and user information intelligence (C)

a. Issuing any information about the operating system and access to the log and configuration files are strictly needs-based.
b. Sensitive data is not provided as a command parameter (on the command row or from the script file). Such parameters are entered by the administrator interactively.

SYS.1.3.M16 Additional prevention of the unauthorised expansion of rights (C-I)

a. System calls are restricted based on needs.
b. Standard profiles and rules (incl. AppArmor or SELinux) are checked based on the security policy.
c. Existing rules are adjusted or new rules or profiles are created, if necessary.

SYS.1.3.M17 Additional kernel security (C-I)

a. The kernel of the operating system is hardened (e.g. grsecurity, PaX) and complemented by the adjustment of role-based access, file system security, and other security mechanisms.

SYS.1.5 Virtualisation system

1 Description

1.1 Purpose

To present the measures applied to ensure the security of the virtualisation environment and virtual hosts (hereinafter together also referred to as the virtualisation system).
The virtualisation interface consists of virtualisation hosts in which the virtualisation environment is executed directly by using hardware or through the operating system of the host. The virtualisation environment hypervisor enables to create guest systems, virtual servers which contain the IT systems accessible for the users.

1.2 Responsibility

The IT department is responsible for the compliance with the security measures specified in the virtualisation system module.
Additional responsible persons: Architect.

1.3 Limitations

In addition to this standard security module, operating system-based sever or client modules and the modules SYS.1.1 Server in general and SYS.2.1 Client computer in general are also applied to virtual servers. Server-based virtualisation is covered in this module. The module does not cover the partial use of virtualisation (e.g. virtualisation of application with terminal servers, containers, Java virtual machine).
Storage area networks (NAS or SAN) or also mostly interfaced with the virtualisation environment. The security of storage solutions is described in the module SYS.1.8 Storage solutions.
Virtualisation also calls for additional requirements for the structure of the network which are described in the module NET.1.1 Network architecture and solution.

2 Threats

2.1 Errors in planning virtualisation

A lack of technical and organisational planning of a virtualisation system may cause errors in the configuration of the virtualisation environment. When virtual servers have been deployed in the operating environment, it is difficult to fix the mistakes made during installation. If the fields of responsibility are not clearly defined (e.g. responsibility for applications, operating systems, and network components), important approvals or operations may be foregone. Excessive access rights may also be granted to a user.

2.2 Configuration errors of virtualisation

Virtual resources such as processors, RAM, network connections, and memory are configured through the hypervisor in the virtualisation environment and are no longer fully dependent on hardware. Errors in determining the resources of a virtual server may later cause errors in the functioning of the guest systems configured in the server. In the event of an error in the segmentation of virtual servers, e.g. if a virtual IT system of a high protection requirement is placed in the same segment with clients or into an external demilitarised zone, the data may leak.

2.3 Lack of resources for the virtual IT system

For the virtualisation system to function, the virtual server requires memory capacity and plenty of storage space in the local virtualisation server itself or in the connected storage area network. If sufficient spare storage and disk space required is not planned right in the beginning, it will soon result in a risk to the availability of the virtual IT systems and the integrity of the data processed there. It is especially important to ensure sufficient capacity and storage space for making snapshots. Lack of resources may also become apparent in the case of a network connection of insufficient capacity. Insufficient virtualisation server resources disturb the cooperation between virtual machines.

2.4 Data leaks or resource shortages related to snapshots

Snapshots are used for backing up virtual servers, among other things. If a snapshot is later activated (recovered), if necessary, all changes made in the IT system after making the snapshot are lost. If a snapshot is too old, the server becomes vulnerable, as the security vulnerabilities which have already been patched reappear. The sessions and transactions ongoing at the moment of taking a snapshot may cause a conflict with other servers after the recovery of a virtual server based on the snapshot.

2.5 Failure in the administration server of the virtualisation system

The functions of the virtualisation system are controlled and managed through the administration server. An administration server failure means that the virtualisation system will no longer be controllable for changing the configuration or adequately responding to the failures of virtual servers.

2.6 Abuse of unapproved applications

The access rights granted to the users of the administration tools of a virtualised environment often exceed those required for the administration of the virtual machines managed by them. This creates the risk of the access rights being exploited to conduct denial-of-service attacks or to take over the virtualisation server.

2.7 Security breach in the virtualisation server

The virtualisation server hypervisor monitors and controls the virtual servers created in the virtualisation system and allocates processor and storage resources to the servers. A successful attack against this component may lead to the unlawful modification or loss of all guest servers and the virtual IT systems thereof.

3 Measures

3.1 Life cycle

Operation

SYS.1.5.M2	Secure implementation of a virtualisation system
SYS.1.5.M3	Secure configuration of a virtualisation environment
SYS.1.5.M6	Logging of a virtualisation system
SYS.1.5.M7	Time synchronisation in a virtualisation system
SYS.1.5.M11	Administration network of a virtualisation system
SYS.1.5.M15	Separation of guest systems with different protection requirements
SYS.1.5.M17	Inspection and monitoring of the configuration of a virtualisation server
SYS.1.5.M19	Regular inspections of a virtualisation system

Implementation

SYS.1.5.M4	Secure network configuration of a virtualisation infrastructure
SYS.1.5.M5	Security of the administrative interfaces of a virtualisation environment
SYS.1.5.M12	Administrative rights to a virtualisation interface and the roles
SYS.1.5.M16	Isolation of virtual machines

Planning

SYS.1.5.M8	Designing a virtualisation system
SYS.1.5.M9	Designing the network architecture of a virtualisation system
SYS.1.5.M10	Administration rules for virtualisation systems
SYS.1.5.M14	Common configuration requirements for the virtualisation infrastructure

Acquisition

SYS.1.5.M13	Hardware suitable for a virtualisation system

Additional advanced measures

SYS.1.5.M20	High-availability architecture
SYS.1.5.M21	Secure configuration of guest systems

SYS.1.5.M22 Hardening the host
SYS.1.5.M23 Restriction of the rights of a virtual server
SYS.1.5.M24 Deactivation of virtual server snapshots
SYS.1.5.M25 Minimum use of the virtual server console access
SYS.1.5.M26 Using the public key infrastructure
SYS.1.5.M27 Certified virtualisation software
SYS.1.5.M28 Encryption of virtualised ID systems

3.2 Key measures

SYS.1.5.M2 Secure implementation of a virtualisation system

a. All virtualisation system administrators are aware of the impact of virtualisation on the IT systems and applications operated.
b. The access rights of the administrators of the virtualisation systems are restricted based on needs.
c. Before the implementation of a virtualisation system, it is checked if:
• the host server of the virtualisation infrastructure has sufficient data communication connections for the virtualisation system;
• the requirements for the separation and encapsulation of the applications operated in the validation environment are complied with;
• the virtualisation system is compliant with the requirements for availability and data communication capacity.
d. The performance of the virtualisation system is regularly monitored.

SYS.1.5.M3 Secure configuration of a virtualisation environment

a. The access to the virtualisation server (the host system) from the guest systems is restricted. Guest systems have no access to the components and interfaces of the host. If necessary, the administrator of the host system may exceptionally grant temporary guest access rights.
b. The configuration and security of the virtual guest systems and the IT systems thereof are compliant with the security policy of the organisation.

SYS.1.5.M4 Secure network configuration of a virtualisation infrastructure

a. The data communication of the virtual servers passes through the security mechanisms (e.g. firewalls) and monitoring systems or the network connections of the virtualisation system.

b. No unauthorised network connections can be made from a guest system with multiple network interfaces.
c. The data communication interfaces of the virtual and hardware-based IT systems are compliant with the security policy of the organisation.

SYS.1.5.M5 Security of the administrative interfaces of a virtualisation environment

a. Administrative access to the administration system and host systems is restricted.
b. Administrative interfaces have no access from unreliable networks.
c. Secure protocols are used for the monitoring of the virtualisation server and administration system and for administrative access. In the case of insecure protocols, a separate administration network is used for administration.

SYS.1.5.M6 Logging of a virtualisation system

a. The status, load, and network connections of the virtualisation system are constantly logged.
b. If the virtual server is about to run out of resources, the amount of resources at its disposal is increased or the virtual server is relocated and the virtualisation server hardware is complemented.
c. The log data of virtual servers is analysed regularly.

SYS.1.5.M7 Time synchronisation in a virtualisation system

a. The system times of all IT systems used are always synchronised.

3.3 Standard measures

SYS.1.5.M8 Designing a virtualisation system [architect]

a. The architecture of a virtualisation system is planned in detail.
b. The policies and rules applicable to IT systems, applications, and networks (incl. storage area networks) are taken into consideration in the planning of a virtualisation system.
c. If the host system has more than one guest system, the security of those systems is aligned.
d. All components of the virtualisation system are covered with administrative operations. The tasks of the administrative groups are defined and do not overlap.

SYS.1.5.M9 Designing the network architecture of a virtualisation system [architect]

a. The network architecture of a virtualisation system is planned in detail.
b. The network segments to be created (e.g. administration network, storage network) and the processes for separating and securing network segments are defined.
c. The administration network is separated from the operating network (see the module SYS.1.5.M11 Administration network of a virtualisation system). If necessary, separate network segments are created for certain virtualisation functions (e.g. online migration).
d. The network architecture ensures the required availability of the virtualised IT systems.

SYS.1.5.M10 Administration rules for virtualisation systems [IT manager]

a. Procedures have been established and documented for the deployment, accounting, operating, and decommissioning of virtual servers and virtualised IT systems.
b. The guidelines for the administration of the virtualisation system are updated regularly.
c. Testing and development environments are not operated in the same virtualisation server with the IT systems of the operating environment.

SYS.1.5.M11 Administration network of a virtualisation system

a. The virtualisation system is managed via a separate administration network.
b. The security mechanisms of the administrative protocols used for authentication, ensuring integrity, and encryption are activated.
c. All insecure administrative protocols are deactivated (see also NET.1.2 Network management).

SYS.1.5.M12 Administrative rights to a virtualisation interface and the roles

a. The rights and roles required for the administration of the virtualisation server have been established (see SYS.1.5.M8 Designing a virtualisation system).
b. The central process of the administration of identity and rights also includes components of the virtualisation system.
c. Managers of virtual servers and administrators of the virtualisation server and hypervisor are separate persons with different access rights.
d. The administration environment allows grouping virtual machines to establish an appropriate hierarchical structure for the distribution of the roles of the managers.

SYS.1.5.M13 Hardware suitable for a virtualisation system

a. The hardware used is suitable for the virtualisation solutions implemented.
b. Product support is ensured for the hardware for the entire planned period of use.

SYS.1.5.M14 Common configuration requirements for the virtualisation infrastructure

a. A unified standard configuration is defined for the virtualisation infrastructure (incl. guest systems).
b. Standard configuration is used in the configuration of guest systems.
c. The configuration rules are checked regularly and adjusted, if necessary.

SYS.1.5.M15 Separation of guest systems with different protection requirements

a. If virtual guest systems of different protection requirements are operated in one host server, the virtual guest systems are separated from one another and encapsulated.
b. The network connections of the guest systems with different protection requirements are sufficiently securely separated in the virtualisation system.

SYS.1.5.M16 Isolation of virtual machines

a. The transfer of data between virtual machines by copying the data from the source machine and pasting it in the target machine is deactivated.

SYS.1.5.M17 Inspection and monitoring of the configuration of a virtualisation server

a. In the course of the regular monitoring of the virtualisation server, the following is checked, among other things:
- sufficiency of the resources of the virtualisation server;
- the lack of conflicts in the shared resources of the virtualisation server;
- the lack of unauthorised changes in the configuration files;
- the connections of the virtual networks with the right virtual IT systems.

b. Any changes in the configuration of a virtualisation server are tested before implementation.

SYS.1.5.M19 Regular inspections of a virtualisation system

a. Regular checks are conducted to verify whether the condition of the virtualisation system is compliant with what was planned.
b. The compliance of the configuration of virtual components with the prescribed standard

configuration is checked regularly.
c. The results of the review are documented and any deviations found are eliminated as soon as possible.

3.4 Advanced measures

SYS.1.5.M20 High-availability architecture [architect] (A)

a. The virtualisation infrastructure is designed to have high availability.
b. In the event of using more than one host server, the host servers are gathered into clusters.

SYS.1.5.M21 Secure configuration of guest systems (I-A)

a. When allocating resources to the guest systems, the total amount of the resources reserved does not exceed the amount of physical resources available.
b. The functionality which enables the overlapping of resources is deactivated.

SYS.1.5.M22 Hardening the host (C-I)

a. The host server and the hypervisor are hardened.
b. MAC (mandatory access control) is used for encapsulating virtual IT systems and separating the systems from one another and from the host server.

SYS.1.5.M23 Restriction of the rights of a virtual server (C-I)

a. All interfaces and communication channels which enable reading and inquiring data from a virtual server to the host system are eliminated or deactivated.
b. Only the server itself can access the resources of the host server.
c. Virtual servers cannot share the main memory sections of the host server.

SYS.1.5.M24 Deactivation of virtual server snapshots (C-I-A)

a. The snapshot function is deactivated in the administrative console of virtual servers.

SYS.1.5.M25 Minimum use of the virtual server console access (A)

a. Access to the emulated consoles of the virtualisation system is restricted to the minimum level.
b. If possible, virtual servers are managed through the network.

SYS.1.5.M26 Using the public key infrastructure [architect] (C-I-A)

a. The public key infrastructure (PKI) of key certificates is used in the encryption of the communications between the components of the virtualisation system.

SYS.1.5.M27 Certified virtualisation software (C-I-A)

a. The virtualisation software is certified based on ISO/IEC 15408; the recommended level is at least EAL 4.

SYS.1.5.M28 Encryption of virtualised ID systems (C)

a. All virtualised IT systems are encrypted.

SYS.1.6 Containerisation

1 Description

1.1 Purpose

Presenting the measures for the protection of the data located in containers or processed with containers.
Unlike virtualisation, containerisation enables to encapsulate applications by using an internal resource of the operation system and without using any further virtual machines with an independent operation system.

1.2 Responsibility

The IT department is responsible for the implementation of the security measures of containerisation.
Additional responsible persons: No additional responsible persons.

1.3 Limitations

The module covers the software and IT services for creating and managing containers, as well as the applications and services included in a container. The module presents general measures of containerisation without defining specific products. Products are selected based on the module

APP.6 Software in general.
The module complements the measures described in SYS.1.1 Server in general and in SYS.1.3 Linux and Unix server with the specifics of containerisation. The module also expands the security measures presented in the modules CON.8 Software development and OPS.1.1 Main IT operations.
The applications included in containers usually communicate with one another through a virtual network executed on a host. Thus, the measures specified in the modules NET.1.1 Network architecture and solution and NET.3 Network components should also be taken into consideration.
If the host itself is virtual, the measures from the module SYS.1.5 Virtualisation system are applied.
If the host system or infrastructure components related to the containers are not fully owned by the organisation, but are partly in the use of third parties or purchased from third parties in the form of a cloud service, measures from the modules OPS.2.1 Outsourcing, OPS.2.2 Using cloud services and OPS.3.1 Information security of the service provider are also applied.
The module does not discuss the operations which are related to creating and managing images. Administration of containers with the help of Kubernetes is discussed in the module APP.4.4 Kubernetes

2 Threats

2.1 Security vulnerabilities of container images or malware

In the creation of containers, ready-made container images obtained from the Internet are also often used in addition to own containers. Software is also increasingly delivered in the form of premade container images. The IT department can adjust the images by adding, changing, or removing software or configuration.

2.2 Insecure maintenance accesses

The maintenance access required for the management of the container services located on the host system is usually executed via network connection. The authentication and encryption mechanisms for secure data exchange are often available, but have not been activated under the default settings or in the course of later configuration.

2.3 Internal conflict of resources

One container may overburden the resources of the host and thereby put to risk the availability of other containers. In the worst case, the entire host system will become unavailable.

2.4 Data exchange with unauthorised IT systems

Containers can communicate with one another, with their host, and with other host systems. If data exchange is unrestricted, an attacker may take advantage of this opportunity by attacking other containers or hosts.

2.5 Container partition failure

If an attacker is able to activate their own code in a container, they may interrupt the isolation of the container from other containers or the host. An attack launched with the aim of gaining access to other containers, the host system, or the infrastructure may be possible due to the vulnerability of processors, the core of the operation system, or local services (e.g. DNS or SSH), for example.

2.6 Data loss arising from the improper administration of containers

If a container is switched off in the course of administration operations without allowing the software running in the container to finish its unfinished task (e.g. finish an unfinished writing process), data loss may occur as a result of such unexpected interruption. The data loss may not only be limited to the data which is being processed at the time of switching off the container.

2.7 Container access information leak

Upon creating a container or a container image, user accounts with respective privileged rights are required for the installation and configuration of the software in the container. Higher-level rights are also required for the configuration of the databases in the container. If the creation of container images is automated, the user accounts, passwords, and other information required for access which are used in the scripts may end up in the hands of unauthorised persons. The risk is higher if the version administration is not sufficiently secure or if same container images are used in different systems.

2.8 Uncontrolled spread of container images

Containers differ from the IT systems installed and configured by using the regular method, in the case of which the IT department has complete control over the applications, components, and services installed. In the case of the containers which are administered by third parties, the IT department has no such control. The IT department usually only provides the platform which

developers can place their containers or containerised applications on. Thus, there is a risk of containers containing unknown security vulnerabilities.

3 Measures

3.1 Life cycle

Planning

SYS.1.6.M1	Designing containerisation
SYS.1.6.M2	Planning the administration of containerisation
SYS.1.6.M3	Secure operation of containerised IT systems
SYS.1.6.M9	Assessing the suitability of applications
SYS.1.6.M10	Guidelines for the use of containers

Implementation

SYS.1.6.M4	Secure implementation of container images
SYS.1.6.M5	Partitioning the management network of containers
SYS.1.6.M11	Partitioning applications in containers
SYS.1.6.M12	Secure distribution of container images
SYS.1.6.M13	Approving container images for use

Operation

SYS.1.6.M6	Use of secure container images
SYS.1.6.M7	Storage of container log data
SYS.1.6.M8	Secure management of container access data
SYS.1.6.M14	Updating container images
SYS.1.6.M15	Defining the resource limitations of a container
SYS.1.6.M16	Secure remote maintenance of containers
SYS.1.6.M17	Defining the minimum rights required for operating a container
SYS.1.6.M18	Restricting the rights of containerised applications
SYS.1.6.M19	Regulating access to data recorders
SYS.1.6.M20	Security of the configuration information of a container

Additional advanced measures

SYS.1.6.M22	Using container images as evidence
SYS.1.6.M23	Ensuring the constancy of containers

SYS.1.6.M24 Host-based attack detection
SYS.1.6.M25 High availability of containerised applications
SYS.1.6.M21 Expanded security rules of containerisation
SYS.1.6.M26 Further isolation and encapsulation of containers

3.2 Key measures

SYS.1.6.M1 Designing containerisation

a. Before deployment of containerisation, the goals are defined which the containerisation aims to achieve (e.g. scalability, availability, agile CI/CD development, security by partitioning applications).
b. Designing involves mapping the security risks of containerisation and the impacts thereof on the business processes of the organisation.
c. The operating costs arising from the deployment and maintenance of the containers are also considered in the course of the planning process.
d. The purposes as well as risk and cost assessments of containerisation are documented.

SYS.1.6.M2 Planning the administration of containerisation

a. The administration processes of containers involve the entire life cycle of containerisation from the deployment of the containers to their decommissioning.
b. Container administration involves ensuring the security of containerisation and installing security updates regularly.

SYS.1.6.M3 Secure operation of containerised IT systems

a. Before the deployment of containers, the effects of containerisation on the IT systems and applications used, primarily the operation and administration of the applications, are analysed.
b. The alignment of the isolation and encapsulation of the IT systems of the containers, the virtual networks, and the applications operated with the protection purposes of the applications is also analysed.
c. It is checked whether the security mechanisms of the operation system of the host ensure sufficient security of the containers.
d. In order to increase the level of security of the virtual network, the host is subjected to measures from the module groups NET.1 Networks and communication and NET.3 Network components.

e. The level of availability of the IT systems located in the containers is compliant with pre-established requirements for availability and data communication capacity.
f. In the course of operating the containers, the functionality of the system is monitored and periodic health checks are performed.

SYS.1.6.M4 Secure implementation of container images

a. The process of creating and implementing container images is planned and documented in sufficient detail.

SYS.1.6.M5 Partitioning the management network of containers

a. In order to ensure a sufficient level of security, the administration network of the host system, the administration network of the containers, and the networks used to gain access to the containerised applications are properly partitioned from one another.
b. Only a specialised administration network is used for the remote maintenance of the host system.
c. Any data communication connections which are not required for operating the containers are blocked.

SYS.1.6.M6 Use of secure container images

a. All container images used originate from secure sources. The creator of a container image is unambiguously identifiable.
b. Before the deployment of a container image, it is verified that the creator of the images has checked the content of the container for security vulnerabilities, fixed any security vulnerabilities known, and sent the respective documentation to their clients.
c. The container images used are versioned. The latest version of a container image available is used.
d. If a container image with a newer version number is available, deployment of the container image is planned based on the process for the management of changes established.

SYS.1.6.M7 Storage of container log data

a. The container log data is stored and retained outside of the container (at least at the level of the host system).

SYS.1.6.M8 Secure management of container access data

a. In the saving and administration of credentials and access data, only authorised persons and containers have access to the credentials.
b. Access data is stored in special secured locations. Access data is not retained in the container image.
c. If there is administration software of the container services, the mechanisms for the management of credentials integrated into the administration software are used.
d. At least the following credentials are stored securely.

- all account passwords;
- the API encryption keys of the services of the applications;
- symmetrical encryption keys;
- private keys of the public key infrastructure (PKI).

3.3 Standard measures

SYS.1.6.M9 Assessing the suitability of applications

a. The suitability of the applications and services used in the container is tested before use.
b. The assessment of the suitability of the applications involves considering the potential consequences of any unexpected disruptions of the container.
c. The checks of the suitability of applications for operating in a container (see SYS.1.6.M3 Secure operation of containerised IT systems) are documented.

SYS.1.6.M10 Guidelines for the use of containers

a. A policy has been drawn up and implemented which defines the rules of operating containers.
b. The policy for using containers also includes the requirements for the secure creation and implementation of container images.

SYS.1.6.M11 Partitioning applications in containers

a. One container can only carry one IT service at a time.

SYS.1.6.M12 Secure distribution of container images

a. Criteria have been drawn up and approved which enable to assess the reliability of container images and approve a container image for use.

b. Container images are equipped with metadata about the creator, purpose, and history of the image.
c. Container images are protected from unauthorised changes (e.g. with the help of digital signatures).

SYS.1.6.M13 Approving container images for use

a. Similarly to software products, container images are tested before installation in the operational environment.
b. Container images are approved for deployment based on the procedure established (see OPS.1.1.6 Software testing and onboarding).

SYS.1.6.M14 Updating container images

a. Updates to container images are installed based on the approved change management process (OPS.1.1.3 Patch and change management).
b. It has been determined when and how updates are installed and deployed for container images or the software and services operated from the containers.
c. In the case of the containers which have been in use for a long period of time, decisions are taken on whether it would be reasonable to update the content of the container used or recreate the container.

SYS.1.6.M15 Defining the resource limitations of a container

a. The host system resources required for functioning (e.g. CPU, RAM capacity, network capacity) have been defined and reserved for each container.
b. There is also an action plan for exceeding the threshold values established for the resources.

SYS.1.6.M16 Secure remote maintenance of containers

a. All management operations from containers in the direction of the hosts and vice versa are considered remote maintenance (see OPS.1.2.5: Remote maintenance).
b. Remote maintenance of a host is not performed from a container located on the same host.
c. A container which operates applications has restricted remote maintenance access to other IT systems.
d. Remote maintenance of the container is only performed through the container runtime.

SYS.1.6.M17 Defining the minimum rights required for operating a container

a. Container runtime and the containers created therein are operated by a non-privileged account created for this purpose which has no privileged account rights in container applications or in the operation system of the host system.
b. Further measures have been taken for the encapsulation of the container runtime, for example with the help of CPU virtualisation extension.
c. If it is, in an exceptional case, necessary to activate host system tasks by using the rights of the account operating the container, the user rights of the account in the host system are limited to the minimum rights required. All such exceptions are documented.

SYS.1.6.M18 Restricting the rights of containerised applications

a. Internal system accounts do not have rights in the host system. In exceptional cases, account management occurs in the host system and the account is only granted access to the required information and IT systems.

SYS.1.6.M19 Regulating access to data recorders

a. Containers only have access to the data recorders and shared directories required for work. Access is only granted in the extent required for fulfilling the duties.
b. If the local storage space of a container is configured for the storage of information in the container runtime, only internal accounts may access the storage space.
c. If network-based storage systems (SAN or NAS) are used, the access rights required are issued to the container from the storage system.

SYS.1.6.M20 Security of the configuration information of a container

a. The container configuration information is versioned.
b. All configuration changes are clearly documented.

3.4 Advanced measures

SYS.1.6.M22 Using container images as evidence (C-I)

a. In order to enable the use of container snapshots as evidence in the case of a potential investigation, the rules established are followed in creating container images (see DER.2.2 Enabling computer forensics.

SYS.1.6.M23 Ensuring the constancy of containers (I)

a. Changing the file system of a container is blocked during operating the container.
b. The file system is mounted with the container without the write permission.

SYS.1.6.M24 Host-based attack detection (C-I-A)

a. Containers and the applications and services used in the containers are subjected to constant monitoring.
b. Any departures from the normal functioning of the containers are registered. Indicated individuals are notified of the departures. Events are handled based on the centralised process of managing security events.
c. At least the following activities and processes are monitored:
- network connections and information exchange;
- the processes initiated in the container;
- inquiries addressed to the file system;
- syscalls to the kernel of the operation system.

SYS.1.6.M25 High availability of containerised applications (A)

a. In the case of the requirement for the high availability of a containerised application, a decision is made as regards the level on which the availability is increased (e.g. ensuring redundancy at the host level (doubling of hosts)).

SYS.1.6.M21 Expanded security rules of containerisation (C-I-A)

a. Detailed rules have been prepared for the management of the access rights of containers.
b. Detailed access rights are granted based on predefined rules by using mandatory access control (MAC) or an equivalent mechanism.
c. The access rules regulate at least the following access rights:
- incoming and outgoing network connections;
- access rights to the file system;

• syscalls to the kernel of the operation system.

d. In the case of launching the container via the container runtime, the kernel of the operating system of the host can at least block the container operations which are prohibited by access rules (e.g. changing the settings of a local package filter or cancelling the rights) or report such operations.

SYS.1.6.M26 Further isolation and encapsulation of containers (C-I)

a. Implementation of the following measures will be considered in the case of establishing more stringent requirements for the isolation and encapsulation of containers:

- allocation of containers to fixed hosts;
- using hypervisors to activate individual containers and/or hosts;
- associating a specific container with a specific host.

SYS.1.8 Storage solutions

1 Description

1.1 Purpose

To present measures for the design, implementation, secure operation, and decommissioning of a storage solution.

The typical target objects of this module are storage systems - network attached storage (NAS) and storage area networks (SANs). In the storage systems, data is stored in the storage devices.

1.2 Responsibility

The IT department is responsible for compliance with the measures applicable to storage solutions.

Additional responsible persons: Technology department, information security manager.

1.3 Limitations

The main requirements applicable to using storage solutions as a file server are specified in the modules SYS.1.1 Server in general and APP.3.3 File server. Long-term data retention in a storage system are described in the modules OPS.1.2.2 Archiving and CON.3 Data backup concept.

Safe placement of the storage solutions in the intranet of the organisation is described in the module

NET.1.1 Network architecture and solution.
Management of the users of the storage solutions is covered in the module ORP.4 Administration of identity and rights.
If a storage solution is acquired as a service from an external service provider, further measures from the module OPS.2.1 Outsourcing are applied.

2 Threats

2.1 Insecure default configuration of storage components

In order to facilitate the simple deployment of storage components without compatibility issues, the storage components are supplied with a standard configuration in which as many functions as possible have been activated. Thus, unauthorised protocols are also available in the devices, such as insecure versions of the HTTP, Telnet, and SNMP (Simple Network Management Protocol) protocols. It is easier for an attacker to gain access to a storage solution with insecure factory settings. Consequently, the functioning of the IT systems may be interrupted, as the databases are no longer available. An attacker can also gain access to the confidential data of the organisation.

2.2 Data manipulation through a storage system

An insufficiently configured storage system may facilitate the access of an attacker to the data of the organisation. If the server connected to the SAN can be connected to from outside of the intranet (from the Internet), a successful attacker may use the server as a springboard to access the sensitive data stored in the storage network without being stopped by the firewall or intrusion detection system of the organisation.

2.3 Phishing during the duplication of storage-based data

Real-time duplication of the data in the storage system is often used to prevent data loss. Automatic duplication of unencrypted data comes with the risk of unauthorised recording of the traffic between the storages by using FC analysers or network sniffers, for example.

2.4 WWN identifier falsification attack

The WWN (World Wide Name) identifiers used for identifying the FC storage network devices with a fibre optic cable connection (similarly to the MAC addresses of the Ethernet network adapters) can be manipulated.

2.5 Violation of the logical separation of networks

If the networks of different clients are separated with the help of virtual storage area networks (WSAN) instead of physical separation, the security of the information of the organisation may be at risk. If an attacker manages to penetrate the network of another client, they may gain access to the virtual storage area network of this client, as well as to the data sent.

2.6 Storage solution component failure

Complex network-based storage solutions consist of many components (such as FC commutators, storage controllers, virtualisation devices). If redundancy at the component level is not applied, a technical failure of a storage solution component may cause a failure in the functioning of the storage solution or cause data loss.

2.7 Unlawful physical access to the commutators of a storage network

If the access controls applied at the organisation for the protection of the storage system are insufficient, an attacker may gain access to the commutators. An attacker may connect further FC commutators to the network for phishing to save the data of the storage system.

3 Measures

3.1 Life cycle

Implementation

SYS.1.8.M1	Appropriate place of installation of a storage system
SYS.1.8.M2	Secure baseline configuration of a storage solution
SYS.1.8.M15	Secure separation of the consumers of a storage solution

Operation

SYS.1.8.M4	Security of management interfaces
SYS.1.8.M10	Guidelines for operating a storage solution
SYS.1.8.M11	Secure operation of a storage solution

SYS.1.8.M13 Monitoring and management of a storage solution

SYS.1.8.M16 Secure deletion of data

SYS.1.8.M17 Documentation of the configuration of a storage system

SYS.1.8.M18 Reviewing storage systems and reporting

Planning

SYS.1.8.M6 Security guidelines for a storage solution

SYS.1.8.M7 Designing a storage solution

SYS.1.8.M14 Segmentation of a storage area network (SAN)

Acquisition

SYS.1.8.M8 Selecting a suitable storage solution

SYS.1.8.M9 Selecting a maintenance partner for the storage solution

Disposal

SYS.1.8.M19 Decommissioning of a storage system

Emergency response

SYS.1.8.M20 Emergency response and operations of a storage solution

Additional advanced measures

SYS.1.8.M21 Using a storage pool for separating consumers

SYS.1.8.M22 High-availability storage area network

SYS.1.8.M23 Encryption in storage solutions

SYS.1.8.M24 Ensuring the integrity of the SAN fabric

SYS.1.8.M25 Multiple overwriting of data upon deletion

SYS.1.8.M26 Hard zoning of a storage network

3.2 Key measures

SYS.1.8.M1 Appropriate place of installation of a storage system [technology department]

a. The storage system components are installed in locked rooms. Only persons with access rights can access these rooms.

b. Uninterrupted power supply is ensured in the premises.

c. The temperature and humidity of the environment are compliant with the recommendations of the manufacturer of the storage system.

SYS.1.8.M2 Secure baseline configuration of a storage solution

a. Before the installation of a storage solution in the operating environment, the updates of the software components are installed and the firmware of the hardware components is updated.
b. All default passwords are changed and all useless user accounts deactivated in the baseline configuration.
c. Any useless interfaces of the storage system are deactivated.
d. The default configuration, baseline configuration, and current configuration files are backed up and protected.

SYS.1.8.M4 Security of management interfaces

a. The administration access rights of storage systems are limited.
b. Administrative interfaces have no access from unreliable networks.
c. Secure protocols are used for the remote administration of storage systems. In the case of insecure protocols, a separate administration network is created for administration.

3.3 Standard measures

SYS.1.8.M6 Security guidelines for a storage solution [information security manager]

a. Security guidelines for storage solutions have been drafted based on the general security policy of the organisation and include requirements for the secure planning, implementation, administration, operation, and disposal of a storage solution.
b. The security guidelines have been introduced to the employees. All administrators of the storage system observe the security guidelines.
c. Amendment of the security guidelines for storage solutions is coordinated with the information security manager and documented.
d. Compliance with security guidelines is checked regularly. The results of the inspection are documented.

SYS.1.8.M7 Designing a storage solution

a. The requirements, performance, and capacity of the storage solution are analysed in the planning stage of a storage solution.
b. Based on the technical specifications for the requirements, a storage solution implementation plan is drafted, which specifies the following:

- the suitable hardware specifications;

- the criteria for selecting the manufacturer and supplier;
- the architecture of the solution to be procured (centralised or scattered);
- the network connection plan;
- the required infrastructure;
- integration with existing processes.

SYS.1.8.M8 Selecting a suitable storage solution

a. The technical specifications and compliance with the requirements of the organisation have been analysed and checked in sufficient detail.
b. The criteria for selecting a storage solution are documented unambiguously.
c. The individuals making the procurement decision have been familiarised with the opportunities and limitations of different storage systems.
d. The decision on selecting a storage system and the explanation of compliance with the selection criteria are documented.

SYS.1.8.M9 Selecting a maintenance partner for the storage solution

a. The maintenance partner of the storage solution is selected based on the requirements of the storage solution.
b. The service level agreement (SLA) concluded with the maintenance partner includes the aspects related to the warranty conditions, maintenance, and repair of the storage solution.
c. The service level agreement is unambiguous and the performance of the agreement can be measured.

SYS.1.8.M10 Guidelines for operating a storage solution

a. Guidelines for operating a storage solution have been drafted, describing the processes of operating the solution, the requirements, and configuration.
b. The guidelines for operating a storage solution are regularly updated.

SYS.1.8.M11 Secure operation of a storage solution

a. In the course of operating a storage solution, the availability of the applications, load indicators of systems, and event messages are monitored constantly.
b. Certain maintenance times have been set for making changes in the storage solution.

c. Updates of the firmware, operating system, or network components of the storage system are only installed during maintenance sessions agreed on in advance.

SYS.1.8.M13 Monitoring and management of a storage solution

a. The monitoring and management of the storage solution and components thereof are organised centrally.
b. Monitoring data enables to conclude whether the operation of the storage solution is compliant with the guidelines.
c. If the storage solution is managed by an external service provider, the monitoring objects, the organisation of monitoring, filtration of important system messages, and the procedure of notifying the parties are defined and documented in the service level agreement.

SYS.1.8.M14 Segmentation of a storage area network (SAN)

a. Distribution of the resources of the storage area network (SAN) between the servers is documented.
b. The distribution of resources of SAN and the actual resource consumption can be clearly monitored by using administration tools.
c. The network of a storage solution is segmented based on the security and administration requirements.
d. The valid zoning configuration is documented. The documentation remains available in the case of an emergency.

SYS.1.8.M15 Secure separation of the consumers of a storage solution

a. The requirements of the organisation for the multi-tenancy capacity of the storage solution have been specified and documented.
b. The storage solution is compliant with the documented separation requirements.
c. In the case of block storage, the consumers are separated from one another (e.g. by the masking of the logical unit number (LUN)).
d. File services are provided to different consumers by separated virtual file servers. There is a separate file service for each client unit.
e. In the case of using IP or iSCSI, the consumers are separated from one another by network segmentation.

f. In the case of using FC (Fibre Channel), the separation is ensured by virtual storage area networks (VSANs) and soft zoning based on WWNs.

SYS.1.8.M16 Secure deletion of data

a. The procedure for secure deletion is provided in the guidelines for operating a storage solution (see SYS.1.8.M10 Guidelines for operating a storage solution). The guidelines establish, among other things, which data is deleted and which procedure is used.
b. In multi-tenancy storage area networks, the LUNs fixed to the consumers are also eventually deleted.

SYS.1.8.M17 Documentation of the configuration of a storage system

a. The configuration of storage systems (incl. specific system configurations) is documented.
b. The configuration documentation is protected from unauthorised access.
c. The configuration documentation is always up to date (especially concerning the granting of access rights).
d. The configuration documentation of a storage system is also available in an emergency situation.

SYS.1.8.M18 Reviewing storage systems and reporting [information security manager]

a. A procedure for the regular review of storage systems has been established and is observed.
b. The frequency and level of detail of the reviewing of storage systems has been established.
c. The content of a review report and the procedure of handling discrepancies have been determined.

SYS.1.8.M19 Decommissioning of a storage system

a. Before the disposal of a storage system, all data in the storage system is migrated to other storage systems.
b. There is a documented and tested transfer procedure for the migration.
c. All user and configuration data is securely deleted from the storage system.
d. Any references to the disposed storage system are deleted from the documentation of the storage system.

SYS.1.8.M20 Emergency response and operations of a storage solution

a. A storage system emergency plan has been drafted, which provides detailed instructions for action in the case of an emergency situation.
b. The emergency plan includes technical instructions for the troubleshooting of the storage solution and for eliminating failures.
c. Regular trainings and repeat tests are organised to practise the emergency plan.
d. After a training or testing, all data created in the course of the training or test is deleted securely.

3.4 Advanced measures

SYS.1.8.M21 Using a storage pool for separating consumers (C-I)

a. Storage space is allocated for different consumers from storage pools.
b. One storage media can only be included in the composition of one storage pool.
c. Each LUN (Logical Unit Number) generated from such storage pool is only at the disposal of one user.

SYS.1.8.M22 High-availability storage area network (A)

a. A high-availability storage area network (SAN) is taken into use, the duplication mechanisms and configuration of which are compliant with the requirements for the availability of storage solutions of the organisation.
b. There is a separate system for testing the solution.

SYS.1.8.M23 Encryption in storage solutions (C-I)

a. All data stored in a storage solution is encrypted.
b. If necessary, the data is also encrypted during transfer, including duplication and backing up.

SYS.1.8.M24 Ensuring the integrity of the SAN fabric (I)

a. Protocols with reinforced security parameters are used to ensure the integrity of the set of network devices forming the storage area network fabric (SAN fabric).
b. The following protocols are used to initiate a data exchange session:
- Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP);
- Fiber Channel Authentication Protocol (FCAP);
- Fiber Channel Password Authentication Protocol (FCPAP).

SYS.1.8.M25 Multiple overwriting of data upon deletion (C)

a. In storage area network environments, data is deleted by multiple overwriting of the storage parts fixed to the logical unit number (LUN) with a special data pattern.

SYS.1.8.M26 Hard zoning of a storage network

a. Hard zoning based on the separation of the commutator ports is used in the segmentation of a storage area network.

SYS.1.9 Terminal server

1 Description

1.1 Purpose

To present measures for the protection of data handled through a terminal server, including for the design, implementation, secure operation, and decommissioning of a terminal server. A client of a terminal server can be a so-called fat client or a thin client. Fat clients are equipped with a complete operating system. In contrast, thin clients are designed only for establishing a connection with a terminal server and for running applications on the server. The terminal server is used for running applications, in which case it has been decided (e.g. for technical or organisational reasons) that they will not be run straight in the client. A graphic user display and the input from the mouse and keyboard is forwarded to the client through specific terminal server protocols (such as RDP, PCoIP) or VNC. The operating system of a terminal server allows several users to work at the same time, running the same or different applications simultaneously.

1.2 Responsibility

The IT department is responsible for compliance with the measures applicable to terminal servers.
Additional responsible persons: Architect.

1.3 Limitations

The measures presented in the module apply to both terminal servers as well as the clients of terminal servers. General requirements for a terminal server and a client are explained in modules SYS.1.1 Server in general, SYS.2.1 Client computer in general, and the ones discussing various operating systems. Measures from the module APP.6 Software in general apply to the software of a terminal server. Module NET.1.1 Network architecture and solution describes the security of the network solution of a terminal server. This module does not focus on remote management or the use of remote management tools. These topics are covered in module OPS.1.2.5: Remote maintenance.

2 Threats

2.1 Low-quality data transmission

When using terminal servers, the response of a terminal server to a client request must be clear and reach the clients without a noticeable delay. Excessive delay may cause disruptions in the functioning of a service, such as difficulties monitoring the movement of the mouse or text cursor and switching images on the screen. Mistakes in input become possible and the terminal server can only be used to a limited extent. Delays could be caused by an excessive latency period of the communication channel or network components. Additional delays may be caused by an insufficiently dimensioned security component, such as a VPN gateway. Moreover, a terminal server may reply to a request with a delay when it is overloaded. Overload might be caused by a number of simultaneous client requests or the insufficient performance of the terminal server.

2.2 Inaccessibility of a terminal server

Applications are started in a terminal server so only a screen output is forwarded to the client. When a terminal server is not available due to a failure (for example, when a session between a client and the terminal server is disrupted), control over the application that was used is lost. The user is not able to control applications launched in the terminal server even if they are currently active in the terminal server. If an application has no alternative user interface, the IT system might shut down completely. The failure of a terminal server may impact a large number of clients at the same time.

2.3 Attack against a terminal server

Client applications launched in a terminal server normally rely on services and data in other servers. Therefore, an attacker who has gained access to a terminal server will easily move to other servers by using the terminal server as a starting point for attacks planned against other IT systems. An

attack is particularly dangerous if the terminal server allows access to applications located in various network segments.

2.4 Inadequate session management

Applications that run on a terminal server share the same resource with various applications and clients within the same operating system, such as a kernel, libraries, and hardware components (e.g. CPU or RAM). Due to configuration errors or vulnerabilities in software, it is possible for instances of different applications to communicate with each other. For example, an attacker may be able to use malicious code where vulnerabilities are present, searching for passwords entered by users in the random access memory (RAM). If a session user of a terminal server has excessive access rights, they may be able to access the file system through an application and to view, change, or store files through a file dialogue from areas that the user does not need to access. Another possible attack is a so-called hijack attack against an RDP session. When users remain logged in after the end of a terminal server session, an attacker may be able to hijack the RDP session if they have the respective rights and to continue the session using the rights of the previous user.

2.5 Exploiting the vulnerabilities of a data communication protocol

As a rule, the data communication protocols of terminal servers use strong authentication and encrypted data communication with the clients of a terminal server. When a terminal server protocol contains vulnerabilities (or when important security functions have been blocked due to a configuration error), it is possible to eavesdrop on the conversations of clients and the terminal server. An attacker may gain unauthorised access to the authentication data of clients, the contents of the clipboard of a user, or forwarded files.

2.6 Shared user accounts

For the constant monitoring of an application that runs on a terminal server (such as by an external maintenance partner), the organisation may be tempted to create a shared user account. This might contradict the internal regulations or security policy of the organisation or licensing terms and conditions of the terminal server software. A shared account may prevent linking specific activities in the terminal server with a concrete person. This might also lead to legal consequences, for example, if the terminal server is used for processing personal data.

2.7 Errors in restricting access rights

Due to the nature of a terminal server, the terminal server might simultaneously act as a server and as a client used for running applications working on other servers. This could lead to errors when assigning access privileges, expressed as granting excessive access rights or the unnecessary restriction of rights. As a rule, a user must be granted the minimum possible access privileges. This type of behaviour might create a situation where a user is able to use an application inefficiently and only to a limited extent. For example, the users might begin to store data in a cloud service due to being blocked from writing on the local hard drive.

2.8 Using unsuitable applications for a terminal server

All applications might not be suitable for use in a terminal server. For example, applications using complex graphics or 3D applications might cause issues. An emulated graphics module of a terminal server might not support the functions of a physical graphics processing unit (GPU). A terminal server or its client software or data communication protocol might not be able to receive data from a special peripheral connected to a client. Without sufficient testing, the shortcomings would only be revealed when in use. This would significantly reduce additional value planned for the commissioning of a terminal server.

3 Measures

3.1 Life cycle

Planning

SYS.1.9.M1	Establishing security requirements for a terminal server
SYS.1.9.M2	Planning the deployment of a terminal server
SYS.1.9.M5	Planning clients and client software
SYS.1.9.M6	Designing a network solution for a terminal server

Implementation

SYS.1.9.M3	Managing roles and authorisations in a terminal server
SYS.1.9.M4	Secure configuration of a terminal server
SYS.1.9.M9	Raising awareness among the users of a terminal server

Operation

SYS.1.9.M7	Security of accessing a terminal server
SYS.1.9.M8	Secure assignment of a terminal server to a network segment

SYS.1.9.M10 Central management of identity and authorisations in a terminal server

SYS.1.9.M11 Secure user profiles of a terminal server

SYS.1.9.M12 Automatic termination of inactive sessions

SYS.1.9.M13 Logging terminal server activity

SYS.1.9.M14 Monitoring a terminal server

SYS.1.9.M15 Hardening of a terminal server

SYS.1.9.M16 Optimisation of data compression

Additional advanced measures

SYS.1.9.M17 Additional encryption of data communication

SYS.1.9.M18 Using only thin clients

SYS.1.9.M19 Expanded monitoring of a terminal server

SYS.1.9.M20 Allocation of terminal servers based on the purpose of use or user group

SYS.1.9.M21 Guaranteeing the high availability of terminal servers

SYS.1.9.M22 Blocking data transmission

3.2 Key measures

SYS.1.9.M1 Establishing security requirements for a terminal server

a. The organisation has documented and established security requirements for a terminal server. As a minimum, the security requirements cover the following topics:

- software to be installed in terminal servers;
- applications that are allowed to be used through a terminal server;
- security requirements for clients using client software, including physical security requirements;
- network security, including the permitted data communication protocols and requirements for the client network;
- encryption mechanisms and authentication methods between clients and terminal servers;
- forwarding files and other data through a terminal server protocol in addition to screen output;
- in addition to normal input and output devices, peripherals that can also be connected to the client.

SYS.1.9.M2 Planning the deployment of a terminal server

a. Functional requirements for applications running on a terminal server have been documented.

b. Terminal server applications comply with the security requirements for a terminal server.

c. The proper functioning of terminal server applications has been tested ahead of time.
d. A prognosis about the total number of users and the estimated number of simultaneous users of a terminal server has been prepared for the entire presumed lifespan of the terminal server.
e. Due to the estimated number of users and the requirements for the applications running on a terminal server, minimum performance parameters have been established for the terminal server (such as for the processor and main memory).
f. When selecting hardware, software, and applications to be used, the agreed service level and the presumed number of simultaneous users of the terminal server are taken into account.
g. The licensing schemes of terminal server applications allow to use the applications on the terminal servers.

SYS.1.9.M3 Managing roles and authorisations in a terminal server

a. Shared accounts may be used in terminal servers only when they do not violate internal regulations or licensing conditions of the software. A written decision containing justifications is required for the implementation of a shared account.
b. Access privileges to applications used in a terminal server correspond to the roles and authorisations of terminal server users, determined ahead of time.
c. Data communication between terminal server sessions is only permitted to the extent necessary for keeping an application functional.
d. The necessity of all of the following rights has been considered carefully;

- running an application as a privileged user;
- access to the specific functions of an operating system;
- access to the file system of a terminal server;
- access to the interfaces and file systems of a client;
- access to support services enabling the use of terminal server applications;
- sending files between clients and a terminal server (for example, to be printed from the client);
- connecting peripherals to the client.

SYS.1.9.M4 Secure configuration of a terminal server

a. Standard configurations based on security and functionality requirements of applications have been established for terminal servers and documented.
b. When commissioning a terminal server, recommendations for the secure configuration of the terminal server made by hardware and software producers have been taken into account.

c. As a minimum, the standard configuration of a terminal server takes into account the following:

- roles and authorisations;
- encryption and its scope;
- data communication protocols of a terminal server and their authentication functions;
- data communication between terminal server sessions;
- data communication between applications in and outside the terminal server;
- data communication between the terminal server and other servers.

d. Configurations are regularly checked to make sure that they are appropriate and applied correctly.

SYS.1.9.M5 Planning clients and client software

a. The organisation has decided which client software is allowed to access a terminal server and whether the same software may be used in other terminal servers.
b. The organisation has determined which conditions clients must meet to connect to a terminal server. As a minimum, the following is taken into account:

- the use of thin clients or fat clients;
- requirements for the software of a client;
- operating systems used in clients.

SYS.1.9.M6 Designing a network solution for a terminal server [architect]

a. Requirements have been established for data networks used by clients for connecting with a terminal server. As a minimum, the following has been decided:

- the presumed number of simultaneous terminal server sessions;
- network capacity;
- the largest permissible packet loss;
- the longest permissible jitter;
- the longest permissible latency.

SYS.1.9.M7 Security of accessing a terminal server

a. It is possible to access terminal servers only through networks that have the respective authorisation.
b. Data communication channels are protected by an encrypted data communication protocol. When the protocols of a terminal server do not enable encryption at a sufficient level of security, the data

communication channels are protected with additional network security measures.
c. Where clients and a terminal server communicate through networks that are not sufficiently reliable (such as through public communication networks), mutual authentication is required from the clients and the terminal server when establishing a connection.

SYS.1.9.M8 Secure assignment of a terminal server to a network segment

a. A terminal server is located in a network segment that is separated from others or a network segment containing the clients of the terminal server.
b. The terminal server is available only in the assigned network segments.
c. A terminal server does not allow bypassing the internal rules of network separation.

SYS.1.9.M9 Raising awareness among the users of a terminal server

a. All users of terminal servers have been trained in the secure use of terminal servers.
b. As a minimum, the users of terminal servers have been trained in the following:
- the main functions of a terminal server;
- the impact of the quality of communication on the usability of a terminal server;
- possible and allowed data storage locations;
- data communication between a client and a terminal server (such as by using a clipboard);
- the impact of resource consumption on other simultaneous users;
- roles and authorisations for accessing terminal servers;
- the authentication of the users in the applications of a terminal server;
- the longest allowed duration of a session and the procedure for logging out (including logging users out automatically).

3.3 Standard measures

SYS.1.9.M10 Central management of identity and authorisations in a terminal server

a. Determining and granting the access rights of a terminal server takes place through a central management system.

SYS.1.9.M11 Secure user profiles of a terminal server

a. The user of a terminal server cannot change settings specific to users (user profiles) to the extent that may put the security of a terminal server at risk or limit the use of a terminal server.
b. The parameters of a user profile are suitable for the use of a specific terminal server. When several terminal servers are in use, user profiles are stored in a central location.

SYS.1.9.M12 Automatic termination of inactive sessions

a. Inactive (i.e. passive) sessions of a terminal server are terminated automatically at a preconfigured time. The period after which an inactive session is terminated is determined based on the user group.
b. Affected persons are notified of the automatic termination of a session.
c. When terminating a session, the user is automatically logged out of the operating system of the terminal server. Situations where an active session in the operating system is necessary for the continued use of applications are an exception.

SYS.1.9.M13 Logging terminal server activity

a. It has been determined which terminal server events are forwarded to a central log infrastructure (see OPS.1.1.5 Logging).
b. As a minimum, the following events in the terminal servers are logged:
- connecting a peripheral of a client to the terminal server protocol;
- the actions of a privileged user in the terminal server;
- changes in configuration that impact the services of the terminal server.

SYS.1.9.M14 Monitoring a terminal server

a. A terminal server is involved in central monitoring activities.
b. As a minimum, the following parameters are monitored:
- the resource utilisation of the terminal server;
- load on the network interfaces of the terminal server;
- the bandwidth of the network and the network utilisation of the terminal server;
- the latency of network connections, taking into account established requirements (see SYS.1.9.M6
- Designing a network solution for a terminal server).

c. To evaluate the results of the monitoring activities, the threshold values of availability and

performance parameters of a terminal server have been established ahead of time. The threshold parameters are checked regularly to make sure that they are appropriate.

SYS.1.9.M15 Hardening of a terminal server

a. Non-essential applications of a terminal server and useless components of an operating system have been removed. Whenever non-essential components cannot be removed, their use is blocked.
b. The use of peripherals is restricted during a terminal server session and only the required peripherals are permitted.

SYS.1.9.M16 Optimisation of data compression

a. When transmitting data between a terminal server and a client, an optimum level for data compression is utilised. At that, requirements for the precision of graphic elements, colour fidelity, and frame rate of the screen have been taken into account.

3.4 Advanced measures

SYS.1.9.M17 Additional encryption of data communication (C-I)

a. The entire data communication between a client and a terminal server takes place through securely encrypted data communication channels.

SYS.1.9.M18 Using only thin clients (I-A)

a. Only physical terminals deemed compatible with terminal servers by the manufacturer are used as clients of the terminal server (the so-called thin clients).

SYS.1.9.M19 Expanded monitoring of a terminal server (C-I-A)

a. The logging function of a terminal server (see SYS.1.9.M13 Logging terminal server activity) is constantly monitored to make sure that it is functional.
b. Logging the security events of a terminal server is interfaced with a security information and event management (SIEM) system.
c. A terminal server is regularly tested to identify vulnerabilities.

SYS.1.9.M20 Allocation of terminal servers based on the purpose of use or user group (C-I-A)

a. The terminal servers of an organisation have been separated into several terminal servers performing a narrow task based on the purpose of use or a group of users.
b. A terminal server that has been adjusted to perform a specific task is only accessible to authorised users.

SYS.1.9.M21 Guaranteeing the high availability of terminal servers (A)

a. Essential hardware components and network connections used by a terminal server have been duplicated.
b. The organisation has backup devices for replacing a terminal server and clients.

SYS.1.9.M22 Blocking data transmission (I-A)

a. Transmitting data used in a terminal server application to a client is blocked.
b. Data transmission through the clipboard is blocked.

SYS.2 Client computers

SYS.2.1 Client computer in general

1 Description

1.1 Purpose

To present the measures applied for the protection of the data processed in a client computer (irrespective of the type of the client computer or the operating system used) and to increase the awareness of the specific threats accompanying this device class.
The module 'Client computer in general' describes client computers with any operating systems which are related to a specific user. Client computers usually include one account with administrator rights and at least one account with user rights. A client computer is usually part of a 'client-server' type IT solution.

1.2 Responsibility

The IT department is responsible for the implementation of the measures of the module 'Client computer in general'.
Additional responsible persons: User, technology department.

1.3 Limitations

For the protection of the operating systems commonly used in client computers, the operating system-specific measures described in the module group SYS.2 Client computers must also be applied. The security measures applicable to mobile devices (e.g. smartphones and tablets) are specified in the module group SYS.3 Mobile devices.
The data exchange interfaces of a client computer (e.g. Bluetooth, local area network, or wireless local area network) are discussed in the respective modules (e.g. NET.2.2 Using wireless local area networks). The use of removable data media is described in module SYS.4.5 Removable data media. Protection of a client computer from malware is discussed in the module OPS.1.1.4 Protection against malware. Client computer logging measures are covered in the module OPS.1.1.5 Logging.

2 Threats

2.1 Malware

Malicious programs are usually activated covertly and without the user's consent. Depending on the execution, malicious programs provide extensive data exchange and management possibilities to the attacker in the client computer. Among other things, malicious programs may provide access to the user's passwords and IT systems, deactivate protective software, and spy on the user data.

2.2 Data loss due to the lack of central data storage

Many users store their files in the local directories of their computers, not in the central file server. Such data may be easily lost in the event of a hardware failure. The loss of the data which was only stored in the local computer may also result in losing the trust of the clients and partners, in addition to the work stoppage.

2.3 Hardware failures arising from improper use

Intentionally or due to negligence, users may damage their computers (pull the computer off the desk, poor liquids on the keyboard, etc.). Such damage often results in a hardware failure due to

which it is temporarily not possible to use the client computer. If the hard drive is also damaged, the data stored in the client computer before the hardware failure may no longer be recoverable. If the hardware failure occurs while the employee is travelling, normal work can only continue after they have returned.

2.4 Unlawful use of information technology

Restricting access to a computer merely by using a username a password is insufficient if the password is easy to guess or identify with the help of shoulder surfing.

2.5 Installation of useless applications and operating system components

In the course of installing an operating system, it is usually possible to choose which additional modules of the operating system to install. In practice, standard installation of the operating system is usually used, with many useless components also downloaded into the client computer in addition to the necessary ones. The more applications installed in a computer, the higher the likelihood of concealed vulnerabilities. If the circle of users of a software program is too small, the manufacturer does not receive enough feedback about security bugs and the bugs remain unfixed. If an application is no longer supported by the manufacturer, it may be presumed that the security vulnerabilities accumulated over time have remained unfixed and the application is not secure.

2.6 Eavesdropping via the microphone and camera of a computer

Many client computers are equipped with a computer microphone and camera. Those can be activated by all applications with respective access rights (e.g. digital personal assistants). In the case of networked systems, the computer microphone and camera can also be controlled remotely. An attacker may use the microphone and camera of a client computer for eavesdropping conversations or covertly recording meetings.

2.7 Insufficient management of devices and systems

Configuration errors of the operating system or applications of a client computer reduce the security of the client computer. Configuration errors may affect the functioning of the client computer. There is also the risk of an unauthorised person gaining access to the computer as a result of a configuration error.

3 Measures

3.1 Life cycle

Operation

SYS.2.1.M1	Secure authentication of users
SYS.2.1.M3	Automatic installation of updates
SYS.2.1.M6	Anti-malware software
SYS.2.1.M42	Use of cloud and network functions
SYS.2.1.M18	Use of cryptographic protocols in data communication
SYS.2.1.M20	Security of management procedures
SYS.2.1.M29	Monitoring of client computers
SYS.2.1.M34	Encapsulation of security-critical applications

Implementation

SYS.2.1.M8	Booting security
SYS.2.1.M13	Restricted access to the execution environment
SYS.2.1.M15	Secure installation and configuration of a client computer
SYS.2.1.M16	Deactivation of useless components and accounts
SYS.2.1.M21	Procedure for using a computer microphone and camera
SYS.2.1.M23	Preferring 'client-server' services
SYS.2.1.M24	Restriction of the use of external data media
SYS.2.1.M26	Secure operation of applications
SYS.2.1.M30	Standard installation of a client computer
SYS.2.1.M43	Local security settings of a client computer
SYS.2.1.M44	Central management of the security settings of client computers

Planning

SYS.2.1.M9	Guidelines for the secure use of the client computer
SYS.2.1.M10	Client computer deployment plan

Acquisition

SYS.2.1.M11	Procedure for acquiring a client computer

Disposal

SYS.2.1.M27	Procedure for the disposal of a client computer

Additional advanced measures

SYS.2.1.M28	Encryption of the content of a client computer
SYS.2.1.M31	Local packet filter
SYS.2.1.M32	Further anti-attack measures
SYS.2.1.M33	Preventing the operation of applications
SYS.2.1.M35	Active root certificate administration
SYS.2.1.M36	Implementation of the SecureBoot function and TPM module
SYS.2.1.M37	Use of multifactor authentication
SYS.2.1.M38	Integration with emergency response
SYS.2.1.M39	Uninterrupted and stable power supply
SYS.2.1.M40	Maintenance documentation
SYS.2.1.M41	Restriction of the storage space of the hard disk of a client computer
SYS.2.1.M45	Expanded logging of a client computer

3.2 Key measures

SYS.2.1.M1 Secure authentication of users [user]

a. Only users who have duly authenticated themselves may use a client computer.
b. The person who performed an operation can be identified for any activity in a client computer.
c. Only authorised users may change authentication data (such as passwords).
d. A user always locks the screen of the computer when leaving their computer unattended. The screen lock may be activated manually by the user or is activated automatically after a certain predetermined period of time. The duration of the period depends on the specifics of the work tasks of the user of the computer. The screen can only be unlocked by authenticating the user.
e. In the case of a longer absence, the user must log out of the client computer or switch off the computer.

SYS.2.1.M3 Automatic installation of updates

a. Automatic installation of updates is activated in the operating system and standard software of the client computer. This does not apply to those IT systems which require the manual installation of updates.
b. Automatic checks of availability of new updates are carried out once a day.
c. If updates are downloaded from the manufacturer's public update server, the authenticity of the update server and the integrity of the update packages are checked.

d. An internal update server (e.g. Windows Server Update Services, WSUS) is used for the management of updates.
e. Mobile devices may receive updates from the update server of the organisation, as well as from the manufacturer's public update server.
f. If necessary, the software situation before the update can be restored in a client computer.

SYS.2.1.M6 Anti-malware software

a. Client computers are equipped with activated anti-malware software.
b. In exceptional cases when an anti-malware application is not installed in a client computer, this decision is justified and documented.
c. The anti-malware application scans the files when they are opened. The files sent and received are scanned automatically immediately before sending or after receiving.
d. The user cannot deactivate the anti-malware application of the client computer or change the configuration thereof.
e. Any client computers which have been infected with a malicious program are removed from the network.

SYS.2.1.M8 Booting security

a. Booting a client computer is protected from manipulation.
b. The data media from which booting is permitted have been specified. Only client computer managers are authorised to boot client computers from internal optical drives and from external storage media.
c. Automatic activation from external data media is deactivated.
d. Only managers can change the boot settings in the firmware. Access to the configuration interface of the firmware is at least password-protected.
e. All useless functions are deactivated in the firmware.
f. The SecureBoot option is activated in the client computers with the UEFI firmware.

SYS.2.1.M9 Guidelines for the secure use of the client computer

a. Guidelines for the secure use of a client computer compliant with the protection requirement of client computers has been drafted based on the general security policy of the organisation.
b. Security (restriction of the functions and rights) and user convenience are balanced in the

guidelines of the secure use of a client computer.

c. The client computer security policy establishes at least the following:

- the rights and obligations of the users in the daily use of the computer;
- the managers' rights and restrictions;
- the procedure for installation and the baseline configuration;
- regulation and authentication of access;
- data backup;
- network connections and network services;
- logging.

d. The guidelines for the secure use of a client computer are observed by all employees who are involved with purchasing, managing, or using client computers.

e. Compliance with the guidelines is checked regularly. The results of the inspection are documented.

SYS.2.1.M42 Use of cloud and network functions

a. Only the required cloud and network functions are activated in the client computer. Unnecessary cloud-based functions are deactivated or blocked.

b. The cloud or network functions permitted in client computers are documented.

c. The standard configuration of a client computer is compliant with the information security and data protection requirements of the organisation.

3.3 Standard measures

SYS.2.1.M10 Client computer deployment plan

a. A client computer deployment plan has been drawn up for the profiling, secure implementation, and operation of client computers.

b. The deployment plan includes at least the following aspects:

- the purpose and tasks of a client computer;
- the requirements for hardware (processor, main memory, disk space, network interfaces, etc.);
- the connections and compatibility with existing systems and data;
- the operating system and file system;
- the protection requirement and security mechanisms;
- the requirements for availability;

• management and maintenance.

c. If necessary, more than one computer profile has been drawn up (e.g. general office computer, laptop computer, manager's computer).

d. The decisions made in the planning phase are documented.

SYS.2.1.M11 Procedure for acquiring a client computer

a. The computer profiles described in the client computer deployment plan are taken into consideration during procurements.

b. As a rule, as many client computers as possible are purchased from the same manufacturer and are equipped with a similar hardware platform.

c. The manufacturers and maintenance partners of the hardware and operating system of the client computer ensure the availability of spare parts and security updates for the entire estimated service life of the client computer.

d. The client computers that are going to be acquired are equipped with a configurable firmware interface (UEFI) and an integrated TPM (Trusted Platform Module) chip for secure central management.

SYS.2.1.M13 Restricted access to the execution environment

a. The execution environment of the operating system which is invisible for an ordinary user (storage areas, firmware areas) cannot be accessed by the ordinary user.

b. Program codes can only be activated in the execution environments with the respective management rights.

c. BIOS or UEFI firmware settings are password-protected from unauthorised changes.

SYS.2.1.M15 Secure installation and configuration of a client computer

a. Before installation, an exhaustive list of the operating system components, applications, and utilities to be installed on the client computer is drawn up.

b. Only authorised managers or external service providers appointed by contracts may perform the installation.

c. A secure baseline configuration has been developed and documented for configuring client computers. The baseline configuration includes at least the following aspects:

• the accounts with administrative rights;

• the system directories and files;
• the user accounts and directories;
• network access;
• local security functions (e.g. a packet filter);
• monitoring functions (incl. the functions of sending information on use to the manufacturer ('Phone Home').

d. The procedure for installation and configuration is documented so that a competent third party would be able to complete the installation and configuration independently based on the documentation.

e. The installation and configuration documentation is protected from unauthorised changes and remains available in emergency situations.

SYS.2.1.M16 Deactivation of useless components and accounts

a. There is an updated overview of the operating system components and applications installed and activated in the client computers.

b. Useless modules, programs, services, user accounts, and interfaces are deactivated or uninstalled.

c. Unnecessary runtime environments, interpreters, and compilers are uninstalled.

d. The decisions to deactivate useless components are documented.

SYS.2.1.M18 Use of cryptographic protocols in data communication

a. Encryption is used, if possible, for the protection of the communication sessions of the client computer.

b. The cryptography algorithms and key lengths used in the client computers are up to date (e.g. TLS v1.3) and compliant with the module CON.1 Cryptography concept.

c. New certificates are only activated after the verification of the authenticity and integrity of the certificate.

d. Operational programs (e.g. browsers and email clients) validate the certificates concerned.

SYS.2.1.M20 Security of management procedures

a. Management guidelines have been drawn up for the regular maintenance of the client computers, which include at least the following:
• creation and deactivation of users;

- installation and uninstallation of applications;
- installation of security updates and security patches;
- installation of new applications;
- regular integrity checks.

b. Security measures appropriate for the manner of management of the client computers (local, by remote access, or via central management tools) have been implemented.
c. Secure protocols are used for the remote administration data communication.

SYS.2.1.M21 Procedure for using a computer microphone and camera

a. A procedure has been established for the use of the microphone and camera of a client computer.
b. The microphone and camera of a client computer may not be used without the user's consent.
c. If it is not permitted to use the microphone and camera, the camera is physically switched off or covered and the microphone is deactivated.
d. During confidential meetings, the microphones and cameras of the computers in the room are switched off.

SYS.2.1.M23 Preferring 'client-server' services

a. If possible, services and applications based on the 'client-server' architecture are used for data exchange within the local area network.
b. If peer-to-peer communication between the client computers is required (e.g. in the case of the VoIP communication service), the permissible exceptions are specified.
c. Peer-to-peer communication between client computers is only possible in a local area network.

SYS.2.1.M24 Restriction of the use of external data media

a. Only approved data media may be connected to client computers. For example, reading and writing rights may only be granted to the mobile data media encrypted with specific encryption keys (see CON.9 Exchange of information).
b. If possible, client computers are used in which the local data exchange possibilities have been restricted by reducing the number of drives (e.g. CD/DVD writer, memory card reader) and external interfaces.
c. Booting from external data media is blocked in the BIOS or UEFI of the client computers.
d. Automatic activation or displaying of the content of the data media is blocked.

SYS.2.1.M26 Secure operation of applications

a. In order to prevent the exploitation of the vulnerabilities of applications, the ASLR (Address Space Layout Randomization), DEP (Data Execution Prevention), and NX (No-Execute) security mechanisms are activated in the operating system and used in the applications.
b. The security functions of the kernel and library of the operating system are activated.

SYS.2.1.M27 Procedure for the disposal of a client computer

a. Important data is backed up and from client computers before the decommissioning of the computers and the client computers to be disposed of are wiped.
b. There is an up-to-date documented overview of the data stored in the IT systems and of the locations of the data.
c. A checklist is always drawn up for the disposal of a client computer, which specifies:
- which data must be backed up or archived before the disposal of the computer and how;
- which rights, references, and entries related to the computer disposed must be eliminated;
- which residual data and backed up data must be deleted and how.

SYS.2.1.M29 Monitoring of client computers

a. The logs of a client computer are stored in the central log server. The client computers are included in the central monitoring system.
b. The status and performance of the client computers are constantly monitored.
c. Managers are notified of any failures of the client computers or of exceeding the established thresholds.

SYS.2.1.M30 Standard installation of a client computer

a. A standard installation has been developed for the client computers which facilitates and automates the process of installation and re-installation of client computers. In the course of installation, the appropriately pre-configured standard installation is cloned into the client computer.
b. The standard installation includes all configuration changes, updates, and security patches.
c. The standard installation is thoroughly tested before installation in the client computer (incl. by the users of the computer).
d. Standard scenarios have been developed for testing and the test results are documented.

SYS.2.1.M34 Encapsulation of security-critical applications (C-I-A)

a. The security-critical data of applications (e.g. authentication and certificate data) is encapsulated to prevent the access of other application or operating system components or isolated into a separate execution environment.
b. Those applications which process data originating from unreliable sources (e.g. web browsers) are activated in an execution environment which is separated from the operating system.

SYS.2.1.M43 Local security settings of a client computer

a. The security settings of a client computer are thoroughly tested and checked before implementation.
b. Local security settings are configured based on the protection requirement of the data stored in the client computer.
c. Local security settings are aligned with the general security policy and other security requirements applicable in the organisation. Any deviations from the security policy are justified and documented.
d. Useless applications and unnecessary operating system components are deactivated.

SYS.2.1.M44 Central management of the security settings of client computers

a. The security settings of the client computers are managed centrally and in compliance with the procedures established by the organisation.
b. Locally managed configuration parameters are justified and coordinated with the information security manager.

3.4 Advanced measures

SYS.2.1.M28 Encryption of the content of a client computer (C)

a. Confidential data is only stored in a client computer in encrypted form. Advisably, the entire hard disk should be encrypted.
b. The configuration of the encryption and the processes of encryption and decryption are documented.
c. Only persons with access rights can access encrypted data.
d. After backing up encrypted files, directories, and data media, the data is no longer readable as plaintext.

e. The encryption key is not stored in the client computer in the form of cleartext.
f. The users know what to do if an authentication tool (e.g. password, PIN, proof of identity) is exposed.

SYS.2.1.M31 Local packet filter (C-I-A)

a. In addition to the central security gateway, local packet filters are also activated in the client computers.
b. Local packet filters function based on whitelisting.
c. After the activation of a local packet filter or changing the rules, the status of the services and ports is checked.

SYS.2.1.M32 Further anti-attack measures (C-I-A)

a. If the existing operating systems or security products lack sufficient functionality, further security products are used to reinforce at least the following functionality:

- separation of the roles of the manager and user;
- administration of rights;
- authentication;
- logging and monitoring.

b. If the technical measures are insufficient, further organisational measures are applied (e.g. if there is no automatic screen lock, the user must activate the lock manually).

SYS.2.1.M33 Preventing the operation of applications (C-I-A)

a. Only permitted programs and scripts can be operated in a client computer. The list of allowed programs is as limited as possible.
b. The list of allowed programs is based on the verification of certificates, comparison of hashes and/or allowed directory paths.

SYS.2.1.M35 Active root certificate administration (C-I)

a. In the course of preparing a client computer, the root certificates required for the functioning of the client computer are documented.
b. The client computer is regularly scanned for any other added root certificates and decisions are made on whether the root certificates used remain compliant with the requirements of the

organisation.
c. All certificate repositories (e.g. the UEFI certificate repository, the certificate repositories of web browsers) are taken into consideration in the scanning for root certificates.

SYS.2.1.M36 Implementation of the SecureBoot function and TPM module (C-I)

a. In the system using UEFI, the boot loader, kernel, and all firmware components required are signed by a secure key.
b. Useless keys have been removed.
c. If the TPM (Trusted Platform Module) is not used, the module is deactivated.

SYS.2.1.M37 Use of multifactor authentication (C)

a. In the event of a higher protection requirement, multifactor authentication is used for logging in to a client computer.

SYS.2.1.M38 Integration with emergency response (A)

a. The emergency response of the client computer is integrated with the general emergency management of the organisation (see DER.4. Emergency management).
b. The data backup of the client computers is part of the general data backup concept of the organisation (see CON.3 Data backup concept).
c. The recovery priority of the client computer is determined based on the priority of the business process using the client computer.
d. An emergency plan of the client computer has been drawn up, specifying the following:
- the availability of spare parts or access to them within the framework of maintenance contracts;
- the reboot triggers and the priorities of rebooting;
- the locations of the passwords and encryption keys;
- the rebooting plan (the procedure for the gradual rebooting of the system);
- the system configuration documentation;
- the additional software and hardware required for the rebooting.

e. A backup computer with a functional hardware, software, and dataset has been put together and is stored securely to enable the rebooting.
f. The backup computer is updated and tested after any changes in the system.

SYS.2.1.M39 Uninterrupted and stable power supply [technical department] (A)

a. In the event of a higher availability requirement, the power supply for the client computer is obtained via an uninterrupted power supply (UPS), which ensures the power supply for the client computer to at least enable applications to be switched off properly.
b. The load on the uninterrupted power supply and the sufficiency of the duration of the supply support are checked regularly and after adding further power consumers.
c. The client computers and uninterrupted power supply are protected from overvoltage and voltage disturbances.

SYS.2.1.M40 Maintenance documentation (A)

a. The maintenance works on a client computer are documented clearly. The documentation specifies who performed the works and when, as well as the content of the maintenance work.
b. All changes in the configuration and security-related operations (e.g. replacement of the hard disk) are documented.
c. If the maintenance works can be logged automatically, the works are documented automatically.
d. The maintenance documentation is protected from unauthorised access.

SYS.2.1.M41 Restriction of the storage space of the hard disk of a client computer (A)

a. The mechanisms which warn of running out of storage space are activated.
b. If necessary, disk quotas are established for storage space.

SYS.2.1.M45 Expanded logging of a client computer (C-I-A)

a. Those user operations which are not directly related to information security are also logged in the client computer.

SYS.2.2 Windows clients

SYS.2.2.3 Windows 10 client

1 Description

1.1 Purpose

To present measures applied for the protection of data stored in client computers (clients) using Windows 10 and Windows 11 operating systems. These operating systems are characterised by a better integration with the server infrastructure and cloud services of Microsoft.

1.2 Responsibility

The IT department is responsible for the compliance with the security measures established for Windows 10 and Windows 11 client computers.
Additional responsible persons: User.

1.3 Limitations

The measures of this module, specific to Windows 10 and Windows 11, complement measures presented in module SYS.2.1 Client computer in general.
In addition, measures from applicable modules are also applied to Windows clients, such as APP.1.1 Office software or APP.1.2 Web browser. In the case of clients that are connected to the Windows domain, measures from module APP.2.2 Active Directory Domain Services are applied.

2 Threats

2.1 Windows-focused malware

Due to the popularity of Windows operating systems, a plethora of malware exists, aimed at the users of Windows 10 or Windows 11. The backward compatibility of the different generations of Windows operating systems increases the risk of unlawful access even further.

2.2 Integrated cloud functions

Windows 10 and Windows 11 include numerous functions which allow to archive and synchronise data with the help of the cloud services of Microsoft. It is possible that cloud services are used for processing and storing data or personal data important for the organisation in a server which is located in a foreign country.

2.3 Software compatibility issues

Even though Microsoft generally ensures the compatibility of software operating in the previous Windows versions with the newer versions of the operating system, compatibility issues may be

experienced in the case of Windows 10 and Windows 11. Therefore, it may become impossible to use old software in a client computer or it may be used only to a limited extent. New security functions, such as User Account Control or Kernel Patch Guard in the 64-bit version of the operating system, may cause compatibility issues. In the case of older devices, problems may arise with signed drivers, which may no longer be available for old hardware components.

2.4 Misuse of Windows telemetry functions

Windows 10 and Windows 11 send diagnostic data to Microsoft. Microsoft may also send queries to a client with the help of an integrated telemetry service. The default settings of Windows allow the level of telemetry which, for example, enables access to the register of a client computer as well as the activation of certain diagnostic tools. This comes with the risk of delicate diagnostic or telemetry data becoming accessible to unauthorised persons.

2.5 Impaired incident handling when using VSM (Virtual Secure Mode)

If the VSM (Virtual Secure Mode) virtualisation solution is used for protecting data and preventing access to it in the Windows Enterprise environment, the analysis of computer processes is hindered. Process data encapsulated with VSM and IUM (Isolated User Mode) cannot be used for memory dumps for the purposes of subsequent analysis in computer forensics, rendering the handling of an IT incident complicated.

3 Measures

3.1 Life cycle

Planning

SYS.2.2.3.M1 Implementation plan for Microsoft cloud services

Acquisition

SYS.2.2.3.M2 Selection of a suitable Windows 10 version

Implementation

SYS.2.2.3.M4 Telemetry data protection settings

SYS.2.2.3.M5 Anti-malware in a Windows client computer

SYS.2.2.3.M12 Management of file and directory rights

SYS.2.2.3.M9 Central authentication

SYS.2.2.3.M13 Deactivation of the SmartScreen function

SYS.2.2.3.M14 Deactivation of the Cortana digital assistant

SYS.2.2.3.M15 Deactivation of the synchronisation mechanisms of Windows

SYS.2.2.3.M16 Secure use of Microsoft Store

SYS.2.2.3.M17 Automatic login prohibition

SYS.2.2.3.M18 Secure implementation of Remote Assistance

SYS.2.2.3.M19 Secure application of the RDP remote management tool

SYS.2.2.3.M20 Use of UAC with privileged accounts

Operation

SYS.2.2.3.M6 Integration of network accounts

Additional advanced measures

SYS.2.2.3.M21 Use of EFS (Encrypting File System)

SYS.2.2.3.M22 Use of Windows PowerShell

SYS.2.2.3.M23 Additional security of login information

SYS.2.2.3.M24 Activation of the time stamping of the last access

SYS.2.2.3.M25 Secure application of CUET remote access functions of a component

SYS.2.2.3.M26 Using VSM (Virtual Secure Mode)

3.2 Key measures

SYS.2.2.3.M1 Implementation plan for Microsoft cloud services

a. In the course of planning a procurement of Windows client computers, a decision has been made on which Microsoft cloud services to use and to which extent.

SYS.2.2.3.M2 Selection of a suitable Windows 10 version

a. The IT strategy, the number of client computers, and their intended purpose and protection requirements are taken into consideration when selecting a Windows version for client computers.
b. Based on the procurement plan, a software licence model and a procedure for the deployment of new versions that are suitable for the organisation are selected (e.g. SAC (Semi-Annual Channel) or LTSC (Long-Term Servicing Channel).

SYS.2.2.3.M4 Telemetry data protection settings

a. Forwarding telemetry data to the manufacturer of an operating system is restricted in the settings. When using Windows 10 or the Windows 11 Enterprise version, the telemetry level is set to the optional value of 0 (Security).
b. If the telemetry settings of a client computer cannot be restricted, sending data to the manufacturer of an operating system is blocked by measures applied at the network level (e.g. firewall rules).

SYS.2.2.3.M5 Anti-malware in a Windows client computer

a. Unless equivalent or more stringent measures have been taken to protect the IT system from infection with malware, Microsoft anti-malware components (such as Microsoft Defender) are activated in Windows client computers.

SYS.2.2.3.M12 Management of file and directory rights

a. Access to local files and directories and to those in the local area network is granted based on need and depending on the principles for managing identity and rights (see ORP.4 Administration of identity and rights).
b. The manager of a Windows 10 client computer has sufficient rights for conducting maintenance works.
c. Writing rights have been granted to the user only in the area of a specified file system. The users do not have writing rights in the directories of the operating system and applications.

3.3 Standard measures

SYS.2.2.3.M6 Integration of network accounts [user]

a. The directory service is used to authenticate the user for the domain as well as applications, if possible.
b. Only managers have the right to use a local account to log into a client computer.
c. Web-based identity management systems (e.g. a Google or Microsoft account) are not used to log into a client computer.

SYS.2.2.3.M9 Central authentication

a. Kerberos is used for central authentication. If not, the NTLMv2 authentication protocol may be used as an alternative.

b. The use of any older protocols (LAN-Manager and NTLMv1) is prohibited in the daily working environment of the organisation by the Windows group policy.
c. The encryption mechanisms used are appropriate for the protection requirement and are documented.
d. All deviations from the central authentication are justified and coordinated with the information security manager.

SYS.2.2.3.M13 Deactivation of the SmartScreen function

a. The SmartScreen function of Microsoft Defender, which scans files and web content downloaded from the internet for potential malware but may send personal data to Microsoft under certain circumstances, is deactivated.

SYS.2.2.3.M14 Deactivation of the Cortana digital assistant [user]

a. The Cortana digital assistant is deactivated.

SYS.2.2.3.M15 Deactivation of the synchronisation mechanisms of Windows

a. Synchronisation of user data with Microsoft cloud services is deactivated.
b. The shared use of WLAN passwords is deactivated.

SYS.2.2.3.M16 Secure use of Microsoft Store

a. The compliance of using Microsoft Store with the data protection and security requirements of the organisation have been assessed.
b. Where Microsoft Store is not required for the installation of apps in client computers, it is deactivated.

SYS.2.2.3.M17 Automatic login prohibition

a. Saving passwords, certificates, and other information for automatic login into websites and IT systems is prohibited.

SYS.2.2.3.M18 Secure implementation of Remote Assistance

a. The configuration of the local firewalls allows the use of Remote Assistance.
b. Remote assistance can only be provided after a clearly expressed request. If the request is saved in a file, the file is password-protected.
c. A user that is logged in must explicitly consent to the creation of a remote assistance session.
d. An appropriate validity period is established for a remote assistance request.
e. If the Remote Assistance service is not required, it is deactivated in the client computers.

SYS.2.2.3.M19 Secure application of the RDP remote management tool [user]

a. The configuration of the local firewall allows to use RDP (Remote Desktop Protocol).
b. Only a designated user group has RDP remote access privileges.
c. In the case of a higher protection requirement, the target system may only be accessed through an RDP gateway.
d. While planning the implementation of RDP, the organisation decides whether to permit the following convenience functions aligned with the protection requirements of the target system:

- using a clipboard;
- integration of printers;
- integration of removable data media and network drives;
- use of file repositories.

e. If the use of RDP is not allowed, it is fully deactivated in client computers.
f. The cryptography protocols and algorithms in use are compliant with the requirements of the organisation (see CON.1 Cryptography concept).

SYS.2.2.3.M20 Use of UAC with privileged accounts

a. The security level and availability of the privileged accounts are balanced in the UAC (User Account Control) configuration.
b. The UAC configuration is been documented.
c. All accounts with administrative rights are listed in the UAC documentation. Regular checks are conducted to make sure that the rights are justified.

3.4 Advanced measures

SYS.2.2.3.M21 Use of EFS (Encrypting File System) (C-I)

a. As the security of EFS (Encrypting File System) depends on the password of the user account, a strong password is used to protect the user account.
b. The Data Recovery Agent is a specialised account, so an administrative account is not used as the Data Recovery Agent.
c. The private key of the Data Recovery Agent is kept securely on an external data medium away from the system. Backup copies are made of all private keys.
d. In the case of using the EFS with a local user account, the local password repository is encrypted with the help of Syskey. Alternatively, Windows Defender Credential Guard may be used.
e. The users have been trained to use the EFS securely.

SYS.2.2.3.M22 Use of Windows PowerShell (C-I-A)

a. Only system administrators may activate PowerShell and WPS files.
b. The commands activated in PowerShell are logged centrally.
c. In order to prevent the activation of unsigned scripts, the activation of PowerShell scripts is restricted by Set-ExecutionPolicy AllSigned command.

SYS.2.2.3.M23 Additional security of login information (C-I)

a. The SecureBoot method is used in a UEFI-based system.
b. Upon the activation of the system, the protection of the status of the credentials repository of LSA (Local Security Authority) is checked.
c. Where RDP is used for the remote maintenance of client systems and the functional level of the domain is 2012 R2 or higher, restrictedAdmin is set as the RDP mode of operation.

SYS.2.2.3.M24 Activation of the time stamping of the last access (A)

a. The Last Access time stamp is activated in the file system (NTFS).
b. Constant time stamping is used if it does not significantly affect the performance of the system.

SYS.2.2.3.M25 Secure application of CUET remote access functions of a component (C-I)

a. Instances of remote access by a Windows 10 component called CUET (Connected User Experience and Telemetry) are logged.
b. As CUET enables the manufacturer of an operating system to request data from the client computer, CUET is blocked where necessary.

SYS.2.2.3.M26 Using VSM (Virtual Secure Mode) (C-A)

a. The fact that using VSM hinders computer forensics has been taken into account.

SYS.2.3 Linux and Unix client

1 Description

1.1 Purpose

To present the measures applied for the protection of the data of the client computers (clients) using Linux or Unix operating systems.
There are different Linux distributions and Unix derivatives, but the configuration and behaviour of the clients are similar. Therefore, Linux and Unix are referred to by using a uniform term of 'Unix client' in this module.
Unix-based client computers are usually networked and use 'client-server' type IT solutions.

1.2 Responsibility

The IT department is responsible for the compliance with the security measures applicable to a Unix client.
Additional responsible persons: User.

1.3 Limitations

The module specifies and complements the measures provided in the module SYS.2.1 Client computer in general with specific guidelines applicable to Unix systems. The security measures of the software used in the client computer (e.g. email clients or office software) are provided in the relevant modules of the module group APP.1 Client applications.
It is presumed in the module that there is only one permanently active user account in the client computer in addition to the administration account designed for the management of the client computer.

2 Threats

2.1 Software from sources which have not been validated

Instead of installing ready-made applications of Unix-like IT systems, the packages are downloaded and the program is compiled on site. Software packages are often downloaded from sources which have not been validated. If the manufacturer's reliable package repository is not used, there is a risk of unintentionally downloading and installing an incorrect or incompatible software package or software which contains malicious functions.

2.2 Exploitation of the script environment

Scripts written in the scripting language and activated from the command line are used in the Unix operating systems to facilitate the work of the administrator and prevent human errors. An attacker may extensively manipulate and exploit the scripts to achieve their goals.

2.3 Dynamic downloading of shared libraries

The 'LD_PRELOAD' command loads the selected dynamic library (dynamically linked shared object library) before any other standard libraries needed in the application. This enables to ignore the specific functions of standard libraries. An attacker may manipulate the system so that a malicious program is activated upon activation of certain applications.

2.4 Configuration errors

Numerous applications which can be configured separately are installed in the course of the standard installation of Unix operating systems. As many applications are configured independently from one another, the configuration choices made may be conflicting and cause conflicts which are not directly visible from the settings of any one specific application. Applications may also include additional functions which are not actually desired by the user of the client computer, or vice versa, some important security functions may not be activated.

3 Measures

3.1 Life cycle

Operation

SYS.2.3.M1 Authentication of administrators and users

SYS.2.3.M4 Updating the kernel of the operating system

SYS.2.3.M9 Secure use of passwords on the command line

SYS.2.3.M12 Secure use of special devices with Linux

Acquisition

SYS.2.3.M2 Selecting a suitable distribution

Implementation

SYS.2.3.M5 Secure installation of software packages

SYS.2.3.M6 Prohibition on the automatic mounting of a removable device on the file system

SYS.2.3.M7 Restriction of file and directory rights

SYS.2.3.M8 Restriction of the access rights of applications

SYS.2.3.M11 Prevention of overloading the hard disk

Additional advanced measures

SYS.2.3.M14 Avoiding unauthorised peripherals

SYS.2.3.M15 Additional protection from activating undesired files

SYS.2.3.M17 Additional protection from the exploitation of vulnerabilities

SYS.2.3.M18 Additional kernel security

SYS.2.3.M19 Encryption of a hard disk or files

SYS.2.3.M20 Restricting critical SysRq functions

3.2 Key measures

SYS.2.3.M1 Authentication of administrators and users [user]

a. Administrators do not log into the client computer as root users for the daily work.
b. The sudo command or a suitable alternative is used for administrative tasks.
c. Several users cannot be simultaneously locally logged into one client computer.

SYS.2.3.M2 Selecting a suitable distribution

a. The suitable Unix derivative or Linux distribution is selected based on the intended purpose and security requirements.
b. An operating system is selected, the issuer of which guarantees product support (e.g. in the form of hardware component drivers) for the entire estimated service life of the system.
c. Most-used applications are part of the distribution and are not downloaded from unapproved sources. The manufacturer's support is ensured for the application programs installed in addition to

the distribution.
d. Distributions which are very often complemented with small updates are not selected for work-related use. Internally compiled distributions are also not used.

SYS.2.3.M4 Updating the kernel of the operating system

a. Before updating the kernel of the operating system of the client computers, the compatibility of the update with the existing system is tested and it is made sure that the update will not cause any errors.
b. After updating the kernel, the client computer is immediately restarted. If this is not enabled by the system, dynamic patching of the kernel is used (Linux Kernel Live Patching).

SYS.2.3.M5 Secure installation of software packages

a. In the event of compiling software from a source code, the software may only be unpacked, configured, and complied under an account with ordinary user rights.
b. In the event of compiling software from a source code, all parameters used are documented. It must be possible to repeat the software compilation based on the documentation.
c. Software is not installed in the root file system of the server.
d. If possible, software packages should be installed with the help of a package manager, not one by one from the command line.

3.3 Standard measures

SYS.2.3.M6 Prohibition on the automatic mounting of a removable device on the file system [user]

a. Removable devices are not automatically mounted to the file system.
b. Mounting removable devices on the file system is configured so that the files cannot be activated (option 'noexec').

SYS.2.3.M7 Restriction of file and directory rights

a. Services and applications can only create, edit, and delete the files allocated to them.
b. Sticky bits are allocated to the directories in which all users have writing rights (e.g. /tmp).

SYS.2.3.M8 Restriction of the access rights of applications

a. The access of an application to files, devices, and networks is restricted by the security module of the kernel of the particular distribution (e.g. App-Armor or SELinux).
b. Access rights of applications are blocked by default; rights are added based on business requirements.
c. The rights are restricted with the enforcing mode of the security module or with the help of an appropriate alternative.

SYS.2.3.M9 Secure use of passwords on the command line [user]

a. Passwords and other pieces of sensitive information are not sent to programs in the form of command line parameters.

SYS.2.3.M11 Prevention of overloading the hard disk

a. Quotas have been set for the users and services. When the disk capacity has been used to a certain level, only the root user will have writing rights.
b. As a general rule, the kernel and data of an operating system are stored in different disk partitions.

SYS.2.3.M12 Secure use of special devices with Linux

a. The security level of the appliances using the Linux operating system is equivalent to the security level of standard Linux client computers.
b. The security requirements applicable to the appliances are documented.
c. If necessary, the manufacturer of the device is asked to prove the compliance of the security.

3.4 Advanced measures

SYS.2.3.M14 Avoiding unauthorised peripherals (C-I-A)

a. The peripherals of a client computer may only be used when the use of the peripheral in question has been permitted in a documented manner.
b. The kernel modules required for the functioning of a peripheral are only downloaded and activated if the device has a permit for use.

SYS.2.3.M15 Additional protection from activating undesired files (C-I)

a. The sections and directories which the users have writing rights to are mounted on the file system so that the files cannot be activated (noexec mounting parameter).

SYS.2.3.M17 Additional protection from the exploitation of vulnerabilities (C-I)

a. The use of the system calls of the services and applications at risk is limited to an appropriate level (e.g. by using seccomp).
b. The standard profiles and rules of App-Armor, SELinux, and alternative security modules are customised based on the security policy of the organisation.
c. New rules or profiles are created, if necessary.

SYS.2.3.M18 Additional kernel security (C-I)

a. Appropriate extensions (e.g. grsecurity, PaX) are applied to reinforce the kernel, which prevent the spread of malware and the exploitation of the vulnerabilities of the operating system.

SYS.2.3.M19 Encryption of a hard disk or files (C-I)

a. The hard disks of the client computer or the files saved in the client computer are encrypted. The respective encryption keys are stored outside of the IT system.
b. The AEAD (Authenticated Encryption with Associated Data) encryption procedure or the alternative dm-crypt application with the dm-verify application are used for the encryption of the disks and files.

SYS.2.3.M20 Restricting critical SysRq functions (C-I-A)

a. The SysRq functions which can be activated by the users in the kernel by using a key combination have been determined.
b. Key combinations cannot be used to activate potentially harmful commands.

SYS.2.4 macOS client

1 Description

1.1 Purpose

To present the measures applied for the protection of the data stored in the client computers using the macOS operating system. macOS is an operating system used in Apple computers. This module focuses of the security of the Mac computers using macOS which are treated as an autonomous system or as a 'client-server' type network client.

1.2 Responsibility

The IT department is responsible for the compliance with the security measures applicable to a macOS client.
Additional responsible persons: User.

1.3 Limitations

The module does not cover the potential use of macOS as a server operating system.
The module specifies and complements the measures provided in the module SYS.2.1 Client computer in general with specific guidelines applicable to macOS.
The security measures of the software operated in the client computer (e.g. email clients or office software) are provided in the relevant modules of the module group APP.1 Client applications.
As both of the Apple operating systems (macOS for the Mac computers and iOS for iPhone and iPad) are tightly connected, the security aspects of central management of Mac computers are also discussed in the modules SYS.3.2.2 Mobile device management (MDM) and SYS.3.2.3_ iOS of the organisation_.

2 Threats

2.1 Uncontrolled access to externally stored data

macOS provides access to several services (e.g. iCloud for data storage and synchronisation) which are operated in the central servers of Apple. As all of the data is no longer fully under the control of the organisation, there is a chance of unauthorised persons gaining access to the servers, viewing the data stored or sent there, and abuse the data for their own purposes.

2.2 Abuse of an Apple ID account

In order to use the macOS functions, the access data must include an Apple ID. The Apple ID is used to centrally grant access to various different Apple services, such as iCloud, iMessage, iTunes, and

the App Store. If an unauthorised person has access to the Apple ID, they can use those services with a falsified identity and access the information in the iCloud, for example.

2.3 Attacks against wireless interfaces

A Mac computer has the interfaces of a wireless local area network and Bluetooth which are used by many services and are usually activated on the computer. For example, the wireless local area network function enables exchanging files directly between Apple devices (AirDrop). AirPlay can be used to send video or audio streams to compatible playback devices. An attacker may abuse the wireless interfaces to catch the confidential information sent between a Mac computer, iPhone, iPad, or other devices.

2.4 Attacks against applications with the preview function

Some applications integrated into macOS (Finder, Safari, the macOS email program) support the preview function of certain file formats, which opens files and email attachments automatically. An attacker may hide malicious code in a document or image file enclosed to an email. In this case, the preview function is likely to activate the malicious code upon opening the file, which may result in a data leak, data deletion, or seizure of the computer by the attacker.

2.5 Insecure protocols in macOS or in the macOS applications

For communication with central servers or other devices, macOS and the applications thereof support different, partly Apple's own protocols, such as AFP (Apple Filing Protocol). If the data communication protocols lack sufficient security mechanisms or are configured in an insecure manner, those protocols can be used for unauthorised access to, falsification of, or other abuse of the data sent.

3 Measures

3.1 Life cycle

Planning

SYS.2.4.M1 Secure macOS implementation plan

Implementation

SYS.2.4.M2 Using the security functions of macOS

SYS.2.4.M3	User account administration
SYS.2.4.M4	Hard disk encryption
SYS.2.4.M5	Deactivating the functions endangering security
SYS.2.4.M7	Multifactor authentication of the Apple ID
SYS.2.4.M9	Using additional security software
Acquisition	
SYS.2.4.M6	Modern hardware
Operation	
SYS.2.4.M8	iCloud prohibition on storing sensitive data
Disposal	
SYS.2.4.M11	Secure disposal of the device
Additional advanced measures	
SYS.2.4.M12	Firmware password and booting protection

3.2 Key measures

SYS.2.4.M1 Secure macOS implementation plan

a. A plan has been drawn up for the deployment of macOS clients.
b. The deployment plan of macOS clients includes at least the following:
- regular updates of macOS and the applications;
- logging of the macOS client;
- backing up the data of the client computer;
- malware control in macOS.

c. Compatibility of macOS with the applications, equipment, protocols, and licence agreements has been analysed, as well as the need to replace applications arising from changing platforms.
d. The need for using additional network protocols for the use of the macOS client in the network has been analysed.

SYS.2.4.M2 Using the security functions of macOS

a. The SIP (System Integrity Protection), Xprotect, and Gatekeeper security mechanisms integrated into macOS are activated.
b. Gatekeeper only allows the activation of the applications acquired from the App Store and signed,

unless unsigned special applications are used by the organisation.
c. When a new application is installed, compliance of the signature thereof is checked and a malware scan is carried out, if necessary.

SYS.2.4.M3 User account administration [user]

a. The administrative account created during the initial configuration of macOS is only used for administrative operations.
b. An ordinary user account is created for the ordinary use of the macOS client. If a macOS computer is used by several users, personal accounts are created for all users.
c. The system can only be logged into by using the username and password; automatic login is deactivated.
d. After a longer break in the use, the user is automatically logged out (the 'Log out after... minutes of inactivity' privacy setting is activated).
e. The guest account option is deactivated.
f. The 'Allow guests to connect to shared folders' option is deactivated under the system settings.
g. The use of the screen lock is activated. The user's password is requested for unlocking the screen.
h. The 'Require an administrator password to access system-wide preferences' option is activated under the security and privacy settings of the macOS client.

3.3 Standard measures

SYS.2.4.M4 Hard disk encryption

a. The hard disk of a Mac computer (especially a mobile MacBook) is encrypted.
b. If the FileVault encryption function integrated into macOS is used:
- the key information is not stored in the web environment of Apple;
- the FileVault recovery key is kept in a secure location;

c. managers have access to the FileVault recovery key, if necessary.
d. Any disk images made of a Mac computer are encrypted.

SYS.2.4.M5 Deactivating the functions endangering security

a. The location services of macOS are deactivated.
b. No files downloaded in Safari are opened automatically.
c. Automatic activation or displaying of the content of the data media is blocked.

d. The list of recently used applications, documents, and network connections is condensed.
e. The 'Secure EmptyTrash' option is used to empty the recycle bin of a Mac computer.

SYS.2.4.M6 Modern hardware

a. Updated product models are selected when purchasing new Mac computers.
b. The existing Mac computers are still supported with Apple's security updates.
c. When the Apple product support is discontinued, any affected Mac models are decommissioned.
d. If possible, the newest macOS version is always used.

SYS.2.4.M7 Multifactor authentication of the Apple ID [user]

a. Multifactor authentication is activated for using the Apple ID account.
b. Two independent components (e.g. a password and a code sent by a text message) are used for multifactor authentication.

SYS.2.4.M8 iCloud prohibition on storing sensitive data [user]

a. Synchronisation of sensitive data between different devices via the iCloud service is prohibited.
b. Sensitive data may only be synchronised between internal services of the organisation.
c. Sensitive data is not stored on iCloud.
d. Automatic saving of draft documents and emails in the iCloud is blocked.
e. The Handoff function for transferring data to another device is deactivated.

SYS.2.4.M9 Using additional security software

a. The personal firewall built into macOS is activated and configured appropriately.
b. Application Firewall is activated and configured accordingly.
c. Camouflage mode is deactivated.
d. After each operating system update, the firewall configuration is checked.

SYS.2.4.M11 Secure disposal of the device

a. Before the disposal of a device, the data is deleted securely from the data media. The disk utility on the macOS installation medium may be used for this purpose.
b. The non-volatile memory (NVRAM) with system settings is also reset upon the disposal of a Mac computer.

3.4 Advanced measures

SYS.2.4.M12 Firmware password and booting protection (C-I-A)

a. Booting a Mac computer from an external data medium is prohibited and a firmware password is activated to prevent changing the settings. On older Mac computers, the firmware password must be activated in the command mode.
b. In Mac computers with the T2 security chip, the firmware password is set via the Startup Security Utility with the 'Full Security' option activated.

SYS.3 Mobile devices

SYS.3.1 Laptop computers

1 Description

1.1 Purpose

To present the measures for the secure use of laptop computers at the organisation and to increase awareness of the specific risks of this device class.
Laptop computers with all of the commonly used operating systems (Microsoft Windows, Apple macOS, or Linux distributions) are used. Laptops are common at most organisations and have often replaced the traditional desktop computers.

1.2 Responsibility

The IT department is responsible for compliance with the measures applicable to laptop computers.
Additional responsible persons: User, procurement department, information security manager.

1.3 Limitations

The module SYS.3.1 Laptop computers is applied to all laptop computers in mobile or stationary use. The security measures suitable for all client computers are provided in the module SYS.2.1 Client computer in general.
The security measures of the different operating systems of laptop computers are described in the

modules SYS.2.2.3 Windows 10 client, SYS.2.3 Linux and Unix client, or SYS.2.4 macOS client. Network connections of laptop computers are covered in the modules NET.2.2 Using wireless local area networks and NET.3.3 Virtual private network (VPN).
Laptop computer data backup is described in the module CON.3. Data backup concept.

2 Threats

2.1 Threats arising from the changing operation environment

Laptop computers may be damaged due to environmental impacts, such as excessively high or too low temperature, dust, or humidity. Mobile devices may be physically damaged during transportation or due to being constantly carried around. Laptop computers are often connected to unknown IT systems or networks, especially when travelling. This always comes with the risks of infection with malware or data theft.

2.2 Loss or theft of a laptop computer

Using laptop computers outside of the organisation is accompanied by the risk of loss or theft of the laptop computer. The devices are transported in car or public transport vehicles, left in unknown offices during breaks, or unattended in a hotel room. The expenses of reconfiguration of the laptop computer and data recovery are added to the cost of replacing a lost or stolen laptop computer.

2.3 Replacement of the users of a laptop computer

If the employees only require mobile IT systems in exceptional cases, for example during work trips, it is often reasonable to have one laptop computer for numerous users. Handing a laptop computer over to the next employee comes with the risk of also handing over the data requiring protection which has remained in the device. The laptop computer may also be infected with malware. It is difficult to determine who has been using the laptop computer and when or who is using it currently. The laptop computer contains the residual data from many users, which may include password and sensitive data.

3 Measures

3.1 Life cycle

Planning

SYS.3.1.M1 Procedure for the mobile use of laptop computers

SYS.3.1.M6 Guidelines for using laptop computers

Implementation

SYS.3.1.M3 Personal firewall

SYS.3.1.M8 Secure connection to a data communication network

SYS.3.1.M13 Encryption of the content of a laptop

Emergency response

SYS.3.1.M5 Data backup of a laptop computer

Operation

SYS.3.1.M9 Secure remote access

SYS.3.1.M7 Procedure for the issuance and return of laptop computers

SYS.3.1.M10 Synchronisation of data

SYS.3.1.M11 Ensuring power supply

SYS.3.1.M12 Reporting the loss of a laptop computer

SYS.3.1.M14 Physical security of a laptop computer

Acquisition

SYS.3.1.M15 Procedure for choosing a laptop computer

Additional advanced measures

SYS.3.1.M16 Central management of laptop computers

SYS.3.1.M17 Secure storage of laptop computers

SYS.3.1.M18 Use of anti-theft tools

3.2 Key measures

SYS.3.1.M1 Procedure for the mobile use of laptop computers

a. The organisation has established a procedure for the mobile use of laptop computers, which specifies the following:

b. The procedure for the mobile use of laptop computers specifies the following:

- which laptop computers can be used outside of the organisation;
- who are permitted to remove laptop computers from the premises;
- which security measures must be implemented;

• the liability of the user.

c. The security measures applied to a laptop computer are appropriate for the protection requirement of the data handled in the device.

SYS.3.1.M3 Personal firewall

a. If a laptop computer is used outside of the intranet of the organisation, a personal firewall is activated in the laptop computer.

b. The personal firewall may be come with the operating system or be part of the security solution of a third party, but it is prohibited to apply several firewalls simultaneously.

c. Only duly authorised managers manage personal firewalls.

d. The filtration rules of the firewall are as restrictive as possible. The incoming connections permitted are limited to remote maintenance, system updates, and the connections required for monitoring.

e. Personal firewalls are configured to function without displaying complex warnings to the users.

f. If a personal firewall supports logging, security events are logged.

SYS.3.1.M5 Data backup of a laptop computer [user]

a. Any files which are being stored locally, but not in the server, are backed up regularly.

b. If necessary, the data in a laptop computer is backed up in the course of temporary network connections (e.g. VPN). If there is no network connection, the data in a laptop computer is backed up onto an external data medium in an encrypted format.

SYS.3.1.M9 Secure remote access

a. The intranet is accessed from a laptop computer in an encrypted format via a virtual private network (VPN) (see NET.3.3 Virtual private network (VPN)).

b. After using a VPN connection, the authentication data and temporary data is deleted.

3.3 Standard measures

SYS.3.1.M6 Guidelines for using laptop computers [information security manager]

a. The organisation has drafted and implemented guidelines for using a laptop computer.

b. The guidelines for using laptop computer specify the following:

- the manner of managing, issuing, and returning laptop computers;
- which data and under which conditions may not be stored in a laptop computer;
- which data must always be encrypted;
- how to use the server resources of the organisation from the laptop computer;
- whether or not it is permitted to use laptop computers for personal purposes;
- how to prevent the loss or theft of a laptop computer;
- how to use passwords and PINs;
- whether and how it is permitted to work in public places (see INF.9 Mobile workplace);
- where and when is it not permitted to use laptop computers.

c. Users are aware of the threats accompanying using a laptop computer and must comply with the guidelines for using a laptop computer.

SYS.3.1.M7 Procedure for the issuance and return of laptop computers [user]

a. If possible, one laptop computer is only used by one employee. If laptops are used alternately by different individuals, the procedure of handing a laptop over from one user to another has been established.
b. In the event of a change in the user of a laptop computer, any sensitive data, including residual data, is securely deleted from the laptop computer.
c. A laptop computer is returned as a complete and entire set.
d. In the event of issuing a used laptop computer to a new user, the initial status of the laptop computer is restored by standard installation. If a laptop computer is not reset upon changing the user, the computer and the data media connected thereto are scanned for malware.

SYS.3.1.M8 Secure connection to a data communication network

a. When data communication is used, a personal firewall is always activated (see SYS.3.1.M3 Personal firewall).
b. Only authorised laptop computers can log into the intranet of the organisation (e.g. by certificate-based authentication of devices).
c. Unnecessary interfaces and protocols have been deactivated on the laptop computers.

SYS.3.1.M10 Synchronisation of data

a. Laptop computers are equipped with synchronisation tools and a procedure has been established for the synchronisation of data between laptop computers and the IT systems of the organisation.
b. The synchronisation tools and settings are protected from unlawful access.
c. Synchronisation tools enable logging the synchronisation processes and solving potential synchronisation conflicts.
d. Users know how to check synchronisation logs.

SYS.3.1.M11 Ensuring power supply [user]

a. In order to prevent data losses, the user must save the data at appropriate intervals in the case of battery-powered operation.
b. In order to extend the service life of the battery, laptop computers are charged by using a charger approved by the manufacturer of the computer and in the manner specified in the user instructions.
c. In the event of a longer mobile use of a laptop computer, the user must always bring along the charger.
d. If there are spare batteries for a laptop computer, the batteries are always transported and stored in appropriate sleeves and environmental conditions.

SYS.3.1.M12 Reporting the loss of a laptop computer [user]

a. The organisation has established a procedure for reporting the loss, theft, or failure of a laptop computer.
b. The user must report the loss, theft, or a failure of a laptop computer immediately.
c. If possible, the measures which enable to lock, wipe, or localise the device must also be used after the loss of a laptop computer (see SYS.3.2.2 Mobile device management (MDM)).
d. After the loss of a laptop computer, the access data of the user is changed in all presumably affected IT systems.
e. If a lost laptop computer is returned, checks are carried out to make sure that the device has not been manipulated. As a rule, software on such laptop computers is fully reinstalled.

SYS.3.1.M13 Encryption of the content of a laptop

a. The data media integrated into a laptop computer (hard disk, SSD) are encrypted.
b. As a rule, encryption tools integrated with the operating system are used for the encryption of the hard disk.

SYS.3.1.M14 Physical security of a laptop computer [user]

a. In the premises of the organisation, laptop computers are protected from theft and unauthorised use during and outside of the working hours.
b. As a rule, laptop computers are not left unattended. Outside of the organisation, the user keeps the laptop computer in a locked location which is protected from theft (see INF.8 Home workplace).
c. In external premises, the employees take their laptop computers with them even if only they leave the room for a moment. If this is not possible, the device must be switched off and locked.
d. Laptop computers are transported in laptop bags with special pockets and padding.
e. In the event of leaving a laptop computer in a motor vehicle, the computer may not be visible from the outside of the vehicle.
f. Laptop computers are protected from harmful environmental conditions (e.g. excessive humidity, extreme temperatures).

SYS.3.1.M15 Procedure for choosing a laptop computer [procurement department]

a. Before the procurement of laptop computers, the requirements for the hardware and software are drawn up based on the intended use of the computers.
b. At least the following is taken into consideration when choosing laptop computers:
- the availability of product support and maintainability;
- reliability;
- accessibility (user friendliness and convenience of installation, configuration);
- the dimensions, weight, and battery life;
- compatibility with the existing devices;
- network interfaces and connection options;
- the security mechanisms and the possibilities for adding such mechanisms;
- any additional hardware (e.g. computer docks and monitors);
- the acquisition cost and additional costs of the hardware and software.

c. The procurement decision is based on the results of analysing the needs and is coordinated with the managers and the persons responsible for IT support.

3.4 Advanced measures

SYS.3.1.M16 Central management of laptop computers (C-I)

a. A procedure for the central management of laptop computers has been established (see SYS.3.2.2 Mobile device management (MDM)).
b. The tools of central management support all operating systems used in the laptop computers of the organisation.

SYS.3.1.M17 Secure storage of laptop computers (A)

a. Any laptop computers of the organisation which are not currently in use are stored securely.
b. The measures described in the module INF.5 Room or cabinet of technical infrastructure are applied to the storage room.

SYS.3.1.M18 Use of anti-theft tools (C-I-A)

a. The users of laptop computers have received anti-theft tools which must be used when a laptop computer is left unattended.
b. Mechanical anti-theft tools (e.g. cable locks, security housings) are equipped with efficient locking systems.
c. When choosing a new laptop computer to purchase, it is made sure that the housing of the computer can be fixed with a cable lock.

SYS.3.2 Smartphones and tablets

SYS.3.2.1 Smartphones and tablets in general

1 Description

1.1 Purpose

To introduce the typical threats related to smartphones and tablets and describe the measures for the prevention and elimination of those threats.
A tablet mainly differs from a smartphone by its larger touch screen and limited functions for making calls. The threats and measures are similar for both types of devices.

1.2 Responsibility

The IT department is responsible for implementation of the measures described under 'Smartphones and tablets in general'.
Additional responsible persons: User, information security manager.

1.3 Limitations

Protection of the specific operating systems of smartphones and tablets is also described in the modules SYS.3.2.3 iOS of the organisation and SYS.3.2.4 Android. The measures related to mobile device management are described in the modules SYS.3.2.2 Mobile device management (MDM) and SYS.3.3 Mobile phone.
Protection of the client applications of smartphones and tablets are described in the modules APP.1.4 Mobile applications (apps) and APP.1.2 Web browser.
The measures for protection against malware are described in the module OPS.1.1.4 Protection against malware.

2 Threats

2.1 Outdated operating system

New versions and updates are regularly published for the operating systems used in mobile devices. Manufacturers usually only offer new versions and updates for the newest generation of devices. No software updates are available for older smartphones and tablets and those of a lower price class. Such operating systems contain known vulnerabilities which cannot be eliminated by regular security patches and are especially easy for attackers to exploit.

2.2 Software vulnerabilities in mobile applications (apps)

The pre-installed applications provided with a smartphone or tablet may contain security vulnerabilities. Those vulnerabilities can be exploited to attack the device through the network connection. Many of the apps installed in the device by the user are also no longer maintained and updated after a while. In such case, those apps may also conceal vulnerabilities which cannot be eliminated even by updating the operating system.

2.3 Manipulation of a smartphone or tablet

By gaining access to a smartphone or tablet, an attacker may deliberately manipulate the data on the device. They can, for example, change the configuration of the device, launch further services, or covertly install malware. In a manipulated system, it may be possible to record communication sessions (i.e. create a data leak) or create new access routes to the device based on the attacker's needs (e.g. permit access from the Internet to check the device).

2.4 Malicious programs of smartphones and tablets

Smartphones and tablets, like any other devices with an Internet connection, come with an especially high risk of being infected with malware. In recent times, particularly large amounts of attacks have been targeted at mobile devices as there are still many devices in use which are equipped with outdated software or have not been updated. Furthermore, the anti-virus and anti-malware applications created for smart devices are not as efficient as the security applications designed for the operating systems of computers. If the user has acquired apps from unreliable sources or if there are no updates available for the vulnerabilities, the risk of infection is especially high. In a device with malware, attackers can read, change, and use the data or the mobile device can be used to access the IT resources of the organisation.

2.5 Web-based attacks against mobile browsers

Mobile browsers are not as capable and secure as analogous web browsers designed for computers. Web content may also be displayed by other mobile apps in addition to the web browsers issued by acknowledged manufacturers (Chrome, Safari, Edge, etc.). This makes smartphones and tablets vulnerable to various different types of web-based attacks (e.g. phishing attacks or drive-by attacks).

2.6 Abuse of health and location data

Smartphone and tablet apps may include special functions and additional applications for managing the user's health, training, or location data. Sensitive personal data, especially data collected over a long period of time, is an attractive target for attackers.

2.7 Abuse of the data displayed on a locked screen

Many operating systems of mobile devices are equipped with a function which enables reading the messages displayed by activated widgets, text messages, or the headers of emails on the locked screen. This may make the user's confidential information visible to an unauthorised person and the

information can be taken advantage of. Some communication applications also enable access to the contact details of individuals even a locked state.

2.8 Personal use of a work phone or tablet

It is usually allowed to also use the smartphones and tablets owned by the organisation for personal purposes. This creates several security issues from the perspective of the organisation. For example, the user may install applications with malware functions or visit a website which infects the device with malware. An attacker may also use the applications installed by the user for personal purposes (e.g. a social media app or an instant messaging application) to access the contact details of the organisation (e.g. the address book).

2.9 Risks arising from using personal devices (bring-your-own-device (BYOD))

Several threats arise from using personal smartphones or tablets for performing work-related tasks. If the need to delete any work-related data is identified via central mobile device management, this may also affect the user's personal data. The persons responsible for IT cannot check the compliance of all personal devices with the security requirements of the organisation. Consequently, inappropriate devices and devices with security vulnerabilities are used. Users are responsible for the maintenance and repair of their own devices. If a smartphone is repaired, the person repairing the phone may gain access to the data of the organisation. Problems may also arise due to a lack of appropriate software licences (e.g. if any apps which are only permitted for personal purposes are used for performing work-related tasks).

2.10 Exploiting software vulnerabilities for unauthorised access

The operating systems of the devices of many manufacturers (especially older Android versions) contain vulnerabilities which allow to ignore security measures implemented by the manufacturer. An attacker can gain unauthorised access to protected system processes and memory areas of the device (root access). Root access rights enable the attacker to manipulate the device and the data on the device or install prohibited apps or malware for attacking the device or the intranet of the organisation. Anyone can take advantage of the vulnerabilities by using publicly available tools and instructions.

3 Measures

3.1 Life cycle

Planning

SYS.3.2.1.M1 Establishing security requirements for smartphones and tablets

SYS.3.2.1.M2 Procedure for using cloud services

Implementation

SYS.3.2.1.M3 Secure baseline configuration of a mobile device

SYS.3.2.1.M8 Procedure for the installation of mobile applications

SYS.3.2.1.M9 Restriction of additional functionality

SYS.3.2.1.M10 Guidelines for using mobile devices

SYS.3.2.1.M11 Encryption of the memory of a smartphone or tablet

SYS.3.2.1.M12 Using anonymous device names

SYS.3.2.1.M13 Procedure for screen sharing and shared media use

SYS.3.2.1.M16 Deactivation of unnecessary communication interfaces

SYS.3.2.1.M19 Restriction of the use of virtual assistants

SYS.3.2.1.M31 Procedure for handling mobile payments

Operation

SYS.3.2.1.M4 Prevention of unauthorised use

SYS.3.2.1.M5 Updating the operating system and applications

SYS.3.2.1.M6 Management of privacy settings and access to applications

SYS.3.2.1.M7 Procedure for responding to security events

SYS.3.2.1.M18 Biometric authentication

SYS.3.2.1.M22 Using VPN for connecting to the intranet

SYS.3.2.1.M28 Filtration of websites

SYS.3.2.1.M32 Use of central mobile device management (MDM)

SYS.3.2.1.M33 Use of an anti-malware application

SYS.3.2.1.M34 Secure configuration of the DNS server

Additional advanced measures

SYS.3.2.1.M25 Separation of execution environments

SYS.3.2.1.M26 Use of PIM

SYS.3.2.1.M27 High-security mobile device

SYS.3.2.1.M29 Organisation-based access point (APN)

SYS.3.2.1.M30 Whitelist of installing apps

SYS.3.2.1.M35 Firewall for mobile devices

3.2 Key measures

SYS.3.2.1.M1 Establishing security requirements for smartphones and tablets [information security manager]

a. The organisation has established the procedure for the secure use of smartphones and tablets.
b. Services containing the data of the organisation which may be used in mobile devices (e.g. the email service) have been identified.

SYS.3.2.1.M2 Procedure for using cloud services

a. The organisation has established a procedure for the secure use of cloud services for smartphones and tablets which specifies which cloud services may be used and how the employees' use of cloud services is monitored.
b. The users have been notified of permitted and prohibited cloud services (incl. for personal use).
c. The users are trained to use cloud services securely.

SYS.3.2.1.M3 Secure baseline configuration of a mobile device

a. Before issuing to the users, mobile devices are configured based on the protection requirement of the data.
b. The organisation has developed and documented a baseline configuration for smartphones and tablets which supports security mechanisms.
c. Useless functions and data connection interfaces are deactivated in mobile devices.
d. The client components required for central mobile device management are added to the baseline configuration.

SYS.3.2.1.M4 Prevention of unauthorised use [user]

a. Smartphones and tablets are protected by sufficiently complex passcodes.
b. It is mandatory to use screen locks on mobile devices. The activation times of the screen locks must be sufficiently short (between 15 seconds and 1 minute, depending on the protection requirement).

c. When changing the password or PIN of a mobile device, recently used passwords cannot be reused.

SYS.3.2.1.M5 Updating the operating system and applications

a. Manufacturers of mobile devices ensure the availability of regular updates of the operating system during the estimated service life of the device.
b. Older devices for which operating system security patches are no longer issued are decommissioned and replaced with devices with the manufacturer's software support.
c. No applications (apps) with expired manufacturer's support are used in the smartphones and tablets of the organisation.

SYS.3.2.1.M6 Management of privacy settings and access to applications

a. The access of applications to the data and data exchange interfaces is strictly need-based. The access rights of an application are approved by the user of the mobile device.
b. Privacy settings are configured as restrictively as possible.
c. Access to the camera, microphone, the user's location and health data is compliant with the data protection requirements. If necessary, access is restricted or the respective function is deactivated.
d. The access rights of mobile applications are reviewed as and when needed.

SYS.3.2.1.M7 Procedure for responding to security events [user]

a. The users notify the organisation of any smartphone- or tablet-related security events as soon as possible.
b. Security events are reported via designated reporting channels.
c. In the event of losing a device or detecting unlawful changes made to software, the employees immediately implement measures to prevent access to the data.

SYS.3.2.1.M8 Procedure for the installation of mobile applications

a. The organisation has established whether and which applications may be installed on mobile devices by the users.
b. Acceptable sources for acquiring applications and the criteria for selecting the sources have been established.

c. Installation of mobile applications from any sources other than the sources specified and approved is prohibited and, if possible, blocked.

3.3 Standard measures

SYS.3.2.1.M9 Restriction of additional functionality

a. Deployment of additional functionalities (e.g. new apps) of smartphones or tablets is considered carefully. If there is no direct need, using such additional functionalities is foregone.
b. Adding additional functionalities does not provide access to sensitive data, unless this is unavoidable.
c. Additional functionalities do not alter the security settings established by the baseline configuration (see SYS.3.2.1.M3 Secure baseline configuration of a mobile device).

SYS.3.2.1.M10 Guidelines for using mobile devices [user, information security manager]

a. Guidelines for the secure use of mobile devices have been drawn up.
b. The guidelines for the secure use of IT resources include at least the following:
- the requirements for the secure use of mobile devices;
- secure storage of the mobile devices when the devices are not in use;
- maintenance of mobile devices;
- guidelines for action in the event of loss or failure of a mobile device.

c. It is not permitted to uninstall installed management software from a smartphone or tablet or change the security settings of a mobile device.
d. The guidelines establish the prohibition on rooting smartphones and tablets.

SYS.3.2.1.M11 Encryption of the memory of a smartphone or tablet

a. The read-only memory (ROM) of a smartphone or tablet is encrypted.
b. Any sensitive data on additional storage media (e.g. SD cards) is encrypted.

SYS.3.2.1.M12 Using anonymous device names

a. The device name specified in a smartphone or tablet does not contain references to the organisation or user.

SYS.3.2.1.M13 Procedure for screen sharing and shared media use

a. Screen sharing or shared use of sound and video on a smartphone or tablet are regulated organisationally or technically.
b. The users have been familiarised to the procedure for screen sharing and shared media use.

SYS.3.2.1.M16 Deactivation of unnecessary communication interfaces [user]

a. Communication interfaces are only activated if required and only in an appropriate environment.
b. If a central mobile device management system is used, the interfaces are managed via the system.

SYS.3.2.1.M18 Biometric authentication

a. Biometric authentication (e.g. by using a fingerprint sensor) are only used if the level of security achieved in this manner is at least equivalent to the security of password protection.
b. If the reliability of biometric authentication is questionable, biometric authentication is not used.
c. The users know how an attacker can attempt to falsify biometric features for the purposes of identity theft.

SYS.3.2.1.M19 Restriction of the use of virtual assistants

a. Voice assistants, such as Siri or Google Assistant, are only used if critically needed. As a rule, this functionality is deactivated in the devices.
b. It is not permitted to use a virtual assistant when the device is locked.

SYS.3.2.1.M22 Using VPN for connecting to the intranet

a. Mobile devices can be connected to the intranet from outside of the organisation only via a virtual private network (VPN).
b. Suitable procedures have been developed for using VPNs. Certificate-based authentication is used instead of passwords.

SYS.3.2.1.M28 Filtration of websites

a. If the organisation is using a reputation service or a respective proxy server, it is set as the global HTTP proxy in all browsers used.
b. If the proxy server is in the intranet, the mobile device is connected to it via the VPN permanently or based on an application.

c. If no proxy-based filtration of websites is used in mobile devices, blacklisting is used in the web browser of the mobile device or filtration based on the content filter of an independent manufacturer.

SYS.3.2.1.M31 Procedure for handling mobile payments

a. A procedure has been established at the organisation which regulates the mobile payments made via smartphones or tablets and compensation thereof.

SYS.3.2.1.M32 Use of central mobile device management (MDM)

a. Smartphones and tablets are managed by using a central mobile device management (MDM) solution (see SYS.3.2.2 Mobile device management (MDM).

SYS.3.2.1.M33 Use of an anti-malware application

a. An anti-malware application (app) has been installed in all smartphones and tablets.
b. If possible, the anti-malware app is installed through the central mobile device management solution and the status and error messages of the app can be managed centrally.

SYS.3.2.1.M34 Secure configuration of the DNS server

a. The DNS server of the manufacturer of the smartphone or tablet has been replaced with the DNS server of the organisation or the service provider of the organisation.
b. If the use of DNS over HTTPS (DoH) is enabled by the service provider, this functionality is activated in the devices.

3.4 Advanced measures

SYS.3.2.1.M25 Separation of execution environments (C-I)

a. If the employees are permitted to use the work devices received from the organisation for personal purposes, a separate execution environment has been created in the devices for this purpose.
b. If possible, separate execution environments are only used in devices which have been appropriately certified (e.g. based on Common Criteria).
c. All work-related data is located in the execution environment designed for work without any exceptions.

d. After a certain predetermined number of unsuccessful attempts to open a mobile device, the data of the work-related execution environment is deleted from the mobile device.

SYS.3.2.1.M26 Use of PIM (C-I-A)

a. The personal information contained in mobile devices has been encapsulated by using PIM (personal information manager) tools.
b. Personal data is protected by separate authentication and by encryption which is independent from the operating system.

SYS.3.2.1.M27 High-security mobile device (C-I-A)

a. The organisation only uses such mobile devices which have been approved for processing information (certified based on the information security classification or compliant with the applicable requirements).

SYS.3.2.1.M29 Organisation-based access point (APN) (C-I-A)

a. For identifying approved mobile devices by an organisation-based access point (APN), a strong, up to 64-bit authentication key has been agreed on with the mobile communication service provider.
b. All devices using the APN receive an IP address coordinated with the organisation from the mobile communication service provider.
c. CHAP (challenge-handshake authentication protocol) is used for authentication.

SYS.3.2.1.M30 Whitelist of installing apps (C-I-A)

a. Smartphone or tablet users may only install the applications which have been whitelisted and have been approved and checked.
b. Installation of any other applications is prevented or unauthorised applications are removed immediately by the central mobile device management tool.

SYS.3.2.1.M35 Firewall for mobile devices (C-I-A)

a. A local firewall has been installed and activated in smartphones and tablets.

SYS.3.2.2 Mobile device management (MDM)

1 Description

1.1 Purpose

To present the measures applied for the secure planning, operation, and implementation of mobile device management.
For the purposes of this module, mobile devices include the smartphones and tablets which use the Android and iOS operating systems adjusted to the mobile devices.

1.2 Responsibility

The IT department is responsible for compliance with the mobile device management measures.

1.3 Limitations

The module supplements the measures described in SYS.3.2.1 Smartphones and tablets in general in the context of central mobile device management. The security measures applicable to smartphones and tablets are also described in the modules of the specific operating systems, SYS.3.2.3 iOS of the organisation and SYS.3.2.4 Android.
The measures from the modules OPS.1.1.2 IT management and ORP.4 Administration of identity and rights are observed in the management of mobile devices.
The module does not cover the use of personal mobile devices for work-related purposes (bring your own device (BYOD)).

2 Threats

2.1 Insufficient synchronisation

Management software and regular data exchange with the mobile devices are required for the functioning of the central management of mobile devices. If a mobile device has not been synchronised with the mobile device management software for a while, there is no overview of the current situation of the mobile device. It is also not possible to centrally install new applications on a device or change the rules (settings) established by the managers of the mobile devices.

2.2 Errors in the management of mobile devices

Configuration of the central mobile device management software is complicated and the actual outcome may depend on the interaction of the configuration completed in different places. It is difficult to detect any mistakes made in the configuration of the mobile device management software. The errors made in the management may cause several threats to the mobile devices, having a direct or indirect effect on the security of the data and applications.

2.3 Insufficient management of access rights

In mobile device management, it is important to specify in detail who may change certain settings and who has access to certain data. If the rights granted to the role of an employee are too extensive, the employee may gain access to data or make unauthorised changes to the settings. In the case of excessive rights, the employee can install mobile applications which are not permitted in the organisation (e.g. use cloud storage services which have not been approved). Insufficient management of rights may result in leaks of sensitive data. The risk of violating personal data protection requirements also arises.

2.4 Unlawful tracking of location information through mobile device management

Most of the mobile device management tools can show where any specific device is located at a certain point in time. This is necessary for various different reasons, for example, data or applications can be permitted or blocked based on the location (so-called geofencing). Unfortunately, this also results in detailed movement profiles of the device and the user related to the device. If such data is collected without notifying the user properly, the data protection requirements arising from the legislation are violated. There is also the risk of the location profiles of the employees being accessed by an attacker who may use this information for extortion or for committing theft, for example. Organisations can also abuse the location information for monitoring employees unlawfully.

3 Measures

3.1 Life cycle

Planning

SYS.3.2.2.M1 Principles of mobile device management

Implementation

SYS.3.2.2.M2 Accepted mobile device models

SYS.3.2.2.M5 Installation of an MDM client

SYS.3.2.2.M12 Security of MDM

SYS.3.2.2.M22 Decommissioning mobile devices

Acquisition

SYS.3.2.2.M3 Choosing MDM software

Operation

SYS.3.2.2.M4 Integration of mobile devices with MDM software

SYS.3.2.2.M20 Regular reviews of mobile device management

SYS.3.2.2.M6 Logging and monitoring the device status

SYS.3.2.2.M7 Installation of mobile applications (apps)

SYS.3.2.2.M21 Certificate management

Additional advanced measures

SYS.3.2.2.M14 Assessment of apps by an external reputation service

SYS.3.2.2.M17 Monitoring the use of mobile devices

SYS.3.2.2.M19 Use of geofencing

SYS.3.2.2.M23 Enforcement of compliance requirements

3.2 Key measures

SYS.3.2.2.M1 Principles of mobile device management

a. The organisation has developed principles for the integration of the mobile devices used at the organisation with the IT infrastructure of the organisation depending of the protection requirement of the information processed.

b. The principles of mobile device management include at least the following:

- whether the mobile device management is organised internally, ordered from an external party, or organised by using a cloud service;
- what the requirements are for the content of the management service;
- what the desired response times are;
- which pieces of legislation, policies, and rules the mobile device management is compliant with;
- which mobile devices and operating systems are supported by the mobile device management;
- whether the mobile device management supports any independently managed device groups;
- whether the document management and data storage systems (e.g. cloud services) are also

interfaced with the MDM;

• whether the mobile device management also includes external (personal) mobile devices;

• the model of use of mobile devices (the employees' personal devices, personalised devices owned by the organisation, or shared devices).

c. The principles of mobile device management have been documented and coordinated with the information security manager.

SYS.3.2.2.M2 Accepted mobile device models

a. Before purchasing mobile devices, if has been determined which devices and operating systems may be used at the organisation.

b. All mobile devices purchased and the operating systems thereof are compliant with the mobile device management principles and the security requirements established at the company.

c. The MDM software has been configured so that the information of the organisation can only be accessed from approved devices.

SYS.3.2.2.M3 Choosing MDM software

a. The mobile device management (MDM) software is compliant with the mobile device management principles.

b. The MDM software allows for implementing technical and organisational security measures.

c. The MDM software supports all mobile devices used at the organisation.

SYS.3.2.2.M4 Integration of mobile devices with MDM software

a. All mobile devices of the organisation are integrated with the MDM software.

b. The MDM software enables the central configuration of the mobile devices and the central management of the configurations.

c. Before the integration of any mobile devices which have already been deployed with the MDM software and the configuration of these devices, the factory settings of the mobile device are restored.

d. No mobile device has access to the internal resources of the organisation without the respective centrally installed settings.

SYS.3.2.2.M5 Installation of an MDM client

a. Appropriate baseline configurations have been developed and documented for mobile devices.
b. The MDM client is installed in the mobile devices before handing the device over to the user. In exceptional cases, the user is required to install the MDM client.

SYS.3.2.2.M20 Regular reviews of mobile device management

a. The security settings of the mobile devices are checked regularly.
b. When new versions of the operating systems of the mobile devices become available, checks are conducted to determine whether the MDM supports the updates of the operating system and whether the profiles and security settings of the baseline configuration still remain efficient and sufficient.
c. If necessary, the baseline configuration of the mobile devices is changed or the security settings are adjusted.
d. Regular checks are carried out to determine whether the rights granted to the users and managers are justified.

3.3 Standard measures

SYS.3.2.2.M6 Logging and monitoring the device status

a. The mobile device management (MDM) system logs all security events and configuration changes during the entire life cycle of a mobile device.
b. The logs of the security events and configuration changes of the mobile devices are centrally accessible.
c. If necessary, the manager can determine the current situation of the mobile devices managed.

SYS.3.2.2.M7 Installation of mobile applications (apps)

a. The apps are managed via MDM. After approving an app for use, the app is published in the internal app catalogue.
b. The mobile device management system launches the installation, uninstallation, and updating of the mobile applications immediately after a connection has been made with the mobile device.
c. Users cannot uninstall the apps installed via MDM.

SYS.3.2.2.M12 Security of MDM

a. The security of the mobile device management is appropriate for the protection requirement of the data handled.
b. The operating system of the administration computer has been hardened and all security updates have been installed in the computer.

SYS.3.2.2.M21 Certificate management

a. Service certificates are installed, updated, and uninstalled in the mobile devices centrally.
b. The MDM system prevents the users from installing unreliable and unverified (root) certificates.
c. The MDM system supports certificate verification mechanisms.

SYS.3.2.2.M22 Decommissioning mobile devices

a. The mobile device management system enables the remote deletion of the data in the mobile device.
b. The process of disposal of the mobile device and deletion from the register thereof ensures that no data which requires protection is left in a mobile device or on an integrated removable data medium.

3.4 Advanced measures

SYS.3.2.2.M14 Assessment of apps by an external reputation service (C-I)

a. If users are permitted to select and install apps on their devices, the external reputation services and the exemptions established by the service are used to make the decisions.
b. The MDM system restricts the installation of apps based on the information received from the reputation service.

SYS.3.2.2.M17 Monitoring the use of mobile devices (I)

a. Monitoring mobile devices enables to detect the jailbreaking of the devices.
b. Personal data protection regulations are observed in the monitoring of mobile devices.

SYS.3.2.2.M19 Use of geofencing (C-I)

a. Geofencing ensures that the devices which contain sensitive data cannot be used outside of a specific geographical area.
b. In the case of leaving the geographical area, the user and the manager are warned and the sensitive

data is deleted after a certain waiting time.
c. Geofencing areas are established by legislation and the requirements of the organisation and based on analysing the protection requirement.

SYS.3.2.2.M23 Enforcement of compliance requirements (C-I)

a. The MDM system identifies attempts to breach the requirements of the organisation or manipulate the operating system and blocks the device automatically.
b. In the event of a suspected violation or manipulation, the MDM system sends a warning to the responsible managers and the information security manager of the organisation.
c. The MDM system is capable of only deleting sensitive data from a device or deleting all data.

SYS.3.2.3 iOS of the organisation

1 Description

1.1 Purpose

To present the measures which must be observed and applied in the case of all smartphones and tablets used for performing work-related duties which are using Apple's iOS or iPadOS operating systems (hereinafter referred to as iOS devices).

1.2 Responsibility

The IT department is responsible for the implementation of the 'iOS of the organisation' measures.

1.3 Limitations

For the implementation of the module, the iOS devices managed must be integrated to the mobile device management infrastructure. The respective measures are described in the module SYS.3.2.2 Mobile device management (MDM).
The general and common measures applicable to working with smartphones and tablets irrespective of the operating system used on the device are described in the module SYS.3.2.1 Smartphones and tablets in general and must also be applied to using iOS devices.

2 Threats

2.1 Jailbreaking of an iOS device

Previous iOS versions contain security vulnerabilities which enable circumventing the security framework established by Apple and accessing system processes and protected memory areas. The user may wish to so to download apps from alternative app stores or add extensions which Apple does not recommend. Attackers use the same method for the installation of malicious programs or for other harmful manipulations in an iOS device.

2.2 Abuse of an Apple ID account

Based on the proof of authorisation of Apple ID, access is granted to all services provided by Apple (e.g. iCloud, iMessage, FaceTime, App Store, iTunes). In the event of unauthorised use of an Apple ID, an attacker can use false identities to access all Apple services. An attacker may also disturb the availability of the Apple ID-based services, monitor the location of the device, reset the factory settings, and access the data in the iCloud. If iCloudBackup is activated in the device, the attacker can clone all files of the user into their own iOS device.

2.3 Extensive rights of pre-installed applications

Along with the iOS, Apple devices include several pre-installed applications which are tightly integrated into the operating system (e.g. Mail and Safari). Those applications are occasionally operated with higher-level rights than the applications downloaded from the App Store. This increases the damage caused in the event of a successful attack against the application.

2.4 Abuse of biometric authentication

The iOS operating system includes the options of biometric authentication by using fingerprint (Touch ID) or facial (Face ID) recognition. Touch ID and Face ID simplify unlocking the device or purchasing from the App Store without further verification. Furthermore, in certain cases, the passcode required for the authentication of the Apple ID can be replaced. Biometric security functions can often be cheated by implementing the creation of an artificial finger by digitally cleaning the fingerprint.

2.5 Abuse of the data displayed on a locked screen

The iOS operating system is equipped with a function which enables viewing activated widgets and push messages even when the screen is locked. This may make the user's confidential information visible to an unauthorised person, which can be taken advantage of. The functions and contact data of the phone can also be accessed even in the locked state via the digital assistant Siri.

2.6 Unauthorised access to externally stored data

The infrastructure operating Apple must be used for several special functions of iOS. When functions such as iCloud Keychain, iMessage, FaceTime, Siri, Continuity, Spotlight Suggestions, push messages, making backup copies into iCloud, or the functions of working with shared documents are used, the data of different devices or users is always synchronised via the central infrastructure of Apple. Thus, there is the risk of the individuals or organisations with access to the data stored in the servers or Apple using the saved data for criminal purposes.

3 Measures

3.1 Life cycle

Planning

SYS.3.2.3.M1 Principles of the implementation of iOS devices

SYS.3.2.3.M2 Implementation plan for cloud services

Implementation

SYS.3.2.3.M7 Security of configuration profiles

SYS.3.2.3.M13 Restriction of iOS services and applications

SYS.3.2.3.M14 Security of using iCloud

SYS.3.2.3.M15 Restriction of the Continuity functions

SYS.3.2.3.M17 Limiting the number of devices related to an Apple ID

SYS.3.2.3.M18 Secure configuration of Safari

Operation

SYS.3.2.3.M10 Biometric authentication

SYS.3.2.3.M12 Anonymisation of Apple ID

SYS.3.2.3.M21 Procedure for adding and approving applications

Additional advanced measures

SYS.3.2.3.M23 Automatic deletion of a configuration profile

SYS.3.2.3.M25 Secure use of the AirPrint service

SYS.3.2.3.M26 Prevention of unlawful connections to the IT systems

3.2 Key measures

SYS.3.2.3.M1 Principles of the implementation of iOS devices

a. The principles for the implementation of iOS devices have been developed and documented and cover the following:

- the criteria for selecting iOS devices;
- the management and configuration of iOS devices;
- use of applications which have not been validated;
- the backup strategy.

b. Devices using iOS are managed and configured via mobile device management (MDM).

c. Jailbreaking an iOS device is organisationally prohibited and technically restricted by MDM.

SYS.3.2.3.M2 Implementation plan for cloud services

a. The possibility and extent of using cloud services is determined before the deployment of iOS devices.

b. Restricting the use of iCloud services is considered in the implementation plan for cloud services.

c. As the iCloud service is also required for registering an Apple ID, then if possible, the Apple Business Manager (formerly Device Enrollment Program, DEP) is used for registering the device.

SYS.3.2.3.M7 Security of configuration profiles

a. Organisational and technical measures have been implemented to prevent the unlawful use of configuration profiles.

b. The users of iOS devices are familiar with the need for and the purpose of the measures.

3.3 Standard measures

SYS.3.2.3.M10 Biometric authentication

a. TouchID and FaceID may be used if the accompanying risks have been taken into consideration and the users have set longer and more complex passcodes to the devices.

b. Guidelines for biometric authentication have been drawn up for the users.
c. The users have been notified that TouchID or FaceID authentication is not fully tamper-proof.

SYS.3.2.3.M12 Anonymisation of Apple ID

a. In the case of the services which require an Apple ID, an anonymous Apple ID string is used instead of an Apple ID which refers to a specific individual.
b. If possible, the Apple Business Manager service is used for the preparation of iOS devices and central installation of applications.

SYS.3.2.3.M13 Restriction of iOS services and applications

a. All unnecessary and prohibited services and applications have been deactivated under the configuration options of the devices (incl. in the 'Screen Time' menu of system settings).
b. Activated services and applications are appropriate for the intended purpose of the device and the protection requirement of the data.

SYS.3.2.3.M14 Security of using iCloud

a. Before using iCloud for performing tasks, it has been assessed whether Apple's terms and conditions of service are compliant with the information security and data protection requirements of the organisation.
b. If the iCloud infrastructure is permitted, multifactor authentication is used for authentication.

SYS.3.2.3.M15 Restriction of the Continuity functions

a. The necessity and compliance with the requirements of the organisation of the Continuity functions (e.g. Handoff, SMS forwarding, Call forwarding) have been assessed.
b. Based on the results of the assessment, the Continuity functions have been restricted technically or organisationally.

SYS.3.2.3.M17 Limiting the number of devices related to an Apple ID

a. The number of unique device codes related to the account is as low as possible in the configuration profile of Apple ID.

SYS.3.2.3.M18 Secure configuration of Safari

a. The configuration of Safari is compliant with the general requirements established for browsers and is subject to the same restrictions that apply to the browsers of the computers.

SYS.3.2.3.M21 Procedure for adding and approving applications

a. For an application to be deployed, the app must pass an internal software approval procedure and App Store validation for mobile applications (apps).
b. All mobile applications approved for use are published in the MDM app catalogue. For the deployment of apps, Apple Business Manager has been integrated with MDM.
c. Biometric methods are not used to authorise any payments related to App Store applications.

3.4 Advanced measures

SYS.3.2.3.M23 Automatic deletion of a configuration profile (C-I)

a. If an iOS device has not been connected to the intranet for a certain period of time, the configuration profile is deleted automatically.

SYS.3.2.3.M25 Secure use of the AirPrint service (C-I)

a. Approved AirPrint printers have been added to the configuration profile.
b. In order to prevent users from using unreliable printers, all connections to the printer are made via the infrastructure of the organisation.

SYS.3.2.3.M26 Prevention of unlawful connections to the IT systems (C-I)

a. iOS devices can only be connected to other IT systems via the mobile device management (MDM) system.

SYS.3.2.4 Android

1 Description

1.1 Purpose

To present the measures which must be observed and applied in the case of all smartphones and tablets used for performing work-related duties which are operating on the basis of the Android operating system.

1.2 Responsibility

The IT department is responsible for the implementation of the Android-specific measures.

1.3 Limitations

The general and common measures applicable to working with smartphones and tablets irrespective of the operating system used in the device are described in the module SYS.3.2.1 Smartphones and tablets in general and must also be applied to using Android devices.
The central management measures of Android devices are described in the module SYS.3.2.2 Mobile device management (MDM).

2 Threats

2.1 Rooting in an Android device

The devices of many manufacturers, especially in the case of older Android versions, contain vulnerabilities which enable to ignore security measures established by the manufacturer and grant root access to certain mobile applications. Rooting is available for anyone with the help of publicly available tools and instructions.

2.2 Malware of Android devices

Due to the wide spread and open architecture, the devices with the Android operating system are a common target for malware. In addition to the Google Play app store, alternative sources can also be used to download apps for an Android device. Installation files can also be copied for local activation directly in the device. This facilitates spreading malware. For example, an attacker may infect a popular paid app with malware and make it available to all for downloading free of charge.

2.3 Outdated operating system

Many manufacturers deliver smartphones or tablets with dated Android versions or devices which do not offer regular operating system updates. Due to the openness of Android, new vulnerabilities are

regularly found in the operating system, making the risk of attacks especially high in the case of Android devices. The problem mainly concerns cheaper models and less known manufacturers. However, owning the best model of a well-known manufacturer also does not guarantee the availability of updates during the entire life cycle of the device. Thus, software vulnerabilities may remain unattended and can be easily exploited by an attacker.

2.4 Abuse of a Google account

After authentication with a Google Account, the user gains access to many services offered by Google (e.g. Google Play, Google Maps, Google Drive, Google Chrome, Gmail, etc.). Many other service providers on the Internet also use Google ID for identifying users. If a Google ID has been leaked, any unauthorised person can abuse this authentication data. An attacker can also track the location of the device, gain access to the data stored on the device, delete the content of the device via remote deletion, or change the passwords of the actual user.

2.5 Extensive rights of pre-installed applications in Android

Many applications tightly integrated with the operating system (e.g. Play Store and the related Play services, Google Chrome) are also pre-installed in the devices with the Android operating system, as well as several apps of unapproved manufacturers which the user cannot remove from the device. This adds to the vulnerabilities of the operating system the vulnerabilities of different applications, making them susceptible to attacks.

3 Measures

3.1 Life cycle

Acquisition

SYS.3.2.4.M1 Procedure for selecting Android devices

Implementation

SYS.3.2.4.M2 Deactivation of the developer's settings

SYS.3.2.4.M3 Restriction of the multiple user mode and guest mode

Operation

SYS.3.2.4.M5 Extended security settings

3.2 Key measures

SYS.3.2.4.M1 Procedure for selecting Android devices

a. Only those devices with the Android operating system are purchased in the case of which the manufacturer regularly issues security updates up to the expected end of the service life of the device.
b. Android devices are delivered with an updated Android version or the version in the device can be updated immediately.

3.3 Standard measures

SYS.3.2.4.M2 Deactivation of the developer's settings

a. Developer options are deactivated under settings in all Android devices.

SYS.3.2.4.M3 Restriction of the multiple user mode and guest mode

a. It has been determined whether or not the multiple user mode or guest mode may be activated in an Android device.
b. The user of an Android device of the organisation must be an unambiguously identifiable person.

SYS.3.2.4.M5 Extended security settings

a. Only approved security applications are granted full access device administrator rights to the devices.
b. Apps are only granted the rights required for the functioning of the app in the device. Only applications with specific rights can access sensitive data.
c. The list of the apps with extended rights is reviewed regularly.

3.4 Advanced measures

There are no advanced measures in this module.

SYS.3.3 Mobile phone

1 Description

1.1 Purpose

To present the measures established for the secure use of mobile phones (incl. feature phones) for telephone communication and sending messages through the mobile connection network.

1.2 Responsibility

The IT department is responsible for compliance with the measures applicable to mobile phones.
Additional responsible persons: User.

1.3 Limitations

The measures are applicable to all mobile phones used to perform work-related duties.
The security measures applicable to smartphones and the operating systems used in smartphones are described in the module group SYS.3.2 Smartphones and tablets. All measures described in the module SYS.3.2.1 Smartphones and tablets in general are applied to smartphones.
The aspects of data communication-based telephone communication are described in the module NET.4.2 IP phone (VoIP) . If the mobile phone in question uses any virtual private network technologies, the module NET.3.3 Virtual private network (VPN) must also be taken into consideration.

2 Threats

2.1 Mistakes in procuring mobile phones

If no requirements have been established for mobile phones and sufficient groundwork has not been done, the mobile phones purchased may lack an important functionality. For example, if the functionality of certain mobile connection standards has not been executed in a specific phone, the phone may not be usable in some countries. The employees who travel between different countries may require a mobile phone with the functionality of multiple SIM cards. The telephone models of all manufacturers may also not be permitted or not be compliant with the requirements of the organisation from the perspective of information security.

2.2 Loss of a mobile phone

Mobile phones are usually light and small and are constantly carried around. Thus, mobile phones may easily be forgotten somewhere, lost, or stolen. Loss of the data stored in the device causes a

greater damage than can be measured by the purchase price of the device. An attacker may use a stolen mobile phone to gain access to the confidential information of the organisation.

2.3 Negligent handling of a mobile phone

A malicious person may take advantage of the inattentiveness or negligence of employees during using a mobile phone to eavesdrop a telephone call or observe writing a message. Important information of the organisation may also leak in this manner. An attacker may use the information collected in this manner to prepare a social engineering attack.

2.4 Personal use of a mobile phone of the organisation

Mistakes may be made due to negligence in using the mobile phones owned by the organisation, in the case of which the work-related matters which require confidentiality are mixed with personal communication. This way, unauthorised persons may gain access to confidential information about the organisation. Personal use of a work phone (e.g. to pay for parking or call paid service numbers) may result in additional expenses for the organisation.

2.5 Failure of a mobile phone

Technical failures of mobile phones may occur for various different reasons. A phone may be dropped if handled carelessly or it may be affected by excessive humidity. Many issues are also related to the battery of the phone, for example, the battery may lose the ability to store energy. The user may also forget their password or PIN and the use of the device may be blocked after multiple attempts to enter an incorrect code. In all of the cases described above, the phone may become unusable, making the user inaccessible and unable to contact others by using the mobile phone.

2.6 Abuse of connection data

Due to the characteristics of mobile connection, it is difficult to prevent the use of special technology to eavesdrop the signals sent. In most cases, the locations of the communication partners communicated via wireless communication can be identified quite accurately. The information collected can be used to draw up a movement profile of the caller.

2.7 Unlawful recording of conversations

Mobile phones can be very successfully used for recording conversations or left in a room and used as an eavesdropping device in an unnoticeable manner. Mobile phones brought to meetings can be used to create connections with eavesdroppers. In the case of many devices, it is not possible to determine visually whether or not the recording function has been switched on.

2.8 Use of outdated mobile phones

The supply of smartphones in the market considerably exceeds the supply of feature phones ('button phones') and the latter have almost been left out of production. Due to the limited supply, many old, already previously decommissioned mobile phones are used.

3 Measures

3.1 Life cycle

Planning

SYS.3.3.M1 Guidelines for the use of mobile phones

Operation

SYS.3.3.M2 Blocking a mobile phone in the event of loss of the device

SYS.3.3.M6 Updating the software of a mobile phone

SYS.3.3.M12 Sufficient inventory of mobile phones

Implementation

SYS.3.3.M3 Training users and raising awareness

SYS.3.3.M5 Using the security mechanisms of mobile phones

SYS.3.3.M8 Deactivation of unnecessary wireless interfaces

SYS.3.3.M10 Secure data exchange

Disposal

SYS.3.3.M4 Procedure for the decommissioning of mobile phones

Acquisition

SYS.3.3.M7 Procedure for acquiring mobile phones

Emergency response

SYS.3.3.M11 Emergency response of a mobile phone

Additional advanced measures

SYS.3.3.M9 Ensuring power supply for mobile phones

SYS.3.3.M13 Prevention of movement tracking

SYS.3.3.M14 Blocking the caller ID

SYS.3.3.M15 Protection against using a mobile phone for eavesdropping

3.2 Key measures

SYS.3.3.M1 Guidelines for the use of mobile phones

a. Guidelines for the use of mobile phones have been drafted and implemented at the organisation.

b. The guidelines for the use of mobile phones specify at least the following:

- the access mechanisms required and implementation thereof;
- permissible services (incl. the services permitted abroad);
- secure use of a mobile phone;
- confidential handling of data;
- personal use of a mobile phone;
- management and maintenance of mobile phones;
- operations in the event of loss or theft of a mobile phone or SIM card.

c. The user of a mobile phone always verifies the actual identity of their communication partner (e.g. by disconnecting an incoming call and calling back to the official number).

d. Mobile phones may only be used during driving if a 'hands-free' device is used.

e. In the case of providing confidential information, the employee makes sure that there are no individuals who could eavesdrop in their immediate vicinity.

f. All users have familiarised themselves with the guidelines for using mobile phones.

g. Compliance with the guidelines for using mobile phones is checked regularly.

h. The invoices for communication services are checked number-by-number to identify potential anomalies or errors.

SYS.3.3.M2 Blocking a mobile phone in the event of loss of the device [user]

a. If a mobile phone is lost, the SIM card of the phone is blocked immediately.

b. If anti-theft remote mechanisms are available, the mobile phone is blocked or the content thereof is deleted immediately.

c. The managers have immediate access to the information required for blocking the SIM card and mobile phone.

SYS.3.3.M3 Training users and raising awareness

a. Secure use of a mobile phone has been included in the information security-related training programme for the employees.
b. The users have been notified of the risks related to mobile phones.
c. The users recognise fraudulent calls and fraudulent messages and know how to respond to them.
d. The users can use the security functionality of mobile phones.
e. The users know how to block their mobile phones and SIM cards after losing a phone.

SYS.3.3.M4 Procedure for the decommissioning of mobile phones

a. Before the decommissioning of a mobile phone, the factory settings are restored (which also deletes the data of the user from the phone) and it is made sure that all data has been deleted from the phone.
b. If the data cannot be deleted from the phone, the device is destroyed physically.
c. Upon the decommissioning of a mobile phone, the memory card in the phone is removed from the phone and erased securely or destroyed (see CON.6 Data erasure and destruction).
d. If it is necessary to store mobile phones before disposal (e.g. until more phones for disposal have been collected), the mobile phones and memory cards collected are protected from unlawful access.

SYS.3.3.M5 Using the security mechanisms of mobile phones [user]

a. The security mechanisms integrated into mobile phones have been configured and deployed.
b. The initial PIN of the SIM card has been replaced by a sufficiently complex PIN.
c. The phone requests the PIN upon activation.
d. The mobile phone is protected by a device password or another security mechanism.
e. Access codes (incl. PUK codes) and service passwords are kept separately from the mobile phone and are only used for the intended purpose.
f. The screen lock of the mobile phone is applied after a few minutes.

SYS.3.3.M6 Updating the software of a mobile phone [user]

a. Regular checks are carried out to find potential security updates for the mobile phone.
b. The organisation has determined whether the updates are installed by the users or centrally.
c. Available mobile phone updates are installed immediately.

3.3 Standard measures

SYS.3.3.M7 Procedure for acquiring mobile phones

a. Technical specifications for the requirements have been drafted before purchasing mobile phones.
b. Phones are selected based on the technical specifications of the requirements.
c. The customer support provided by the supplier and the availability of spare parts (e.g. batteries, charging devices) are taken into consideration in the procurement.

SYS.3.3.M8 Deactivation of unnecessary wireless interfaces [user]

a. If there is no need for them or during breaks in the use, the wireless interfaces (e.g. WLAN or Bluetooth) of mobile phones are deactivated.

SYS.3.3.M10 Secure data exchange [user]

a. Processing data on a mobile phone is regulated by the guidelines for the use of mobile phones (see SYS.3.3.M1 Guidelines for the use of mobile phones).
b. The interfaces which may be used for data exchange and the requirements for the encryption of the data for transportation are established.
c. In the case of exchanging emails via a mobile phone, automatic downloading of email attachments is blocked.

SYS.3.3.M11 Emergency response of a mobile phone [user]

a. The data saved on a mobile phone (e.g. contacts and messages) is regularly backed up to a remote location.
b. Important mobile phone access and configuration data is documented.
c. Before handing over a defective mobile phone for repair works, the SIM card and memory card are removed from the device and, if possible, all data is deleted from the phone and the factory settings are restored.
d. Mobile phones are repaired at a reliable company.
e. There are always replacement phones which can be used in the case of a failure of a mobile phone.
f. The individuals occupying critical positions can also use an alternative communication channel in addition to a mobile phone.

SYS.3.3.M12 Sufficient inventory of mobile phones

a. If the organisation has many mobile phones or the phone users change often, a sufficient inventory of mobile phones is kept.
b. The issuance and return of the mobile phones and accessories is documented.
c. Before issuing for use, mobile phones are equipped with the programs and data required by the new owner.
d. Upon returning mobile phones, the data is deleted from the phone and the factory settings of the phone are restored.
e. The person accepting the mobile phone checks the integrity, condition, and configuration of the devices returned or handed over.

3.4 Advanced measures

SYS.3.3.M9 Ensuring power supply for mobile phones [user] (A)

a. In order to ensure the sufficient power supply of a mobile phone, the battery of the phone is kept at a sufficiently charged level.
b. If a mobile phone needs to be used for a longer period of time, a charger and/or battery bank is brought along.
c. In order to save the battery, extreme temperatures are avoided and unnecessary wireless interfaces are switched off.

SYS.3.3.M13 Prevention of movement tracking [user] (C)

a. A decision has been made on whether the effect of the availability of the employees' location data is so negative that additional measures must be taken to alleviate the effect.
b. No unapproved applications processing GPS data are used in mobile phones.
c. The GPS functionality is deactivated in the mobile phone, unless there is a direct need for using GPS.
d. If the location data of specific employees is confidential, the phones and SIM cards of those employees are often replaced.
e. If an employee's location may not be identifiable temporarily, the mobile phone is switched off with the battery removed.

SYS.3.3.M14 Blocking the caller ID [user] (C)

a. Displaying the caller ID of outgoing calls is deactivated on the phone.
b. No text or MMS messages are sent from a phone which uses a SIM card with a concealed telephone number.
c. The mobile phone number is not disclosed or sent to third parties.

SYS.3.3.M15 Protection against using a mobile phone for eavesdropping (C)

a. It is prohibited to take mobile phones to confidential meetings.
b. The entries to the premises where mobile phones are prohibited are equipped with clear prohibition signs and space has been prepared for the secure storage of the phones.
c. If necessary, the room is scanned with a mobile phone detector.

SYS.4 Other systems

SYS.4.1 Printer and multifunction printer

1 Description

1.1 Purpose

To present the measures applied for the secure use of the printer and multifunction printer.
Modern printers, copiers, and multifunction printers are complex networked devices and are often used to process confidential information.
Please note! Copiers will hereinafter not be referred to separately, but many of the risks and measures covered in this module must also be taken into consideration and implemented in the case of copiers.

1.2 Responsibility

The IT department is responsible for the implementation of measures applicable to printers and multifunction printers.
Additional responsible persons: Information security manager.

1.3 Limitations

The measures described in the module apply to the use of any printers, multifunction printers, and copiers connected to the network of the organisation. Thus, the measures of the module group NET.1 Networks are applied. In order to protect the devices using wireless local area networks (WLAN), further measures from the module NET.2.2 Using wireless local area networks are applied.
Secure disposal of the information saved in printers or office equipment or printed out is described in the module CON.6 Data erasure and destruction.
In the case of a printing server (IT systems which enable the management of the printing queue and printing requests), general (see SYS.1.1 Server in general) and operating system-specific security measures are applied. Regular updating of the software of a printer or a multifunction printer is covered in the module OPS.1.1.3 Patch and change management.

2 Threats

2.1 Leaving printed documents unacceptably unattended

Users often leave printed documents in the output bins of printers or multifunction printers for a long time (e.g. in order to pick up all printed documents together). The user may also accidentally choose the wrong printer which is in a location where the user will not go to pick up their document.

2.2 Visibility of metadata

Along with the print job, the metadata which usually include the username, data, time, and the name of the print job are also sent to the printing server. The metadata is visible in the form of plaintext in the printing server (unless it has been anonymised). In the case of certain devices, this data is displayed on the control panel of the device, as well as in the web server or the printer or multifunction printer. Thus, printing operations can be monitored via a browser.

2.3 Insufficient protection of saved information

Printers and multifunction printers are equipped with non-volatile memory or a hard disk where data is stored temporarily or for long periods of time (e.g. address books or printable documents). If such data is not sufficiently protected, the content of the non-volatile memory can be accessed. If insecure deletion methods are used, an attacker may even be able to restore deleted information in certain cases. Data can be saved in printers via network protocols which is accompanied by the risk of a printer being used as an unapproved file server.

2.4 Unencrypted connection

Printed and scanned data is often sent over the network in an unencrypted format. This allows attackers to eavesdrop the data sent to a printer or read the print files temporarily saved in the printing servers. If devices are managed via unencrypted interfaces (e.g. if the printer is accessed via HTTP, SNMPv2, or Telnet), the access data and passwords or the devices are also at risk.

2.5 Unauthorised transfer of documents

Many networked printers can be configured to accept print jobs from the Internet via email. Scanned documents can also be sent as attachments to emails. This way, documents may intentionally or accidentally end up in the hands of unauthorised recipients. This may happen, for example, if the users enter the address of the recipient incorrectly. Free entry of the address of the sender can be abused by sending emails to internal and external addressees under someone else's name.

2.6 Unauthorised copying and scanning of documents

Multifunction printers enable making high-quality copies of paper documents quickly. USB or SD connections of a multifunction printer also allow direct digitalisation, saving on flash drives or SD cards, and removing numerous paper documents from the premises unnoticeably without any inspection.

2.7 Insufficient network security

The firewalls between a local area network and the Internet are often configured so that the Internet connection is permitted for the entire sub-network. Printers and multifunction printers are often allocated to the same sub-network with workstations. Thus, network printers can be used to access the information on the Internet. If the incoming and outgoing Internet traffic of the printers is not blocked by security gateways, printers can be used to send sensitive data out of the network. The device may also accept data from the Internet and share the data. Thus, a network printer may become the access gate for attacks from the Internet.

2.8 Insufficient security of the management of the devices

Networked printers and multifunction printers can be managed through the control panel and the web server of the device. Standard settings of devices are not initially equipped with passwords or simple

and known default passwords are used. If the device is not equipped with an access password or if the default password is not changed, the device can be accessed very easily. Many organisations use uniform passwords for all printers and multifunction printers which are changed rarely. Thus, those passwords are known to many people in the organisation as well as outside of the organisation, who may use them to gain unlawful access to a device.

3 Measures

3.1 Life cycle

Planning

SYS.4.1.M1	Implementation plan for printers and multifunction printers
SYS.4.1.M4	Security guidelines for printers and multifunction printers

Implementation

SYS.4.1.M2	Restriction of physical access to printers and multifunction printers
SYS.4.1.M5	Guidelines for using printers and multifunction printers
SYS.4.1.M7	Restriction of administration access to printers and multifunction printers
SYS.4.1.M11	Restriction of the network connection of a printer or multifunction printer
SYS.4.1.M17	Security of temporary data and metadata
SYS.4.1.M18	Secure configuration of a printer or multifunction printer

Disposal

SYS.4.1.M22	Procedure for the disposal of printed documents

Operation

SYS.4.1.M15	Encryption of data in a printer or network printer
SYS.4.1.M16	Reducing the downtime of a printer or multifunction printer

Additional advanced measures

SYS.4.1.M14	Additional authentication of the user of a device
SYS.4.1.M20	Additional security of the dataset of a printer or a multifunction printer
SYS.4.1.M21	Expanded security of a printer or multifunction printer

3.2 Key measures

SYS.4.1.M1 Implementation plan for printers and multifunction printers

a. The organisation has drawn up and documented an application plan for printers and multifunction printers which specifies the following:

- the required functions and productivity of the printers and multifunction printers;
- whether the printers and multifunction printers are purchased or rented;
- whether local or networked devices are used;
- who has the user and administrative rights to the printers and multifunction printers;
- which threats the devices must be protected from;
- what the data communication and physical security requirements of the device are;
- what the required data communication protocols and file formats are;
- which measures are used to prevent unauthorised access to documents;
- how the maintenance of printers and multifunction printers and the supply of consumables are organised;
- which measures are used to ensure the availability of the printers and multifunction printers;
- how the training of the users and administrators is organised.

b. Suitable secure locations are planned for printers and multifunction printers.

SYS.4.1.M2 Restriction of physical access to printers and multifunction printers

a. Printers and multifunction printers are placed in locations where using the devices is noticeable for other employees and which are not visited by unattended guests.
b. Printers and multifunction printers are only managed by individuals with administration rights. Written confidentiality agreements are concluded with service providers (e.g. for maintenance and repair works).
c. Configuration of printers and network printers via control panel and web server is password-protected.

SYS.4.1.M5 Guidelines for using printers and multifunction printers [information security manager]

a. The information security manager has drawn up guidelines for the users of printers and multifunction printers on the secure handling of the devices.
b. The guidelines for secure use of printers and multifunction printers include at least the following:

- how to select a printer (e.g. from several networked printers);
- authentication for using the device (if this function is used);
- the obligation to immediately remove or destroy the printed document;

• how to use the memory of the device;
• what to do in the event of technical issues or failures;
• the restrictions applicable to printing and copying sensitive documents.

c. The guidelines for using printers and multifunction printers have been introduced to all users.

d. Most important instructions are provided in the form of a fact sheet displayed next to printers and multifunction printers.

SYS.4.1.M22 Procedure for the disposal of printed documents

a. A procedure has been established for the disposal of unnecessary documents containing sensitive information.

b. There is a shredder or a container for the paper documents to be destroyed in the vicinity of a printer or multifunction printer.

c. Accidentally printed unnecessary documents are destroyed immediately, mistakenly scanned documents are deleted.

3.3 Standard measures

SYS.4.1.M4 Security guidelines for printers and multifunction printers [information security manager]

a. The organisation has drawn up and documented security guidelines for printers and multifunction printers which establish the security principles and terms and conditions for processing data in the devices.

b. The security guidelines for printers and multifunction printers establish the following:
• the requirements for the physical and technical security of a device;
• network-specific security requirements of a networked device;
• organisation of access rights;
• ensuring availability;
• requirements for the administration of devices;
• the use of encryption;
• secure disposal of devices.

SYS.4.1.M7 Restriction of administration access to printers and multifunction printers

a. Only designated managers and maintenance technicians are granted administrative access to printers and multifunction printers.
b. If central device management software is used, only designated managers have access rights to the administration tool.
c. The device can only be accessed after the authentication of the user (e.g. by a password or PIN).
d. Remote access is only possible after the authentication of the user.
e. The connections are encrypted (e.g. with the help of HTTPS or SNMPv3).
f. The use of unencrypted connections is blocked.
g. All printer or multifunction printer ports which are not needed for printing or administration of the printer are blocked, if possible.
h. Remote monitoring of the control panel display of printers and multifunction printers is only permitted to designated managers.
i. Excessive and unnecessary functions of printers and multifunction printers are deactivated.

SYS.4.1.M11 Restriction of the network connection of a printer or multifunction printer

a. Irrespective of the local settings of the device, the connection of a network printer or multifunction printer from the external network is blocked in the central firewall.
b. If a printing server is used, connections can only be made with the printers or multifunction printers from the printing server and from the workstations of the managers which are used to configure and monitor the devices.
c. In order to facilitate administration, network printers and multifunction printers are placed in a separate network segment.
d. The multifunction printers connected to the telephone network are not connected to the local area network or are separated from the local area network by an additional firewall.
e. If the fax and modem functionalities of a multifunction printer are not needed, the nearby phone sockets are disconnected from the telephone exchange or the interface of the telephone exchange of the multifunction printer is removed from the device.

SYS.4.1.M15 Encryption of data in a printer or network printer

a. If the printer or multifunction printer enables the encryption of data, the information in the memory of the device is encrypted.
b. Print jobs are sent to the printer via protocols which enable encryption (TLS/SSL with the IPP

protocol). No printing protocols which do not support encryption (e.g. Unix LPR/LPD and Windows SMB/CIFS) are used.

SYS.4.1.M16 Reducing the downtime of a printer or multifunction printer

a. The downtime periods caused by failures or maintenance of printers and multifunction printers are as short as possible.
b. There are always sufficient inventories of the consumables for printers and multifunction printers.
c. If possible, frequently needed spare parts are stored in a local storage and the spare parts are replaced without calling an external maintenance technician.
d. There is always a replacement device with a similar functionality available for the replacement of critical devices.
e. Sufficiently short response times are ensured by maintenance contracts. If necessary, the spare parts can be ordered from different suppliers.

SYS.4.1.M17 Security of temporary data and metadata

a. Temporary data and metadata (such as the data of print jobs or scanned files) are stored in the devices for the shortest period possible and they are not accessible by unauthorised persons.
b. Temporary data and metadata are deleted automatically after the expiry of the predetermined period.
c. The internal file server of the device and the functions of issuing the list of objects saved into the memory have been deactivated.

SYS.4.1.M18 Secure configuration of a printer or multifunction printer

a. Printers and multifunction printers are only configured by appropriately authorised managers.
b. Unnecessary functions and network interfaces have been deactivated in the configuration.
c. Any pre-set passwords have been changed.
d. Encrypted protocols (HTTPS, SNMPv3) are used in the data communication for management.
e. Insecure protocols which do not use encryption (SNMP, Telnet, PJL) have been blocked.

3.4 Advanced measures

SYS.4.1.M14 Additional authentication of the user of a device (C-I-A)

a. Only individuals with access rights can access printed or copied documents.
b. Only centrally managed printers and multifunction printers are used.
c. The users must authenticate themselves to obtain the document printed from a printer or used a scanner (e.g. with the help of a secure-print solution related to the access card of the user).
d. Authenticated users can only use the functions which they are permitted to use and see their own print jobs.

SYS.4.1.M20 Additional security of the dataset of a printer or a multifunction printer (C)

a. The names of print jobs in the printing server are anonymised.
b. The interfaces of the external storage media of the device are blocked.
c. The access to the internal address book of the device is blocked.
d. In the case of the printers and multifunction printers with an email function, documents can only be emailed to internal email addresses.
e. Incoming fax messages and sending notices are only available to authorised users.

SYS.4.1.M21 Expanded security of a printer or multifunction printer (I-A)

a. The security settings of printers and multifunction printers are checked regularly and adjusted, if necessary.
b. If possible, an automatic checking system is used to check the configuration of the devices.
c. The option to reset the factory settings from the booting menu of the devices is blocked.
d. No firmware or software without the approval of the manufacturer of the specific device is used in printers and multifunction printers.

SYS.4.3 Embedded systems

1 Description

1.1 Purpose

To present the measures for the secure use of embedded systems.
An embedded system is a functional unit with specific hardware and software performing a data processing task assigned to it which is integrated into the composition of a wider IT system or

product. Embedded systems perform tasks related to management, regulation, and data processing (e.g. an airplane computer system, special medical technology, or a data communication centre component). An embedded system can be programmed and largely resembles a universal computer, but the software of the system is stored in EEPROM or ROM. An embedded system does not have an ordinary user interface. Data buses and local ports are the inputs and outputs of an embedded system. Some types of embedded systems also have a web interface for the configuration of the embedded system.

1.2 Responsibility

The IT department is responsible for compliance with the measures applicable to embedded systems.
Additional responsible persons: The procurement department, developer, architect.

1.3 Limitations

The module does not cover the peculiarities of the specific hardware and software architectures used in embedded systems.
The security aspects of the embedded systems used in industrial control systems are described in the IND module group (Industrial IT).
The security aspects of IoT systems are also not included in the scope of this module. Unlike embedded systems, networked IoT systems with smart functions are not integrated into a larger system or product. Due to the wireless connection to data communication networks thereof, various different security measures must be implemented, which are discussed in the module SYS.4.4 Device in the Internet of Things (IoT) in general.

2 Threats

2.1 Insufficient security requirements in the development of embedded systems

In the development of embedded systems, security is often only the third priority after functionality and performance due to financial considerations. If security requirements are disregarded during one or more stages of developing the system, the resulting embedded system may have significant security vulnerabilities.

2.2 Unsecured input and output interfaces of an embedded system

The interfaces of embedded systems are potential targets of attacks. If the control mechanisms of the access to the interfaces are weak, an attacker can connect devices (e.g. miniature control devices) which support the espionage or sabotage to the embedded system, which may remain unnoticed. By connecting a microcontroller to the input or output ports, data can be downloaded directly into the microcontroller or saved on the output signal of the microcontroller. If there is a resetting input, the attacker can temporarily switch off the system.

2.3 Insufficient physical security of an embedded system

If embedded systems are physically easily accessible, an attacker can destroy or damage the system by using mechanical force, short-circuiting, or voltage surges. An attacker may also gain access to the electronic components of an embedded system, such as the outputs or contacts of microcircuits. If an attacker is able to manipulate the data of an embedded system, the integrity and availability of the entire system is at risk.

2.4 Failures or errors of the hardware of an embedded system

Impacts of the surrounding environment (e.g. electromagnetic interferences, fluctuating of the temperature, unstable power supply) may cause failures of embedded systems. System failures may also arise from normal or premature wear and tear of the components. Any failures may cause significant disturbances in the operation of the systems related to the embedded system.

2.5 Manipulation of the software outputs of an embedded system

Many embedded systems store their software in flash memory or EEPROM. The firmware of such embedded systems is updated with the help of a programming tool connected through an interface or network connection. An attacker may also load manipulated software updates and thereby affect the normal functioning of the embedded system.

2.6 Side-channel attacks of integrated cryptosystems

Side-channel attacks can be used to break a cryptosystem or signatures. Side-channel attacks are based on analysing the observable features of the physical and software-based structure of the cryptosystem. For example, it is possible to draw conclusions about the operations completed and the keys based on the energy consumption of the cryptological calculations of the microprocessor and the timing of the signals.

2.7 Manipulation of an embedded system through a communication interface

The energy consumption, dimensions, memory capacity, maximum code size of the software, cost, or other restrictions of the embedded system do not allow developing sufficient security functions (e.g. reinforced cryptography). Modern embedded systems are connected to the network via commonly used technologies and protocols and are thus potentially vulnerable.

2.8 Use of inauthentic components

If analogues are used in the production or maintenance of an embedded system instead of original components, such components may not be as reliable as the original components. This may cause the malfunctioning or failure of the system.

3 Measures

3.1 Life cycle

Planning

SYS.4.3.M1	Procedure for the implementation of embedded systems
SYS.4.3.M5	Protection of an embedded system from harmful environmental impacts
SYS.4.3.M7	Secure execution of the functions of an embedded system in hardware

Implementation

SYS.4.3.M2	Deactivation of unnecessary interfaces and services of an embedded system
SYS.4.3.M6	Security of the program code of an embedded system
SYS.4.3.M8	Secure operating system of an embedded system

Operation

SYS.4.3.M3	Logging the security events of an embedded system

Acquisition

SYS.4.3.M4	Technical specifications of the requirements for an embedded system

Emergency response

SYS.4.3.M10	Recovery of an embedded system

Disposal

SYS.4.3.M11	Secure disposal of an embedded system

Additional advanced measures

SYS.4.3.M9	Use of cryptoprocessors and coprocessors
SYS.4.3.M12	Reliable delivery and logistics chain of an embedded system
SYS.4.3.M13	Certified operating system
SYS.4.3.M14	Security and authentication of the booting of an embedded system
SYS.4.3.M15	Security of the memory management of an embedded system
SYS.4.3.M16	Prevention of tampering attacks against an embedded system
SYS.4.3.M17	Self-testing of the embedded system modules
SYS.4.3.M18	Prevention of side-channel attacks against an embedded system

3.2 Key measures

SYS.4.3.M1 Procedure for the implementation of embedded systems

a. The following have been established to ensure the implementation and smooth management of embedded systems:

- requirements for the compatibility, working environment, and infrastructure (see SYS.4.3.M4 Technical specifications of the requirements for an embedded system);
- roles, responsible persons, rights, and obligations;
- reporting channels and contact persons for failures and security incidents.

b. All embedded systems and interfaces of embedded systems are documented.

c. A procedure for testing the integrity and functioning of embedded systems has been established.

d. Embedded systems are securely preconfigured. The used configurations are documented.

e. Guidelines for action in the case of suspected failures, malfunctions, or security incidents as well as reporting channels are explained to all users and managers.

SYS.4.3.M2 Deactivation of unnecessary interfaces and services of an embedded system [developer]

a. Users only have access to the physical and logical interfaces which they require.

b. Only those services and protocols which are necessary for serving a purpose have been activated.

c. Port scanners and other appropriate network security applications are used to identify vulnerabilities related to the interfaces of an embedded system. Useless and insecure protocols and services (NetBios, Telnet, http, ftp) are deactivated.

d. The access of an application using an embedded system to the interfaces of the embedded system is protected by secure authentication.

SYS.4.3.M3 Logging the security events of an embedded system

a. The following security events are logged, depending on the possibilities of the specific embedded system:

- attempts of unauthorised access;
- attempts of unlawful access:
- system failures;
- privileged operations;
- attempts to acquire privileges.

b. If it is not possible to log electronically or it is only possible to a very limited extent, the following is documented in a manual log book:
c. all works performed in the embedded system, including the place, time, executing party, type of the operation, and description of the cause;
d. all failures, obvious violations, and other deviations.

SYS.4.3.M5 Protection of an embedded system from harmful environmental impacts [developer, architect]

a. Depending on the manner and location of using an embedded system, the components of the embedded system are protected from dust, heat, humidity, and other harmful environmental impacts.
b. The required safeguard measures are taken into consideration while planning the infrastructure for the embedded system.
c. The internal safeguard measures of an embedded system depend on the location of the system (e.g. if it is included in the composition of a larger system, it may not be necessary to protect the embedded system by using a closed and unbreakable housing).

3.3 Standard measures

SYS.4.3.M4 Technical specifications of the requirements for an embedded system [procurement department]

a. Technical specifications of the requirements have been drawn up for procuring an embedded system which are used for assessing the systems or components.
b. The technical specifications of the requirements include at least the following security requirements:

• the organisational framework conditions (notification, customer support, updates, trainings, etc.);
• the technical and economic requirements (functions, real time requirements, energy consumption, expenses, etc.);
• compliance with the industry standards and practice (certificates);
• physical protection from environmental threats and attacks;
• requirements for the hardware (architecture of the processor, type of the firmware memory);
• the requirements for the software (administration of rights, logging, alarms, etc.);
• TPM module (Trusted Platform Module) support;
• the development tools and security mechanisms thereof.

SYS.4.3.M6 Security of the program code of an embedded system [developer]

a. The debugging function of the embedded system has been deactivated or fully removed from the system.
b. The use of a debugger via remote connection has been blocked.
c. The input interfaces of the test signals, the measurement points, and the debugging interfaces of the chips are protected from unauthorised use.

SYS.4.3.M7 Secure execution of the functions of an embedded system in hardware [developer, architect, procurement department]

a. In the case of an embedded system created on the basis of universal, programmable processors, additional security measures have been implemented for protection against undesired functions and the installation of backdoors.
b. If an embedded system is developed on site, the development and operating environment thereof is protected from unauthorised access.
c. The components and development tools originate from reliable sources and have been tested.

SYS.4.3.M8 Secure operating system of an embedded system [developer, architect]

a. The operating system used in the embedded system and the configuration thereof are appropriate for the intended purpose.
b. Only the services, functions, and interfaces which match the intended purpose of the embedded system are activated in the operating system.
c. The operating system supports the use of the TMP module.

SYS.4.3.M10 Recovery of an embedded system

a. When loading a new software version, the previous version can be restored.
b. Changes in the configuration can be cancelled and the initial state of the system can be restored.
c. The last functional state of the system is always backed up.

SYS.4.3.M11 Secure disposal of an embedded system

a. Before the disposal of an embedded system, all data is securely deleted from the system.
b. If data stored in an embedded system cannot be deleted, the hardware of the embedded system is destroyed physically.
c. The deletion of the data and the destruction of the hardware are documented.

3.4 Advanced measures

SYS.4.3.M9 Use of cryptoprocessors and coprocessors [developer, architect] (C-I)

a. If an additional microcontroller is used for cryptographic operations, further measures have been implemented for the data exchange between this microcontroller and the microcontroller of the system.
b. A chain of trust has been implemented in the embedded system and the required trust anchors have been created.

SYS.4.3.M12 Reliable delivery and logistics chain of an embedded system [procurement department] (C-I-A)

a. The qualifications and reliability of the manufacturer of the embedded system and the companies included in the delivery and logistics chain can be proved.
b. The manufacturer of the system has made sure that the embedded system does not include any manipulated, counterfeit, or replaced components.
c. The embedded systems are protected from the manipulation of the programmable logic modules and the replacement of components during storage, reselling, and transportation.
d. The supplier of the system has checked the compliance of the embedded systems with the technical specifications.
e. The embedded systems do not contain any concealed functions. It is not possible to gain unlawful access to confidential information via an embedded system.

SYS.4.3.M13 Certified operating system [developer, architect] (C-I-A)

a. The operating system of the embedded system has been assessed to meet an appropriate level based on an acknowledged standard (e.g. ISO 15408).

SYS.4.3.M14 Security and authentication of the booting of an embedded system [developer, architect] (C-I)

a. The booting is carried out in several stages with the security of each stage checked.
b. Upon booting an embedded system, a boot loader checks the integrity of the operating system and only loads the operating system if the system is complete. The operating system is only activated if the operating system has confirmed the reliability of the boot loader.
c. In the event of an ARM-based embedded system, the ARM Secure Boot security tool is used or the operating system is activated from write-once memory.
d. In the case of the UEFI (Unified Extensible Firmware Interface) of the x86 platform, the Secure Boot security tool is used.

SYS.4.3.M15 Security of the memory management of an embedded system [developer, architect] (C-I)

a. The main memory of the embedded system has been structured so that an error of one program does not affect the stability of other programs or the entire system.
b. Hardware is used to restrict the data access of the programs to the memory areas of other programs - a MPU (Memory Protection Unit) or a MMU (Memory Management Unit).
c. If there is no hardware-based security, software is used to check requests from the memory. The inspection may take place after compilation or during the operation the software in the form of automatic checks.

SYS.4.3.M16 Prevention of tampering attacks against an embedded system (C-I)

a. Appropriate means are used for the detection and registration of tampering attacks and for tamper response.
b. Secure housings are used for the physical protection of an embedded system and the embedded system is tightly fixed to a metal structure.
c. Sealing of the devices, security stickers, or active sensors which respond to the changes in the

environment are used to detect tampering.
d. Guidelines have been drawn up for responding to tampering incidents.

SYS.4.3.M17 Self-testing of the embedded system modules (I-A)

a. The embedded system modules include a built-in self-test function.
b. Self-testing is used to check the integrity of the module during switching on, as well as during operation at certain intervals.
c. If the required technical capability is available, the security functions of the module are also tested.
d. In the case of a module with a higher protection requirement (e.g. vital control systems), the built-in self-test also involves checking the integrity of the input and output components and the memory.

SYS.4.3.M18 Prevention of side-channel attacks against an embedded system (C)

a. The following may be used for protection against side-channel attacks against an embedded system, for example:
- randomised masking of interim outcomes and/or queue times;
- ensuring a uniform power consumption profile during encryption and decryption;
- concealing the power consumption in background noise (e.g. with the help of artificial power consumers);
- additional memory elements, the content of which is not changed in the course of normal operation.

SYS.4.4 Device in the Internet of Things (IoT) in general

1 Description

1.1 Purpose

To present the measures applied for the secure use of devices in the Internet of Things (IoT devices). IoT devices are networked objects or devices with smart functions. IoT devices are mostly connected to a wireless local area network, the devices have access to the date on the Internet and are accessible from the Internet themselves (e.g. surveillance cameras, remote-controlled heating equipment).

1.2 Responsibility

The IT department is responsible for implementation of the measures of the module 'Device in the Internet of Things (IoT) in general'.
Additional responsible persons: Procurement department, technology department, information security manager.

1.3 Limitations

The module does not cover the peculiarities of the hardware and software architectures of different IoT devices.
The security aspects of the industrial control system devices are described in the IND module group (Industrial IT).
This module also does not cover embedded systems. Unlike IoT devices, embedded systems with smart functions are integrated into a wider system or product. The security of embedded systems is described in the module SYS.4.3 Embedded systems.
The measures applicable to wireless data communication applicable to IoT devices are specified in the module group NET.2 Wireless networks.
The measures for the management of the access rights to IoT devices are described in the module ORP.4 Administration of identity and rights.

2 Threats

2.1 Spying through an IoT device

The information security aspect is usually not focused on sufficiently in the course of developing IoT devices. Consequently, IoT devices have been repeatedly abused to collect information about the users or the scope (e.g. there have been repeated incidents involving IP-based networked surveillance cameras).

2.2 Use of automatic tuning (UPnP)

IoT devices integrated in local area networks often create an internet connection via UPnP (Universal Plug and Play) to be visible and available outside of the local area network with the help of port forwarding. The channel created can be used to deliver other malware into the network or for other malicious activities. By taking advantage of the vulnerability of an IoT device, an attacker can make the IoT device part of a botnet.

2.3 Distributed denial-of-service attack (DDoS)

If regular security updates are not installed in IoT devices, an attacker can exploit the known vulnerability of an IoT device to include the device in a botnet. After that, the attacker can organise distributed denial-of-service attacks (DDoS attacks) by exploiting the device with the aim of disturbing the availability of the services of the targeted organisation.

2.4 Espionage through a backdoor of an IoT device

It has been determined that some video camera and room sensor models are equipped with backdoors which allow access to the camera images and videos, as well as copying the images to a server in the internet.

3 Measures

3.1 Life cycle

Acquisition

SYS.4.4.M1	Determining the security requirements of IoT devices
SYS.4.4.M8	Criteria for the acquisition of IoT devices

Implementation

SYS.4.4.M2	Authentication of an IoT device
SYS.4.4.M5	Restriction of the network access of an IoT device
SYS.4.4.M9	Procedure for using an IoT device
SYS.4.4.M10	Secure installation and configuration of an IoT device
SYS.4.4.M11	Encryption of data exchange
SYS.4.4.M13	Deactivation and uninstallation of the useless components of an IoT device
SYS.4.4.M15	Restriction of the access rights of an IoT device

Planning

SYS.4.4.M6	Involving IoT devices in the security policy of the organisation
SYS.4.4.M7	Implementation plan of IoT devices

Operation

SYS.4.4.M16	Anti-malware
SYS.4.4.M17	Monitoring the data exchange of an IoT device

SYS.4.4.M18 Logging the security events of an IoT device

SYS.4.4.M19 Security of the administrative interface of an IoT device

Disposal

SYS.4.4.M20 Proper decommissioning of an IoT device

Additional advanced measures

SYS.4.4.M21 Working environment and power supply

SYS.4.4.M22 Monitoring the Internet of Things

SYS.4.4.M23 Auditing IoT devices

SYS.4.4.M24 Secure configuration and use of the online server of an IoT device

3.2 Key measures

SYS.4.4.M1 Determining the security requirements of IoT devices

a. The minimum required security requirements have been drawn up for IoT devices which all IoT devices used in the organisation must comply with.

b. All IoT devices must at least ensure the following:

- the firmware and software of the device can be updated;
- the manufacturer ensures regular software updates of the device during the reasonable service life of the device;
- the device enables authentication;
- the default passwords of the device can be changed;
- the device does not have any concealed functions.

SYS.4.4.M2 Authentication of an IoT device

a. Authentication is always activated in an IoT device.

b. The passwords used for authentication are compliant with the password policy of the company and do not overlap with any password used in other IT systems. If possible from the technical perspective, more secure authentication mechanisms are used (e.g. certificate-based authentication).

c. The default passwords of an IoT device have been changed before connection of the device to the intranet of the organisation.

SYS.4.4.M5 Restriction of the network access of an IoT device

a. The access of IoT devices to the intranet is as restricted as possible. If IoT devices (e.g. security cameras) are included in a system of a wider purpose (e.g. the building management system), they only exchange data with this system.
b. The incoming and outgoing network connections and destinations are restricted by access-count lists (ACL) and firewall rules (e.g. a connection with the manufacturer's update server, the site of recording the video data, and the management system are sufficient for a surveillance camera).
c. Access via Telnet (port 23) is blocked.
d. Routing is restrictive, default routes are blocked.
e. The UPnP automatic tuning function has been deactivated in all routers.
f. IoT devices and the sensors are located in a separate network segment which is only connected to the administration network segment.
g. Remote access to an IoT device is only possible via SSH (default port 22) and secure authentication.
h. IoT devices are protected from unauthorised physical access.

3.3 Standard measures

SYS.4.4.M6 Involving IoT devices in the security policy of the organisation [information security manager]

a. The general security policy of the organisation includes requirements for IoT devices. The security as well as functionality aspects have been taken into consideration in the security requirements for IoT devices.
b. All individuals who purchase and operate IoT devices are familiar with the security policy requirements.
c. Compliance with the policy requirements is inspected regularly. The results of the inspection are documented.

SYS.4.4.M7 Implementation plan of IoT devices

a. The implementation plan of the IoT devices includes at least the following:
- the purpose and services of the Internet of Things;
- the places and manners of use;
- the need for and the type of authentication;
- management of the devices;

• network connections and network services;
• logging;
• security mechanisms.

b. All decisions made in the planning stage are documented.

SYS.4.4.M8 Criteria for the acquisition of IoT devices [procurement department, information security manager]

a. The information security manager is involved in the procurement of IoT devices.
b. The procurement is based on the implementation plan of IoT devices (see SYS.4.4.M7 Implementation plan of IoT devices).
c. Before purchasing any IoT devices, the security requirements which the devices must be compliant with are defined and used to assess the products available in the market. The products are compared based on the following criteria, among other things:

• physical protection from environmental threats and attacks;
• fault tolerance and reliability;
• compliance with the standards and practices of the field;
• the architecture of the system;
• the software and the security mechanisms thereof (communication protocols, administration of rights, logging, alarms, etc.).

SYS.4.4.M9 Procedure for using an IoT device

a. A main user has been appointed for each IoT device who is closely familiar with the specifics of the device.
b. The environmental conditions and power supply required for the deployment of the device have been ensured.
c. The IoT device has been configured based on the work-related needs and security requirements.

SYS.4.4.M10 Secure installation and configuration of an IoT device

a. IoT devices are only installed and configured by authorised persons (persons responsible for IoT devices, managers or contractual service providers) who must follow the established procedures.
b. All stages of the installation and configuration are documented so that a competent third party would be able to conduct the procedure based on the documentation.

c. At least the following changes are made in the initial configuration:

- the default passwords are changed;
- user and manager rights are allocated;
- access to the extranet and to important external services is configured;
- sending data to the manufacturer or supplier is blocked.

d. The initial configuration of the IoT device is appropriate for the intended use and compliant with the security policy requirements.
e. If possible, IoT devices are only connected to the data communication network after installation and configuration have been completed.

SYS.4.4.M11 Encryption of data exchange

a. IoT devices exchange data by SSL/TLS or SSH in an encrypted form.
b. Insecure network protocols (e.g. Telnet) have been deactivated.
c. If a product does not support encryption, VPN is used for data exchange.

SYS.4.4.M13 Deactivation and uninstallation of the useless components of an IoT device

a. After installation of an IoT device, a check is conducted to determine which protocols, applications, and services have been installed and activated in the device.
b. Useless protocols, services, user accounts, and interfaces (e.g. Bluetooth, Zigbee, Firewire) are deactivated or uninstalled.
c. If useless network services cannot be deactivated directly in the device, a firewall is used to block the services.
d. The actual statuses of the available services are checked by scanning the ports.

SYS.4.4.M15 Restriction of the access rights of an IoT device

a. IoT devices only have user rights in the minimum extent required for operating.
b. If the access rights cannot be restricted sufficiently in the IoT devices, the access rights are restricted at the local area network level.

SYS.4.4.M16 Anti-malware

a. The IT department is familiar with the measures for alleviating the malware threats and risks of IoT devices.

b. Any malware is eliminated immediately.
c. If the malware can only be located in the main memory, it is removed by booting the device (which does not, however, prevent the reinfection of the device).
d. If the cause of the infection cannot be eliminated or reinfection cannot be ruled out, the infected device is disposed of.

SYS.4.4.M17 Monitoring the data exchange of an IoT device

a. Regular checks are conducted to identify which IT systems IoT devices exchange data with, which protocol the IoT devices used for the connection attempts, and whether the connections were permitted or blocked.
b. If necessary, logging and statistical analysis of the network traffic are used to collect data.

SYS.4.4.M18 Logging the security events of an IoT device

a. Security events are logged automatically. If it is not possible to log via IoT devices, the logging mechanisms of routers or other IT systems are used.
b. The following security events are logged, depending on the technical possibilities:
- attempts of unauthorised access;
- attempts of unlawful access:
- system failures;
- privileged operations;
- attempts to acquire privileges.

c. If it is not possible to log electronically or it is only possible to a very limited extent, the following is documented in a manual log book:
- all works performed with the IoT devices with the place, time, executing party, type of the operation, and description of the cause;
- all failures, obvious access and data access violations, and other deviations.

d. Only designated persons can access the logs of an IoT device.
e. Incident-based as well as regular analyses of the logs are carried out.

SYS.4.4.M19 Security of the administrative interface of an IoT device

a. The administrative measures approved by the security policy are observed in the management of IoT devices.

b. Remote access interfaces can only be accessed from the designated IT system or network segment.
c. Local administrative interfaces are preferably used for the management of IoT devices.

SYS.4.4.M20 Proper decommissioning of an IoT device

a. There is an overview of which data is being retained in each IoT device.
b. Before the decommissioning of an IoT device, the data in the device is backed up and any sensitive data is deleted.
c. In order to dispose of IoT devices, a checklist is drawn up which includes at least the aspects required for backing up and securely deleting the data; among other things, the data saved in a cloud or on a removable data medium is taken into consideration.
d. The rights, links, and references related to the device disposed of are removed as needed.

3.4 Advanced measures

SYS.4.4.M21 Working environment and power supply [technology department] (I)

a. Before the installation of an IoT device, compliance of the location with the following requirements is checked:
- the environmental conditions required by the manufacturer (appropriate temperature, humidity, power supply parameters);
- the requirements for information security (e.g. the protection requirements of the related systems and the data protection requirements).

b. IoT devices are protected from theft, destruction, and manipulation. If necessary, additional security mechanisms are applied (e.g. reinforced housing of the device).
c. If the device is equipped with an internal power source, the functioning thereof is checked regularly. If necessary, the battery is charged or replaced.

SYS.4.4.M22 Monitoring the Internet of Things (A)

a. Constant monitoring of IoT devices has been implemented. If the thresholds established are exceeded, the managers of the device are notified immediately.
b. If more stringent requirements have been set for the availability of IoT devices, there is always a preset backup device or a cluster of devices has been created in the case of which the failure of one device does not put to risk the availability of the entire system.

SYS.4.4.M23 Auditing IoT devices (C-I-A)

a. In the areas which are critical from the security perspective, all IoT devices used have been subjected to a safety technology audit and testing before the installation of the devices.

SYS.4.4.M24 Secure configuration and use of the online server of an IoT device (C-I-A)

a. The configuration of the online server in an IoT device is as restricting as possible.
b. Only the required components and functions have been installed and activated.
c. The rights of the account used for managing the online server are as restricted as possible.
d. The online server is not activated by using a privileged account.
e. The server can only be accessed via stringent authentication.
f. Data exchange is encrypted.
g. All messages which are related to security or failures (successful and unsuccessful data accesses, failure messages, faulty or incomplete HTTP requests, and system messages) are logged.

SYS.4.5 Removable data media

1 Description

1.1 Purpose

To present the measures for the secure use of removable data media.
Removable data media are used for transporting or storing data or for granting mobile access to the data. Removable media include, among others, external hard disks, CDs, DVDs, memory cards, magnetic tapes, and flash drives.

1.2 Responsibility

The IT department is responsible for compliance with the measures applicable to removable media.
Additional responsible persons: The user, the responsible specialist.

1.3 Limitations

The module does not cover the protection of the IT system which the removable data media are connected to. The respective measures are described in the modules SYS.1.1 Server in general, SYS.2.1 Client computer in general, and in the operating system-specific modules.
The measures applicable to the mobile devices which, unlike removable data media, are capable of processing data (such as smartphones) are described in the module SYS.3.2.1 Smartphones and tablets in general. The organisation of secure data exchange with the help of removable data media is described in the module CON.9 Exchange of information.

2 Threats

2.1 Negligence in the handling of information

Any mistakes in the use of a removable data medium made due to negligence may physically damage the removable data medium. If no backup copies have been made of the data, the data may not be recoverable.

2.2 Insufficient knowledge of the rules

If no guidelines for the secure use of removable data media have been drafted for the employees, the employees cannot be required to observe those requirements. If the employee is not aware of the threats related to removable data media, they may cause a security incident due to their lack of knowledge or negligence (e.g. if a flash drive which has not been scanned is connected to the IT systems of the organisation).

2.3 Theft or loss of removable data media

Using removable data media comes with a higher risk of data loss than using stationary systems. The threat level is especially high in the case a theft or loss of a data medium. In this case, the information archived on the removable data medium is lost permanently. The data stored on a stolen or lost data medium may also end up in the hands of unauthorised individuals.

2.4 Defective media

Due to their compact form and the technologies used, removable data media are susceptible to damage, errors, and failures which may be caused by mechanical impacts during transportation or by using the removable data media.

2.5 Damage due to a changing operating environment

Removable data media are also used in harmful environmental conditions (e.g. excessively high or too low temperature, dust, or humidity) which may damage the data media. Connection of the media to an unknown IT system is also accompanied by the risk of the removable data medium being damaged by a defective reader (e.g. CD reader).

2.6 Spreading of malware

If a removable data medium is used with different devices and in different workstations, there is a risk of the data medium spreading malware from one IT system to another. Malware may also damage or delete the data on the data medium.

3 Measures

3.1 Life cycle

Implementation

SYS.4.5.M1	Raising employees' awareness
SYS.4.5.M6	Management procedure for removable data media

Operation

SYS.4.5.M2	Reporting a loss or a manipulation of a removable data medium
SYS.4.5.M12	Scanning removable data media for malware
SYS.4.5.M7	Secure deletion of a data medium before and after use
SYS.4.5.M13	Labelling removable media during the transportation of the media
SYS.4.5.M17	Long-term storage of data on removable media

Planning

SYS.4.5.M4	Guidelines for the use of removable data media
SYS.4.5.M5	The procedure for the removal of removable data media

Additional advanced measures

SYS.4.5.M10	Encryption of a data medium
SYS.4.5.M11	Protection of integrity with a verification code or digital signature
SYS.4.5.M14	Secure transportation and packaging
SYS.4.5.M15	Certified removable data media

SYS.4.5.M16 Specialised data gateways

3.2 Key measures

SYS.4.5.M1 Raising employees' awareness

a. The employees have been informed of the types and purposes of removable data media.
b. The employees know which data may be saved on a removable data medium.
c. The employees have been trained to handle removable data media in a manner which prevents the loss or theft thereof to ensure a long service life of the data media.
d. It is prohibited to connect removable data media from unknown sources to the IT systems.
e. The employees know how to securely dispose of removable data media.

SYS.4.5.M2 Reporting a loss or a manipulation of a removable data medium [user]

a. The organisation has defined clear reporting channels and contact persons for reporting incidents related to removable data media.
b. A user must immediately notify the contact person of a loss, theft, or suspected manipulation attempt involving a removable data medium.
c. In the incident report, the user must specify which information was stored on the removable data medium.
d. If a data medium is found or restored after being lost, it is checked for possible data manipulation and malware.

SYS.4.5.M12 Scanning removable data media for malware [user]

a. Before saving data on a removable data medium, the data medium is scanned for malware.
b. Before handling the data on a removable data medium, the data medium is scanned for malware.

3.3 Standard measures

SYS.4.5.M4 Guidelines for the use of removable data media

a. The organisation has drafted guidelines for the use of removable data media.
b. As a minimum, the guidelines for the use of removable data media must specify the following:
- which removable data media may be used;
- which data may not be saved on removable data media;

• how to protect data from unauthorised access, manipulation, or loss;
• how to encrypt data on a removable data medium;
• how to securely store removable data media;
• whether removable data media may be connected to the IT systems of third parties;
• how to delete data from removable data media;
• whether or not and how to use personal data media;
• external employees and service providers with whom it is permitted to exchange data media and the terms and conditions of such exchange;
• how to transport data media;
• how to prevent spreading malware through removable data media.

c. Only authorised users may access removable data media.

d. The relevance of security requirements applicable to the use of removable data media and their compliance with the requirements are checked regularly.

SYS.4.5.M5 The procedure for the removal of removable data media

a. A procedure has been established for removing removable data media which specifies the following:
• whether and when it is permitted to remove removable data media from the territory of the organisation and which media may be removed;
• who and how may remove removable data media;
• which security measures (primarily data encryption) must be implemented.

SYS.4.5.M6 Management procedure for removable data media [responsible specialist]

a. Uniform rules have been established for the management of removable data media.

b. The removable data media used in the organisation:
• are labelled in a uniform manner which does not reveal excessive information to unauthorised persons;
• are registered in the list of inventory of the organisation;
• are backed up and archived;
• do not contain excessive data.

SYS.4.5.M7 Secure deletion of a data medium before and after use [responsible specialist]

a. After passing on, reusing, or disposal of rewritable data media, the data on the data media is properly deleted.
b. Guidelines have been drawn up for the secure deletion of the data. The employees have access to the tools which enable to ensure secure deletion.
c. In the case of a higher protection requirement, the data medium may only be used once.

SYS.4.5.M13 Labelling removable media during the transportation of the media [user]

a. A dispatched data medium and its packaging are labelled in a manner which is comprehensible for the recipient and the sender.
b. The labelling of a data medium which contains delicate information does not allow unauthorised persons to draw any conclusions about the content of the data.

SYS.4.5.M17 Long-term storage of data on removable media

a. Suitable removable media are used for the long-term storage of data.
b. The readability of data on removable media is regularly tested to verify that the data is available and has maintained its integrity.

3.4 Advanced measures

SYS.4.5.M10 Encryption of a data medium (C-I)

a. The data on a removable data medium is fully encrypted (see CON.1 Cryptography concept).
b. The procedure of encryption is secure and the tools of encryption are sufficiently protected.

SYS.4.5.M11 Protection of integrity with a verification code or digital signature (I)

a. In order to ensure the integrity of confidential information, the integrity of the data on a removable data medium is protected with CRC codes or a sufficiently secure digital signature.

SYS.4.5.M14 Secure transportation and packaging (C-I-A)

a. The method of transport used is sufficiently secure and appropriate for the protection requirement.
b. Secure transport packaging which allows for the immediate detection of any manipulation is used for transporting data media.
c. The employees know which packaging and transport method must be used for sending data media.

SYS.4.5.M15 Certified removable data media (C-I-A)

a. Only certified removable data media are used in the organisation.
b. Certification takes into account the long-term and full preservation of data and the possibility of encryption.

SYS.4.5.M16 Specialised data gateways (C-I)

a. The organisation uses a specialised data gateway system which reads the data from one data medium, scans the data for malware, and writes the data on another data medium.

SYS.EE Estonian IT systems

SYS.EE.1 X-tee security server

1 Description

1.1 Purpose

Presenting measures for the protection of the X-tee security server. The owner of the X-tee security server is an organisation or a responsible structural unit which enables information systems to use the security server for communication via X-tee.
The IT systems interfaced with the X-tee security server may not endanger the infrastructure of X-tee or become vulnerable due to being interfaced with X-tee. Proper application of the X-tee security server ensures the probative value of data exchange and the reliability of the business processes related to X-tee.

1.2 Responsibility

The IT department is responsible for the implementation of the measures of the X-tee security server.
Additional responsible persons: The responsible specialist, the management of the organisation.

1.3 Limitations

The measures for the user of the service of the X-tee security server are described in the module APP.EE.1 X-tee data service.

The agreements on the use of the security server and on the data service are based on modules CON.9 Exchange of information and OPS.3.1 Information security of the service provider.
The general administration measures of the server and the Linux operation system are described in the modules SYS.1.1 Server in general and SYS.1.3 Linux and Unix server.

2 Threats

2.1 Misuse of the data of the security server

The security server is used to mediate and store the data of service providers as well as the consumers of the services. Any misuse, leak, or unauthorised modification of the data would affect the parties to the data service and the owners of the data (incl. private individuals).

2.2 Misuse of the e-seal

The security server generates an e-seal to ensure the probative value of data. The owner of the security server has their own e-seals and the e-seals of other organisations at their disposal for the provision of the service.

2.3 Administrative errors of the security server

The owner of the security server is responsible for the appropriateness of the accesses to the data service. Any errors in the administration of the security server may lead to unauthorised access to data or prevent the access of authorised users to the data service without a reason.

2.4 Availability error of the security server

The functioning of the data services and the business processes (incl. external business processes) depending on it rely on the availability of the security server. An availability error of the security server may result in sanctions arising from the violation of regulations or contracts and cause reputational damage to the organisation.

2.5 Errors in the interfacing of the security server with the data service

The errors made in the interfacing of the security server and a data service may lead to data leaks and unauthorised access to the data services.

3 Measures

3.1 Life cycle

Planning

SYS.EE.1.M1 Planning the installation of the security server

SYS.EE.1.M2 Selecting the cryptographic module of the security server

Implementation

SYS.EE.1.M3 X-tee subscription contract with the X-tee centre

SYS.EE.1.M4 Contracts for trust services

Operation

SYS.EE.1.M5 Management of the certificates of the security server

SYS.EE.1.M6 Using the X-tee trust anchor in the security server

SYS.EE.1.M7 Secure use of the timestamping service

SYS.EE.1.M8 Secure interfacing of X-tee data services

SYS.EE.1.M9 Testing the security server and data service

SYS.EE.1.M10 Secure archiving of the message log of the X-tee security server

SYS.EE.1.M11 Secure operation of the security modules of the security server

SYS.EE.1.M12 Network security of the security server

SYS.EE.1.M13 Updating the software of the security server

SYS.EE.1.M14 Synchronising the time of the security server

SYS.EE.1.M16 Single-purpose use of the security server

SYS.EE.1.M17 Using the administration API of the security server

SYS.EE.1.M18 Logging and monitoring the security server

SYS.EE.1.M21 Administration of the security server as the owner of the security server

Emergency response

SYS.EE.1.M15 Back-up and recovery of the configurations of the security server

SYS.EE.1.M22 Security server recovery plan

Disposal

SYS.EE.1.M19 Decommissioning of the security server

SYS.EE.1.M20 Secure termination/amendment of the use of the security server

Additional advanced measures

SYS.EE.1.M23 Using personalised accounts and roles in the administration of the security server

SYS.EE.1.M24 Expanded monitoring of data exchange
SYS.EE.1.M25 Restriction of external network connections
SYS.EE.1.M26 High availability of the security server
SYS.EE.1.M27 Using qualified e-seals

3.2 Key measures

SYS.EE.1.M1 Planning the installation of the security server

a. The capability and the features of the network connection of the security server are derived from the requirements for the availability and capacity of the data services mediated.
b. Archiving the message log of the security server is planned based on the purposes of the data services.
c. Monitoring and processing the operational logs of the security server is planned based on the rules of the organisation (see OPS.1.15 Logging) and the purposes of the security server service.
d. The resources required for the operation of the security server (network, security modules, databases, message log archival service) are aligned with the purposes of the security server service.

SYS.EE.1.M2 Selecting the cryptographic module of the security server

a. The hardware security module (HSM) used for signing keys is based on the requirements for the security guarantees of the data services mediated (see APP.EE.M1 Planning the use or provision of an X-tee data service).
b. When selecting a security module, the following is taken into account:
- the requirements for generating a qualified e-seal and for the secure storage of a private key;
- the criteria established for the HSM and the security certificates thereof by the certification authority of signing keys;
- the capacity and manner of interfacing of the network device planned;
- the capacity, availability, and substitutability of the security module in an emergency situation are aligned with the purposes of the security server service.

c. The activation tools or passwords of the encryption module are aligned with the security purposes and the acknowledged good practice.

SYS.EE.1.M3 X-tee subscription contract with the X-tee centre [management of the organisation]

a. An X-tee subscription contract has been concluded with the X-tee centre.
b. Authorised administrative and technical contact persons are registered in the self-service environment of the X-tee centre. In the event of any changes in the authorised persons, the contact details are updated immediately.
c. The email address for receiving notices is redirected to a separate address/mailing group with more than one recipient.

SYS.EE.1.M4 Contracts for trust services [management of the organisation]

a. The organisation has concluded contracts for trust services.
b. There is a procedure for reviewing the contracts. The contracts are updated, if necessary.
c. The administrative and technical authorised contact persons of the organisation are registered by the provider of trust services (timestamping service, certification centre, OCSP). In the event of any changes in the authorised persons, the contact details are updated immediately.
d. The email address for receiving notices is redirected to a separate address/mailing group with more than one recipient.

SYS.EE.1.M5 Management of the certificates of the security server

a. The expiry dates of the signing and authentication certificates of the security server are monitored and the certificates are renewed in a timely manner.
b. New private keys are generated upon renewing the certificates. Repeated or multiple use of a private key is prohibited.
c. If a certificate is no longer in use, an application for cancellation of the certificate must immediately be submitted to the trust service provider.

SYS.EE.1.M6 Using the X-tee trust anchor in the security server

a. A trust anchor is downloaded from the source specified by the X-tee centre.
b. Upon downloading the trust anchor, the integrity thereof is checked by verifying the e-signature.
c. Upon uploading to the security server, the hash displayed in the user interface of the security server is compared to the hash published by the X-tee centre.
d. Regular checks are conducted to make sure that the trust anchor is up to date (the latest trust anchor published by the X-tee centre or the hash thereof is compared to the trust anchor applied in the security server).

e. If the X-tee centre notifies the owners of the security server of the need to update, a new trust anchor is applied within the prescribed period of time.

SYS.EE.1.M7 Secure use of the timestamping service

a. The timestamping services of the security server are configured based on the agreements for trust services and are aligned with the security targets of the data service (availability, the level of the timestamping service (qualified vs. unqualified)).
b. If possible, more than one timestamping service is used in the security server.
c. If the X-tee centre notifies the owners of the security server of the need to update the details of the timestamping service, a new configuration is applied within the prescribed period of time.
d. Any timestamping services with expired agreements for use are immediately removed from the configuration.

SYS.EE.1.M8 Secure interfacing of X-tee data services

a. There is a mutually authenticated TLS connection between the security server and the data service, the TLS certificates of the security server and information system of which are verified.
b. In the event of using protocols which have not been authenticated and/or encrypted, further security measures which ensure confidentiality and integrity are applied.
c. The data service can only be used through the authorised security server.

SYS.EE.1.M9 Testing the security server and data service

a. The development and testing operations of the security server and data exchange interface are conducted in the development or testing environment.
b. It is not permitted to use the data or services of the production environment (operational environment) in the development and testing environments.
c. The security measures of the security server and data services of the development and testing environments prevent the abuse of those environments and attacks against those environments.

SYS.EE.1.M10 Secure archiving of the message log of the X-tee security server

a. The message log is archived and stored securely. The retention periods of the message logs arise from the legislation and the goals set by the owners of data.
b. Message logs are only retained in the security server for as long as absolutely necessary.

c. Access to the message log (in the security server as well as in the archive) is restricted based on the targets of the owners of the data.

SYS.EE.1.M11 Secure operation of the security modules of the security server

a. The means required for activating the encryption module (token, PIN, etc.) can only be accessed by authorised individuals.
b. The encryption module can be activated outside of the working hours and in emergency situations.
c. The means required for activating the encryption module and the security features thereof (incl. the complexity of the PIN) are aligned with the protection requirement.
d. The access of an encryption module used through the network is protected by a firewall with only the source addresses required for fulfilling the task permitted.
e. If it is identified that the encryption module or key has been compromised or if the key is removed from use, the trust service provider is notified immediately for the cancellation of the respective certificates.

SYS.EE.1.M12 Network security of the security server

a. The security server is separated from the public network and user networks by a firewall, with incoming traffic from the Internet only permitted for the X-tee transport protocol (by default: TCP 5500 and 5577).
b. The administration interfaces of the security server (by default: TCP 4000 [webui] and 22[ssh]) can only be accessed from authorised networks.
c. Service interfaces of the security server (by default: TCP 443, 8443, 80, 8080) can only be accessed by the consumers of the security server service based on individual or network addresses. Any changes in the access lists of those addresses (incl. removal of the addresses which are not in use) are made immediately.

SYS.EE.1.M13 Updating the software of the security server

a. If any repair or updated versions of the X-Road software of the security server are issued, the software of the security server is updated within the period prescribed by the X-tee centre.
b. The repository approved by the X-tee centre is used to obtain updates.
c. Regular checks are conducted to make sure that the addresses and authentication keys of the repository are up to date.

d. Updates of the operation system are installed based on the module OPS.1.1.3 Patch and change management.

SYS.EE.1.M14 Synchronising the time of the security server

a. The computer clock of the security server is synchronised with trusted NTP servers (see NET.1.2.M8. Synchronisation of time).

SYS.EE.1.M15 Back-up and recovery of the configurations of the security server

a. The configurations of the security server are backed up regularly.
b. The interval of making back-up copies and the retention periods of the copies are compliant with the terms and conditions of the security server service.
c. Only authorised individuals can access the back-up copies.
d. In the event of recovering a back-up copy, it is made sure that the configuration deployed from back-up is aligned with the actual need and does not include outdated or missing elements (e.g. definitions of the consumers, access lists, configurations of services).

SYS.EE.1.M16 Single-purpose use of the security server

a. Only the programmes and services required for the functioning of the security server are launched in the security server.

SYS.EE.1.M17 Using the administration API of the security server

a. The management of the application programming interface (API) keys of the administration of the security server is compliant with the requirements of the organisation.
b. The roles established for the API keys are based on the principle of minimality.
c. In the system issuing API calls, the association of the operation with the actual identifier of the user is ensured.
d. Any API keys with questionable confidentiality or which are no longer required are immediately removed from use.

SYS.EE.1.M18 Logging and monitoring the security server

a. The logs of the security server are processed and retained based on the policies of the organisation.
b. The functioning of the operation system of the security server, the use of resources, and the metadata of exchanging messages are monitored based on the goals of the organisation.

SYS.EE.1.M19 Decommissioning of the security server

a. Before decommissioning the security server, the consumers of the security server are notified thereof.
b. An application is filed for the cancellation of the respective configuration elements of the X-tee copy (security server certificates, addresses, any subsystems which will no longer be used, etc.).
c. Retention of all message logs (incl. those which have not yet been archived) or the delivery of the logs to the respective consumers of the security server is ensured.
d. The retention of the operating logs of the security server is ensured.
e. The certificates of the security server and of the consumers of the security server are cancelled.
f. Encryption keys are destroyed based on the nature of the encryption module and the instructions of the producer.

SYS.EE.1.M20 Secure termination/amendment of the use of the security server

a. Any configuration elements related to the consumers of the security server to be decommissioned (description of the service, access lists, TLS keys, X-tee subsystems, etc.) are removed from use.
b. Upon ceasing to use the security server, the retention of the message logs based on the needs of the consumer of the security server is ensured.

3.3 Standard measures

SYS.EE.1.M21 Administration of the security server as the owner of the security server [responsible specialist]

a. Standard terms and conditions for the security server service have been established, which include at least the following:

- the capability to generate qualified e-seals (access to a proper HSM and using appropriate trust services);
- the accuracy (frequency) of timestamping and the permitted delay (the maximum period for which messages may remain without a time stamp;
- the service level goals, incl. from the perspective of availability;

• the standard terms and conditions for storing, archiving, retaining, accessing, and destroying an X-tee security server message log;

• the procedure for receiving and processing service requests.

b. Service requests and any changes in the configurations which concern the consumer of the service are documented.

c. Responding to the service requests of the consumers of the service is ensured based on the standard terms and conditions of the service and/or the agreement concluded with the consumer.

d. Consumers of the service are notified of the following in a timely manner:

• the need for updating the signing certificates of the organisation;

• changes in the technical parameters.

e. Upon expiry of a service agreement, a confidentiality failure of an encryption key or keys, or unauthorised use, the following steps are taken immediately:

• the use of the respective key is prevented (e.g. by deactivation, removal from the system);

• the respective trust service provider is notified for the cancellation of the certificate;

• consumers of the service are notified of the circumstances concerning them and any action taken.

SYS.EE.1.M22 Security server recovery plan

a. The emergency and administrative contacts of the X-tee centre and trust services and the required means of authentication are quickly available in an emergency situation.

b. Replacement of encryption modules is ensured by back-up devices, maintenance agreements, and respective emergency instructions.

c. There is a documented security server recovery plan. Functioning of the recovery plan is tested regularly.

3.4 Advanced measures

SYS.EE.1.M23 Using personalised accounts and roles in the administration of the security server (C-I)

a. Personalised accounts are used in the security server management.

b. Roles are allocated to the personalised accounts based on the principle of minimum rights.

SYS.EE.1.M24 Expanded monitoring of data exchange (I)

a. In order to identify potential deviances, the metadata and the patterns of use of data exchange are monitored.

SYS.EE.1.M25 Restriction of external network connections (C-A)

a. Incoming traffic to the X-tee transport protocol (by default, TCP 5500 and TCP 5577) is only opened for the addresses of authorised security servers. Such authorised security servers may include all client security servers registered in the respective X-tee copy or specified in a separate agreement.

SYS.EE.1.M26 High availability of the security server (A)

a. In order to make sure that the security server service is failsafe and/or to distribute the load, several copies of the security server are operated.
b. Technical and procedural measures are used to ensure that the subsystems, services, and access lists of the different copies are synchronised.

SYS.EE.1.M27 Using qualified e-seals (C-I)

a. All signing keys are generated and are only kept in an encryption module compliant with the requirements for a qualified key device for the purposes of the eIDAS regulation.
b. The signing certificates are obtained from a qualified trust service provider.
c. A qualified timestamping service is used for timestamping.

SYS.EE.2 eID components

1 Description

1.1 Purpose

To present measures for the implementation of eID (i.e. ID cards, Mobile-ID, Smart-ID, etc., and related services) in organisations.
Correct handling of eID service components and client components ensures the trustworthiness of the evidential value of data and the reliability of related business processes.

1.2 Responsibility

The IT department is responsible for the compliance with the security measures applicable to eID components.
Additional responsible persons: The management of the organisation.

1.3 Limitations

Exchange of information between organisations relies on the module CON.9 Exchange of information.
In addition, measures from the module OPS.1.1.6 Software testing and onboarding are applied to software using eID components.

2 Threats

2.1 Improper use of eID components

Improper use of eID tools or neglecting to validate transaction details threatens the reliability of business processes and may lead to remarkable economic losses. The reputation of the organisation is also damaged.

2.2 Implementation errors of eID tools

Ignoring the measures may lead to violations of privacy, integrity, and confidentiality. Neglecting to implement the measures may put the operational continuity of the processes of an organisation at risk.

2.3 Management errors concerning eID components

Errors made in the management of eID components (such as failing to update the components) may cause leaks of personal data, unauthorised access to data, or prevent the access of authorised users to data services without any reason.

3 Measures

3.1 Life cycle

Planning

SYS.EE.2.M1 General plans for the utilisation of eID tools

SYS.EE.2.M2	Planning authentication based on eID
SYS.EE.2.M3	Planning e-signatures and e-seals
SYS.EE.2.M4	Planning the validation of e-signatures or e-seals
SYS.EE.2.M5	Planning software interfaces, modules, and configurations of eID

Implementation

SYS.EE.2.M6	Service agreements for eID services

Operation

SYS.EE.2.M7	Secure use of e-seal and decryption tools
SYS.EE.2.M8	Secure interfacing of an ID card with a (web) application
SYS.EE.2.M9	Secure interfacing of an eID interface (Smart-ID, Mobile-ID), a service (SiVa, SiGa, etc.) or an intermediate (TaRa, etc.)
SYS.EE.2.M10	Installing and updating eID client software
SYS.EE.2.M11	Data preparation for creating e-signatures or e-seals or for encryption
SYS.EE.2.M12	Secure reception of data bearing an e-signature/e-seal
SYS.EE.2.M13	Secure reception of encrypted data in CDOC format
SYS.EE.2.M14	eID user training
SYS.EE.2.M15	Regular review of trust anchors and configurations
SYS.EE.2.M16	Restamping e-signatures/e-seals
SYS.EE.2.M17	Security of an ID card reader

Emergency response

SYS.EE.2.M18	Emergency response for eID

Additional advanced measures

SYS.EE.2.M19	Self-hosted service in older (DDOC, BDOC, etc.) and other formats (PDF, X-tee, etc.) for the validation of e-signatures/e-seals
SYS.EE.2.M20	Use of phishing-resistant authentication tools

3.2 Key measures

SYS.EE.2.M1 General plans for the utilisation of eID tools

a. The need for using eID in business processes has been identified and the following has been decided:

- presumable volumes and patterns of utilisation;
- the need to differentiate between subjects based on a characteristic (citizen, e-resident, EU

resident, etc.) or the used eID tool (ID-card, Digi-ID, etc.).

b. When support for other European (compliant with the eIDAS requirements) and eID tools is needed in addition to Estonian national eID tools, then the minimum required level of security guarantees for the supported eID tools is determined:

- when authenticating (High, Substantial, or Low);
- when creating or validating e-signatures/e-seals (Qualified, Advanced, or Other).

c. The levels of eID tools nationally recognised in Estonia are High and Qualified, respectively.

d. The fact that the eID tools (mainly the ones supported by eIDAS) submit subject identifiers differently and that one subject may have several identifiers has been taken into account.

e. When selecting eID tools, the following criteria have been taken into account:

- costs for the organisation and user;
- how common the tool is among the target group;
- accessibility and experience of the target group;
- the need to use additional devices;
- reliability;
- complexity of interfacing with the information system and the modularity/replaceability of the interface;
- replaceability of the tool and/or the possibility to use an alternative tool in the case of an emergency.

SYS.EE.2.M2 Planning authentication based on eID

a. The organisation has decided the minimum level of the authentication tool (High, Substantial, Low).

b. The allowed level of authentication in the IT system is High when the IT system:

- processes special categories of personal data or enables access to special categories of personal data;
- grants access to personalised benefits;
- could be used for causing extensive economic damage.

c. The validity of an eID tool is verified based on validity information and in the case of certificates with OCSP (Online Certificate Status Protocol).

d. The validity information of an eID tool (including a buffered reply from OCSP) is no older than 1 hour.

e. The results of the authentication operations along with appropriate proof are logged pursuant to the objectives of the organisation and of the business process.

SYS.EE.2.M3 Planning e-signatures and e-seals

a. The following has been determined based on the requirements of the business process:
- acceptable levels of an e-signature/e-seal (qualified, advanced, other);
- formats of the issued e-signature/e-seal;
- suitable eID tools for creating e-signatures/e-seals.

b. Suitable e-seal tool is used for adding e-seals on behalf of the organisation.
c. The employees have appropriate eID tools and their instructions are up to date.
d. The technical limitations of validity confirmation (OCSP) and time-stamping services and the costs associated with using them have been taken into consideration in the e-signature/e-seal work flows (including the number of queries and authentication requirements).
e. When planning to use external e-signature/e-seal services, the permissibility to send signed data/documents to third parties (such as creating an e-signature for a service provider) and the relevant terms and conditions of the service have been taken into consideration.

SYS.EE.2.M4 Planning the validation of e-signatures or e-seals

a. When using external validation systems, the permissibility of sending data to be validated to a third party (provider of the validation service) and the terms and conditions of the service have been taken into account.
b. Based on the requirements of a business process, the logging and storage requirements have been decided for the validation process.

SYS.EE.2.M5 Planning software interfaces, modules, and configurations of eID

a. The software interface, module, and configuration of eID can be upgraded and replaced.
b. Procedures for replacement, configuration, and upgrades have been documented and can be reproduced.
c. Well-known and supported standards are preferred for interfacing protocols.
d. It is possible to set up trust configuration, including:
- a whitelist of certificates of permitted certification authorities (CA) that have issued a certificate or source of a Trust Service List (TSL) and the configuration of authenticity (certificate);

• configurations of the sources of validity (including OCSP, CRL) and their authenticity (including service certificates);

• settings for the update period of validity and limitations on the duration of validity;

• settings for utilised time-stamping services and their authenticity;

• if necessary: whitelists of certificate issuance policies permitted in a subject certificate and the permitted key usage of the private keys of a subject.

SYS.EE.2.M6 Service agreements for eID services [management of the organisation]

a. The organisation has concluded the necessary service agreements for using eID components.
b. Administrative contact persons and contact persons with technical authorisations are registered by the service provider.
c. Contact details are updated immediately in the case of any changes.
d. The email address for receiving notices is redirected to an address/group with more than one recipient.

SYS.EE.2.M7 Secure use of e-seal and decryption tools

a. Cryptographic tools and the level of security of certificates used for e-seals and decryption correspond to the requirements of the business process.
b. The requirements of the issuer of a certificate to security and certification have been met.
c. A procedure has been established for storing, accessing, and utilising e-seal and decryption tools and physical security modules necessary for their activation.
d. The applied security measures exclude unauthorised use, copying, or destruction of e-seal and decryption tools.

SYS.EE.2.M8 Secure interfacing of an ID card with a (web) application

a. A client certificate is verified with cryptographic means. The client certificate is checked to make sure that it is issued directly by a CA in the whitelist (i.e. intermediate certificates are not used).
b. The validity of a client certificate is checked by using OCSP queries for verifying validity.
c. If necessary, creating a session is limited with the help of the issuance policy and key usage controls presented in the client certificate.
d. Authentication accesses and their responses along with corresponding proof are logged based on the objectives of the organisation and its business process.

e. The duration of the validity of an authenticated session is restricted. When a session expires, authentication is repeated.

SYS.EE.2.M9 Secure interfacing of an eID interface (Smart-ID, Mobile-ID), a service (SiVa, SiGa, etc.) or an intermediate (TaRa, etc.)

a. The interfacing of an eID interface (Smart-ID, Mobile-ID), a service (SiVa, SiGa, etc,) or an intermediate service (TaRa, etc.) complies with technical guidelines.
b. Secure TLS protocol is used for data communication between the endpoints of services and the eID interface. The certificates of the respective endpoints have been pinned.
c. Information contained in a service request (including the one displayed to the user) is clear for the user, can be linked to the eID operation at hand, and takes into consideration user privacy and data confidentiality requirements.
d. Responses to service requests are validated in the manner indicated in the technical specifications of the interfaces. The information in the response (including the subject certificate) is authentic, complete, and up to date as well as compliant with the requirements of the IT system/business process.
e. If necessary, creating a session is limited with the help of the issuance policy and key usage controls presented in the client certificate.
f. Service requests and their responses along with the respective proof are logged based on the objectives of the organisation and business processes.
g. The duration of the validity of an authenticated session is restricted. When a session expires, authentication is repeated.

SYS.EE.2.M10 Installing and updating eID client software

a. The client software and the data of eID solutions are acquired from approved sources.
b. The authenticity of the software is verified through the verification of a digital signature.
c. An updated version of client software is tested in the required combinations with operating systems and applications before commissioning it.
d. A software update is installed for all eID users and services during the period determined by the Information System Authority or recommended by the respective software supplier.

SYS.EE.2.M11 Data preparation for creating e-signatures or e-seals or for encryption

a. File formats are used that do not support the implementation of active content (JavaScript, macros, etc.) and the dynamic inclusion of objects external to documents.
b. If necessary, the metadata of the document is added to the e-signature container (date/time of preparation, roles of signatories, etc.).
c. The data/documents are made safe (active components are removed, they are checked for malware, etc.) before adding an e-signature/e-seal.
d. Document management processes are followed where document is signed before sending it to other (external) parties (to prevent a situation where the other party would alter the document before adding their e-signature).

SYS.EE.2.M12 Secure reception of data bearing an e-signature/e-seal

a. Employees carrying out validation are equipped with suitable tools and up-to-date instructions.
b. The file format of the data container bearing an e-signature/e-seal is checked to make sure that it is suitable.
c. The e-signatures/e-seals of received data are validated with the help of a software or a service.
d. The results of the validation are logged and stored based on the objectives of the organisation and its business process.
e. Before using the data or storing it in the IT systems, the data is checked to make sure that it is safe (malware, active components, etc.).
f. The data container with an e-signature/e-seal is stored pursuant to the objectives of the organisation and its business process.

SYS.EE.2.M13 Secure reception of encrypted data in CDOC format

a. The need to receive encrypted document containers in CDOC format (including when DigiDoc software is used for decryption) in a business process has been identified.
b. The organisation has decided on the manner of sending to the encryptor the personal identification code of a person, the commercial registry code of the organisation to whose name a document container is encrypted, or an authentication certificate needed for encryption.
c. The received data is decrypted at the first opportunity and the decrypted data is stored in compliance with data protection requirements.
d. Before using the decrypted data, the safety of the data (malware, active components) is verified.

3.3 Standard measures

SYS.EE.2.M14 eID user training

a. Users are trained in the secure use of eID tools in the following aspects:

- recognising manipulation attempts and the procedure for informing of suspicion of manipulation;
- choosing, changing, and secure storage of PINs;
- security of mobile devices related to the eID;
- guidelines for instances of theft or destruction of an eID tool;
- validity of eID tools and certificates (including the impact on the decryption of encrypted containers) and timely updates of tools;
- checking the existence of eID tools and their good working order regularly (including Mobile-ID and Smart-ID, which may exist in several devices simultaneously);
- secure decommissioning of eID tools (including Mobile-ID and Smart-ID, which may exist in several devices simultaneously);
- procedure established in the organisation for adding e-signatures and e-seals, the validation of e-signatures and e-seals, and the decryption of encrypted containers;
- removing a smart card from smart card readers after completing an operation or at the end of a session;
- based on the professional responsibilities of the employee: different formats and levels of e-signatures as well as tools for identifying the levels.

SYS.EE.2.M15 Regular review of trust anchors and configurations

a. The lists of trust anchors used in eID interfaces (CA certificates, issuance policies of certificates, etc.) are checked regularly and updated in a timely manner.
b. Expired, revoked, or unused trust anchors are removed from configurations.
c. Trust anchors that are going to be commissioned are added to configurations.
d. Endpoint certificates are updated in a timely manner.
e. The settings of services meant for utilising eID components have been updated based on the requirements of the service provider.

SYS.EE.2.M16 Restamping e-signatures/e-seals

a. Additional timestamp or an e-signature in an up-to-date format has been added to e-signatures and e-seals that have expired and that require evidential value in the future. Restamping proves that the original signature container existed before adding another timestamp/e-signature.

SYS.EE.2.M17 Security of an ID card reader

a. A smart card reader is connected to a computer directly (connecting a reader through USB hubs and docks is avoided).
b. A workstation that is in public use, is shared by several users, or has a higher protection requirement, utilises certified smart card readers with PIN keypads.
c. The smart card is removed from the reader after completing the necessary activity and when leaving the computer.

SYS.EE.2.M18 Emergency response for eID

a. More than one eID tool is supported or the organisation is prepared to switch to using an alternative tool.
b. Configurations and guidelines are prepared for instances of failures in the validity confirmation service of certificates (OCSP) used in IT systems to continue working based on certificate revocation lists (CRL).
c. Timestamps are duplicated or the organisation is prepared to switch to an alternative service.
d. Alternative tools, alternative services, and the correctness of their guidelines are checked regularly.

3.4 Advanced measures

SYS.EE.2.M19 Self-hosted service in older (DDOC, BDOC, etc.) and other formats (PDF, X-tee, etc.) for the validation of e-signatures/e-seals (C)

a. To prevent sensitive documents from being forwarded to external parties, a suitable self-hosted validation service (SiVa, etc.) is used.
b. The service addresses of the validation service are replaced with the self-hosted service information for all users in the user and server applications (DigiDoc, etc.) conducting validation.
c. Appropriate measures prevent access to a public validation service (such as firewall rules).
d. Trust service lists and validation software are updated in a timely manner.
e. The DigiDoc mobile application of the Information System Authority or other external validation services are not used for the validation of e-signatures/e-seals.

SYS.EE.2.M20 Use of phishing-resistant authentication tools (C-I)

a. Critical IT systems use phishing-resistant tools as means of authentication, which may be an ID card with a mutually authenticated TLS connection or a certified physical token with WebAuthn protocol.

APP: APPLICATIONS

APP.1 Client applications

APP.1.1 Office software

1 Description

1.1 Purpose

To present measures for the protection of data that is processed in office software and for secure office software management. Office software includes applications for the compiling, processing, and data analysis of documents.

1.2 Responsibility

The IT department is responsible for complying with the security measures for office software.
Additional responsible persons: User.

1.3 Limitations

When selecting and implementing office software, the measures of APP.6 Software in general are also implemented.
The measures for the email application are presented in the module APP.5.3 Email server and client in general.
In case of a cloud-based office software, the measures presented in the module OPS.2.2 Using cloud services are followed.
When using database systems integrated into office software (such as LibreOffice Base and Microsoft Access), the measures of the module APP.4.3 Database systems are implemented as well.

2 Threats

2.1 Disregard for the needs of the organisation

When acquiring or adapting office software without considering business requirements, it might cause loss of performance, malfunctions, and errors in the business processes. The reasons could include incompatibility with the existing document formats and documents, deficient functionality of the new office software, or the lack of interoperability with the applications of business partners.

2.2 Document manipulation

The active content of automating documents (e.g. macros or ActiveX components) could contain malicious code which is activated when the document is opened. The malicious code could also spread to other documents after manipulating the specific document and thereby disturb the business processes of the organisation. Failing to identify manipulation is a significant security vulnerability.

2.3 Loss of integrity of the document

Usually, changes in the data of office software are not logged. Therefore, when a user makes a mistake or someone takes advantage of a product weakness, the contents of the document could be changed intentionally or unintentionally. When the altered documents are not identified and they continue to be a part of the work processes, there is a risk of making erroneous business decisions or damaging the reputation of the organisation.

2.4 Insufficient verifiability of the document

When the person who prepared, reviewed, or approved a document cannot be proved verifiably or a function of an office software can be manipulated, the authenticity of a document can become doubtful. This could lead to a cancellation of a contract, for example.

3 Measures

3.1 Life cycle

Planning

APP.1.1.M2	Limiting active content
APP.1.1.M10	Regulating the development of add-ons for office software by users
APP.1.1.M11	Proper implementation of add-ons for office software

Operation

APP.1.1.M3 Secure manner of opening documents from external sources

APP.1.1.M17 Training on the implementation of security functions of office software

APP.1.1.M12 Withdrawing from cloud storage

APP.1.1.M13 Utilising view functions

APP.1.1.M14 Protecting data against retroactive modification

Implementation

APP.1.1.M6 Testing new versions of office software

Additional advanced measures

APP.1.1.M15 Encryption and digital signatures

APP.1.1.M16 Checking the integrity of documents

3.2 Key measures

APP.1.1.M2 Limiting active content

a. The autorun of active content has been deactivated in the office software.
b. When the active content is necessary for work operations, it is installed from an authorised source.

APP.1.1.M3 Secure manner of opening documents from external sources [user]

a. Each document from an external source is checked for malware before the document is opened (see also OPS.1.1.4 Protection against malware).
b. The organisation has prohibited unnecessary file formats that have been classified as problematic.

APP.1.1.M17 Training on the implementation of security functions of office software

a. The users are aware of threats related to active content and of the possibilities of limiting active content.
b. The users are aware of dangers of using documents from external sources.
c. The users have completed training on the safe use of office software and in the implementation of security functions (incl. encryption functions).
d. The users are aware of which file formats should be used when saving documents to protect them from retroactive changes and possible manipulation.

3.3 Standard measures

APP.1.1.M6 Testing new versions of office software

a. Before approving office software for use, the compatibility of the software with the information technology environment of the organisation (e.g. document templates, forms, document macros in use) is first tested based on a previously prepared test plan.
b. The office software is first piloted to ascertain that the product functions in the operational environment and with real data. The results of the pilot are documented.
c. If the new versions of the office software are not compatible with the older documents, an action plan is created for finding a suitable solution (e.g. for the conversion of documents).

APP.1.1.M10 Regulating the development of add-ons for office software by users

a. A written decision stipulates whether user-developed add-ons for the office software (such as macros and linked spreadsheets) are allowed in the organisation.
b. If the organisation allows developing add-ons based on office software, suitable security measures are applied (see also APP.1.1.M2 Limiting active content).
c. The organisation has established a procedure for developing add-ons of office software, which stipulates the requirements for documentation and testing, competences of the responsible employees, and the procedures for the implementation of the outcome.
d. The development of add-ons created by the user are documented and the documentation is made available to the rest of the employees.

APP.1.1.M11 Proper implementation of add-ons for office software

a. Add-ons and plugins of office software are tested and their implementation is approved in a similar manner to testing new versions (see also APP.1.1.M6 Testing new versions of office software). Testing add-ons and plugins provides certainty about the lack of side effects in the office software and the IT systems in use.
b. The add-ons and plugins of office software are tested in a testing system which is isolated from other IT systems.

APP.1.1.M12 Withdrawing from cloud storage [user]

a. The cloud storage functionality of the office software and the storage room provided by the cloud have been blocked.
b. Documents are stored in a single, centrally managed environment.

c. In order to share documents with persons outside the organisation, special applications or data exchange rooms with suitable security and privilege management functions (such as encrypted data storage and transmission) are used.

APP.1.1.M13 Utilising view functions [user]

a. Documents from potentially insecure sources (from the internet or an email attachment, for example) are opened in an automatically restricted mode where data cannot be processed directly.
b. When only reading privileges have been granted for documents, the special applications for document examination that are installed in the computer are used for opening the documents.

APP.1.1.M14 Protecting data against retroactive modification [user]

a. Depending on the planned purpose of using the document, the security mechanisms in the office software are used for limiting further processing of the file that has been created.
b. Documents that are sent out of the organisation are protected with a digital signature. All authorities of the European Union must accept an eIDAS qualified digital signature that can be given in Estonia with an ID-card, mobile-ID, or Smart-ID certificates.

3.4 Advanced measures

APP.1.1.M15 Encryption and digital signatures (C-I)

a. Data with a higher protection requirement is encrypted before the data is transmitted or stored.
b. Before the implementation of cryptographic mechanisms that are integrated in the office software, it has been verified whether the cryptographic mechanism guarantees sufficient protection (mostly, in case of older product versions) and complies with the requirements of the organisation (see also CON.1 Cryptography concept).
c. The IT systems of the sender and the recipient have restricted access to cryptographic mechanisms.
d. Documents and document macros are signed digitally to guarantee authenticity and integrity.

APP.1.1.M16 Checking the integrity of documents (I)

a. When sending a document to which integrity requirements apply, it is protected with a checksum (such as CRC or SHA hash) or a digital signature (see also APP.1.1.M5 Encryption and digital

signatures).
b. In order to correct unintentional changes, the automatic recovery functions that are integrated into office software are used.

APP.1.2 Web browser

1 Description

1.1 Purpose

To present security measures for the protection of the web browsers in client devices (including desktop computers and laptops, tablets, and smart phones). The section covers both centrally managed and independent work environments.

1.2 Responsibility

The IT department is responsible for the compliance with the web browser measures.
Additional responsible persons: User.

1.3 Limitations

This module does not discuss browsers if they are used only for access to local data networks without an internet connection.
As the web browser is closely connected with the operational systems of the client device and uses its interfaces and functions, additional measures from the modules SYS.2 Desktop computers and SYS.3.2.1 Smartphones and tablets in general are implemented.
Web browsers and servers that are linked to the browser are described in the modules APP.3.1 Web applications and APP.3.2 Web server. General security requirements that apply to the software are discussed in the module APP.6 Software in general.

2 Threats

2.1 Malicious code that spreads through a web browser

When downloading malicious content from an untrustworthy source through a web browser, there is a risk of covertly infecting the user's device. An activated malicious code could download additional malware. The code can be activated by the browser itself (such as JavaScript) or by a plugin linked to the browser (such as Adobe Flash, Java, or the components of PDF documents). In addition, the web browser can install a code in the client computer which is activated outside the browser processes.

2.2 Exploit kits

The spread of malware is significantly fostered by vulnerability lists and the so-called exploit kits. An attacker could exploit the vulnerabilities of a web browser or its add-ons for carrying out an attack without any special knowledge.

2.3 Surveillance of data exchange

Authentication and encryption during data transmission are often implemented poorly. If web services continue to use outdated encryption methods, an attacker can eavesdrop or change network traffic.

2.4 Loss of integrity in the web browser

A malicious program, malicious plugin, or a counterfeit browser component that has been added to the browser could change the data that is displayed to a user on a website or forward data to an attacker. A compromised website can be used for phishing attacks.

2.5 Security failure

Without a secure configuration of the browser, sensitive data could become available to unauthorised persons. A browser can be used for communicating the passwords of the user unintentionally. An attacker might come into the possession of sensitive data that is saved in browser cookies, history, entered data, or search queries.

3 Measures

3.1 Life cycle

Implementation

APP.1.2.M1	Using the security mechanisms of a web browser
APP.1.2.M2	Encryption of communications

Operation

APP.1.2.M3	Secure certificates
APP.1.2.M6	Using a password manager in a web browser
APP.1.2.M13	Using the DNS-over-HTTPS protocol
APP.1.2.M7	Data protection in a web browser

Additional advanced measures

APP.1.2.M9	Isolated browser environment
APP.1.2.M10	Private browsing
APP.1.2.M11	Checking for malicious content
APP.1.2.M12	Two-browser strategy

3.2 Key measures

APP.1.2.M1 Using the security mechanisms of a web browser

a. The web browser uses sandboxing. Every browser and processing instance has access only to its own resources.
b. A browser is used that isolates websites from each other as autonomous processes or separate threads. Plugins and add-ons are only run in areas isolated from each other.
c. The browser implements a content security policy (CSP) that complies with the up-to-date W3C specifications.
d. The web browser supports the Same-Origin Policy (SOP) and Subresource Integrity functionalities.

APP.1.2.M2 Encryption of communications

a. The web browser supports the secure version of the TLS security protocol of the transport layer (2020, TLS 1.3).
b. The insecure versions of TLS have been deactivated.
c. The browser supports the RFC 6797 HSTS security mechanism (HTTP Strict Transport Security).

APP.1.2.M3 Secure certificates

a. The browser enables issuing a list of trusted root certificate issuers and completing it with certificates that have been implemented in the organisation.
b. The browser supports extended validation (EV) certificates.
c. Root certificates can be added, changed, or deleted only when the person has administrative privileges.
d. The certificates can be cancelled through the local web browser.
e. The browser checks the validity of the server certificates with the help of public keys and time of expiry.
f. The browser checks the status of the server certificate and verifies the certificate chain along with the root certificate.
g. The user can understand and see clearly whether data exchange is encrypted or not. If necessary, the user can check the server certificate in the browser.
h. The browser notifies the user of the absence or invalidity of certificates. The connection is terminated only after a clear confirmation from the user.

APP.1.2.M6 Using a password manager in a web browser

a. The password manager creates a unique and secure connection between the website, username, and password in the web browser.
b. The passwords are stored in the password manager in an encrypted format. Access to the passwords that are stored in the password manager is only possible after entering the master password.
c. Authentication with a password manager is only applied for the ongoing session.
d. The user can delete their own saved passwords.
e. Synchronisation of passwords in the password manager via a cloud service is prohibited.

APP.1.2.M13 Using the DNS-over-HTTPS protocol

a. Browsers that are used in client devices support the use of the DNS-over-HTTPS (DoH) protocol.
b. Once DoH has been implemented, the DoH is activated in the web browsers of client devices.
c. The DNS server used for internal reverse resolving supports the DNS-over-HTTPS protocol.

3.3 Standard measures

APP.1.2.M7 Data protection in a web browser [user]

a. Third-party browser cookies are blocked. The user can delete any cookies that have been saved.
b. The autocompletion of data entry has been deactivated. If the function is still used, the user can delete the autocompletion data.
c. The user can delete browser history.
d. The synchronisation of the browser with a cloud service is deactivated.
e. The telemetry functions of a manufacturer and the automatic forwarding of error messages have been deactivated.
f. Any connected external devices (such as a microphone or a web camera) are deactivated in the browser by default.
g. The browser enables configuring or blocking the use of WebRTC, HSTS, and JavaScript.

3.4 Advanced measures

APP.1.2.M9 Isolated browser environment (C-I)

a. A browser is only used in an isolated environment (e.g. ReCoBS (Remote-Controlled Browser System) or virtualised instance).

APP.1.2.M10 Private browsing [user] (C-I)

a. The browser is used in a private/incognito browsing mode where the user's IT system does not save the data permanently.
b. The browser has been configured to delete the browsing metadata when the browser is closed.

APP.1.2.M11 Checking for malicious content (C)

a. When browsing, the web pages are checked for malware and their reputation is verified. Visiting web pages that are classified as malicious is blocked.
b. Web pages are checked in compliance with the data protection legislation.

APP.1.2.M12 Two-browser strategy (A)

a. If any unsolved security issues occur with the web browser, a secure browser of another manufacturer is installed for alternative use.

APP.1.4 Mobile applications (apps)

1 Description

1.1 Purpose

To present measures for the protection of data that is processed in mobile applications (apps) that support the business processes. Apps are discussed regardless of origin (self-built or purchased from a mobile app store).

1.2 Responsibility

The IT department is responsible for the compliance with the mobile application measures.
Additional responsible persons: Responsible specialist.

1.3 Limitations

The security measures for the operating systems iOS and Android in mobile devices are discussed in the modules SYS.3.2.3 iOS in the organisation and SYS.3.2.4 Android.
The central management of mobile devices is described in the module SYS.3.2.2 Mobile device management (MDM).
The aspects of implementing applications is examined in the modules APP.3.1 Web applications and APP.4.3 Database systems of the module group APP (Applications).
The modules OPS.1.1.6 Software testing and approval and APP.6 Software in general explore the general aspects of applications.

2 Threats

2.1 Choosing an unsuitable mobile application

If compatibility with business processes is not considered when selecting mobile apps, the applications could begin to hinder business processes. If the necessary conditions for the functioning of a mobile app (such as the speed of the mobile network connection or compatible hardware) are not taken into account sufficiently, the application might not work as required. A mobile app could prove useless in the long run if the manufacturer cannot guarantee long-term stability when using it or if they do not provide sufficient maintenance for the application.

2.2 Excessive privileges

The mobile applications of the iOS and Android operating systems need comprehensive access and user privileges for the functions and services to work. When a mobile app is used which requires more rights than it would really need to function, it threatens the confidentiality and integrity of the data in the endpoint. Apps can forward information (e.g. location of the device, photos, contact and calendar information) to unauthorised third parties. Excessive privileges in a mobile app could cause direct financial damages (e.g. due to phone calls, text messages, or purchasing mobile apps).

2.3 Unwanted functions in mobile apps

When installing a mobile app from an unchecked or untrustworthy source, the user might download malware along with the application to their device.

2.4 Software vulnerabilities and errors in mobile apps

A mobile app could contain security vulnerabilities. Known and yet-to-be published vulnerabilities (the so-called zero-day vulnerabilities) can be used for attacking entire IT systems through the device or its network connections. The updates and user support of many applications ends soon after they are developed. As the identified shortcomings are not fixed with updates and security patches, the mobile app retains its vulnerabilities.

2.5 Insecure local storage of application data

When the data stored in the device with the mobile apps (such as user profiles and documents) is not sufficiently secured, other applications could gain access to them. Unauthorised persons can easily read that data (for example, if an employee has lost their device). Locally stored data is often not taken into consideration in data backup concepts, and therefore, this data could be lost if the endpoint is lost or malfunctions.

2.6 Deducing confidential data from metadata

Mobile apps are used for collecting a lot of metadata, some of which could be confidential (such as phone and network connections, movement data, and the visited websites). Metadata can be used for deducing other kinds of information as well, such as the systems in the organisation, its exact locations of activity, and personnel.

2.7 Leak of confidential data from mobile applications

The operating systems of mobile devices enable using various interfaces for data exchange between mobile applications and external devices. The user also has several opportunities for data exchange (e.g. through a local memory card, device camera, or other applications). The data from a mobile application could be sent to a cloud service. Often, data is forwarded through the server of the seller of the mobile app or the manufacturer of the mobile device, where third parties could find opportunities for accessing confidential data.

2.8 Insecure connection with backend systems

Data transmission between mobile devices and backend systems usually takes place through insecure networks (mobile network, WLAN, etc.). When insecure protocols are used for connecting with backend systems, data can be intercepted and corrupted.

2.9 Communication routes outside the organisational infrastructure

Mobile apps enable creating communication routes which the organisation cannot identify or control. The user can use cloud services for forwarding data from the mobile device, the use of which is not controlled by the organisation. The close connection of social media services with mobile applications makes it difficult to understand whether the data has been transmitted from the endpoint and when.

2.10 Dependence on the backend or external systems and services

The work of many mobile applications depends directly on the external systems and services. Without data connection, many mobile apps have limited function or they cannot be used at all. If the data connection linked to an external service or the service itself is unavailable, the availability of the mobile application is disrupted.

3 Measures

3.1 Life cycle

Planning

APP.1.4.M1 Analysis of the requirements for mobile applications

Implementation

APP.1.4.M5	Limiting and controlling the access rights of mobile applications
APP.1.4.M3	Secure distribution of mobile applications

Operation

APP.1.4.M7	Security of the local data of mobile applications
APP.1.4.M8	Detection and prevention of data leaks
APP.1.4.M16	Mobile application management

Disposal

APP.1.4.M12	Secure uninstallation of mobile applications

Additional advanced measures

APP.1.4.M14	Multi-factor authentication in mobile applications
APP.1.4.M15	Penetration testing of mobile applications

3.2 Key measures

APP.1.4.M1 Analysis of the requirements for mobile applications [responsible specialist]

a. Before the implementation of a mobile app, mobile application requirements based on business processes are mapped.
b. Risks related to implementing a mobile app are analysed and security requirements are determined while taking into account the protection requirement of the processed data, the IT environment, and legal framework conditions.

APP.1.4.M5 Limiting and controlling the access rights of mobile applications [responsible specialist]

a. Before implementing a mobile app, the access rights of the app are restricted to the minimum that is required for its operation.
b. The security settings of a mobile app cannot be changed by the users or the application itself independently. If this is technologically impossible, compliance with the restrictions is checked regularly.

APP.1.4.M7 Security of the local data of mobile applications

a. When granting access to the internal documents of the organisation to a mobile app, sufficient measures are applied for the protection of local data.
b. Access keys are encrypted.
c. The operating system does not cache sensitive data in other storage sites.

APP.1.4.M8 Detection and prevention of data leaks

a. In order to avoid transmitting confidential data, data transmission is analysed when testing the mobile app (see also APP.1.4.M4 Testing and approval of mobile applications).
b. The mobile app is checked for storing confidential data in log or subsidiary files.
c. Unnecessary transfer of sensitive data is limited in the data exchange of the mobile app.

3.3 Standard measures

APP.1.4.M3 Secure distribution of mobile applications

a. Mobile applications are acquired only from secure and trustworthy sources.
b. Internal applications of the organisation which are used for processing data that needs protection are only distributed through an internal app store or Mobile Device Management (MDM).

APP.1.4.M12 Secure uninstallation of mobile applications

a. When uninstalling a mobile application, all applications files, files generated by the app, and temporary data related to the app (such as buffers) are deleted.
b. When uninstalling a mobile app, the application data is deleted in external systems (such as data backed up in a cloud service).

3.4 Advanced measures

APP.1.4.M14 Multi-factor authentication in mobile applications (C-I)

a. Several authentication factors are used for authentication in a mobile app. The devices used for running a mobile app support multi-factor authentication.
b. The authentication factors are sufficiently forgery-proof. When using biometric identification measures, the reliability of the authentication has been analysed regarding its ability to avoid forgery attempts.

APP.1.4.M15 Penetration testing of mobile applications (C-I-A)

a. Before implementing a mobile app, a penetration test is conducted for the app.
b. In order to detect security vulnerabilities, the data exchange interfaces with backend systems and the local data storage are also checked.
c. Penetration tests are repeated when major changes are made to the mobile app or the operating system of the mobile device.

APP.1.4.M16 Mobile application management (C-I-A)

a. Central mobile device management is used for the configuration and management of mobile applications.

APP.2 Directory services

APP.2.1 Directory service in general

1 Description

1.1 Purpose

To present measures for the secure use of a general directory service and the protection of directory service data.

1.2 Responsibility

The IT department is responsible for implementing the information security measures of the module 'Directory service in general'.
Additional responsible persons: Data protection specialist, responsible specialist.

1.3 Limitations

The module describes the general security aspects of directory services. The measures for the protection of the most well-known directory services are presented in modules APP.2.2 Active Directory Domain Services and APP.2.3 OpenLDAP.
Security measures pertaining to a server that shares directory services are presented in module group

SYS.1 Server. The management of access rights of directory services complies with module ORP.4 Administration of identity and rights.
Additionally, the measures of module group OPS.1.1 Main IT operations should be taken into consideration.

2 Threats

2.1 Missing or insufficient planning of the implementation of a directory service

The security of a directory service depends largely on the security controls of the server sharing the directory service. A directory service may be installed and used in many operating systems. In the case of a very heterogeneous or complex comprehensive solution, the directory service might retain some vulnerabilities which were not addressed in the planning stage. Insufficient planning of administrative operations puts the system in danger of being managed in an insecure or inadequate manner.

2.2 Incorrect or inadequate implementation of partitioning and duplication

If the partitioning and duplication of the data structure of a directory service is not planned from the beginning, changing the settings later is possible, but could cause problems. When the partitioning or duplication of directory service data is inadequately or insufficiently planned, it could lead to data losses, errors in data storage, poor performance of the directory service, or malfunctions in the directory service.

2.3 Inadequate management of access rights

Due to inadequate management of the access rights of users and groups that are managed through a directory service (e.g. by not granting the necessary access rights), there could be malfunctions in the daily operation of systems.

2.4 Wrong access configuration of a directory service

When implementing a directory service, the directory service is granted access to regular applications (such as internet or intranet applications) as well. As a result of a wrong configuration, unauthorised access is granted to the directory service.

2.5 Malfunctions in the components of a directory service

Technical malfunctions due to hardware and software problems could cause interruptions in a directory service. As a result, the data that is stored in the directory is not temporarily accessible and the business processes of the organisation are interrupted. In extreme cases, the data may be lost.

2.6 Interfering with a directory service through unauthorised access

If an attacker manages to gain access to a directory service, they may be able to damage the directory service and its data. Excessive rights could grant unauthorised access to network resources and services and affect or damage them.

2.7 Incorrect configuration of a directory service

Configuration errors of numerous functions of a directory service could lead to unauthorised access to the entire directory service. If the standard configuration is not sufficiently monitored or adapted, authentication data that is transmitted as cleartext may be used for further attacks.

3 Measures

3.1 Life cycle

Planning

APP.2.1.M1	Security guidelines for a directory service
APP.2.1.M2	Implementation plan for the directory service
APP.2.1.M8	Partitioning a directory service
APP.2.1.M15	Security for the migration to the directory service

Implementation

APP.2.1.M3	Organisation of access rights of the directory service
APP.2.1.M11	Regulating access to a directory service

Operation

APP.2.1.M5	Secure configuration of the directory service
APP.2.1.M6	Secure operation of the directory service
APP.2.1.M17	Ensuring the security of access details requiring protection
APP.2.1.M12	Monitoring the directory service
APP.2.1.M13	Data exchange security of the directory service
APP.2.1.M18	Duplication of directory services

APP.2.1.M19 Managing anonymous access to a directory service

Acquisition

APP.2.1.M9 Selecting suitable directory service components

Disposal

APP.2.1.M14 Decommissioning a directory service

Additional advanced measures

APP.2.1.M16 Emergency action plan for the directory service

APP.2.1.M20 Security of the duplication of a directory service

APP.2.1.M21 Guaranteeing the high availability of a directory service

3.2 Key measures

APP.2.1.M1 Security guidelines for a directory service

a. Security guidelines for a directory service have been prepared, which comply with the general information security policy.
b. The security guidelines for the directory service have been introduced to the managers and users of the directory service.

APP.2.1.M2 Implementation plan for the directory service [data protection specialist, responsible specialist]

a. When planning a directory service, its compatibility with the applications in use is taken into consideration.
b. The implementation plan for the directory service documents:

- structure of the directory service;
- a model of object classes and attribute types that complies with the established usage;
- a need-based access rights management model;
- the data protection specialist is involved in the planning of a directory service containing personal data.

c. Measures are planned to prevent the unauthorised collection of data from the directory service.

APP.2.1.M3 Organisation of access rights of the directory service [responsible specialist]

a. Administrative operations of the directory service and its data are kept separate from each other. The administrative tasks are documented; persons fulfilling the tasks do not act in conflicting roles.
b. The access rights of the users and managers comply with the security guidelines for the directory service. Operations related to the access rights are traceable.
c. When several directory service trees are merged, actual consolidated rights are checked.

APP.2.1.M5 Secure configuration of the directory service

a. Directory services and the entire infrastructure of the directory service (server, client computers, applications) are configured in a secure manner.
b. The users of the directory service are informed about the changes to the configuration of the directory service ahead of time.
c. Prior to changing the configuration, relevant data is backed up.

APP.2.1.M6 Secure operation of the directory service

a. The management and operational processes of the directory service are documented.
b. A special user account is used for managing the directory service. Administrative accounts are not used for regular daily work tasks.
c. Access to administrative instruments is blocked for regular users.

APP.2.1.M17 Ensuring the security of access details requiring protection

a. Access to attributes of directory services that contain access details requiring protection (such as passwords) is strictly limited.

3.3 Standard measures

APP.2.1.M8 Partitioning a directory service

a. When planning partitioning, the availability and protection requirement of the directory service have been taken into account.
b. The partitioning of the directory service is planned in such a manner that it would limit the impact of security incidents and allow to restore the directory service one partition at a time.

APP.2.1.M9 Selecting suitable directory service components [responsible specialist]

a. Based on the established selection criteria, suitable components for the implementation of a directory service have been determined (see APP.6 Software in general).
b. Components of a directory service allow to implement security requirements that have been previously established based on the purpose of the directory service.

APP.2.1.M11 Regulating access to a directory service

a. Access to a directory service has been configured in accordance with the security policy for directory services.
b. When using a directory service via the internet, the server is protected with a security gateway

APP.2.1.M12 Monitoring the directory service

a. The log data of a directory service is analysed regularly according to the policy and criteria established in the organisation.
b. The monitoring of a directory service also includes the servers where the directory service is used.

APP.2.1.M13 Data exchange security of the directory service

a. Data exchange between the directory service server and the client is secure (encrypted with the SSL/TLS protocol).
b. Access to the directory service server from the internet is restricted.
c. Access to data is only granted based on need.
d. When using service-oriented architecture (SOA) through the service registry, the validity of the user's access rights is verified.

APP.2.1.M14 Decommissioning a directory service [responsible employee]

a. When a directory service is decommissioned, the availability of the necessary rights and data is guaranteed and everything else is deleted.
b. The users are informed ahead of time of the decommissioning of the directory service.
c. Removing single partitions does not affect the availability of other partitions.

APP.2.1.M15 Security for the migration to the directory service

a. A migration plan is prepared before migrating a directory service. The planned changes to the directory service scheme are documented.

b. When the access rights have been increased temporarily for migration, then the previous level of rights is restored after the migration is complete.
c. Access rights of users who have transferred to the new directory system are updated.

APP.2.1.M18 Duplication of directory services

a. When planning to duplicate directory services, the objectives of the duplication are determined and an action plan describing the application scenario and network topology is prepared.
b. If the objective is not the high availability of an entire directory service, only the necessary components of the directory service are duplicated.
c. When applying duplication, sufficient performance has been taken into consideration.

APP.2.1.M19 Managing anonymous access to a directory service

a. If anonymous users need greater access rights to specific sections of a directory tree, a special temporary user account (a so-called proxy user) is created. Once the account is no longer used, access rights to the directory service are fully cancelled.
b. The search function of the directory service is limited to avoid a leak of sensitive directory data.

3.4 Advanced measures

APP.2.1.M16 Emergency action plan for the directory service (C-I-A)

a. When preparing for an emergency, an emergency plan that corresponds to the needs of the organisation has been established and documented.
b. The system configuration and recovery procedures of the directory service components are included in the emergency plan.

APP.2.1.M20 Security of the duplication of a directory service (C-I)

a. When duplicating a directory service with confidential content, the data is encrypted on the level of the application or transport layer (for example, using the IPSec protocol).
b. Methods for authentication are as secure as possible.

APP.2.1.M21 Guaranteeing the high availability of a directory service (A)

a. A suitable strategy has been selected to ensure the high availability of a directory service (either Master-Master or Master-Replica replication).
b. Procedures for the directory service under exceptional circumstances have been established (for example, when duplicated parts of the directory service contradict each other).

APP.2.2 Active Directory

1 Description

1.1 Purpose

To present measures for the security of the regular use of Active Directory Domain Service (AD DS) in a situation where the AD service is used for managing an infrastructure that consists of Microsoft Windows systems (clients and servers).

1.2 Responsibility

The IT department is responsible for compliance with the Active Directory Domain Service measures.
Additional responsible persons: Responsible specialist.

1.3 Limitations

The module is applied to all Microsoft AD DS directory services, including Active Directory Lightweight Directory Services (AD LDS).
General security recommendations for directory services are presented in the module APP.2.1 Directory service in general.
The implementation of AD DS must take place in compliance with the following modules: ORP.4 Administration of identity and rights, OPS.1.1.3 Patch and change management, CON.3 Data backup concept, OPS.1.2.2 Archiving, and OPS.1.1.5 Logging. OPS.1.1.2: IT systems management, OPS.1.2.5: Remote maintenance, DER.1 Detection of security incidents, DER.2.1 Handling of security incidents, DER.4 Emergency management, and APP.3.6 DNS server also affect AD DS modules.
The module does not cover security measures for the operating systems of Windows servers and

clients (e.g. SYS.1.2.2 Windows Server or SYS.2.2.3 Windows client) and the management of the network infrastructure.

2 Threats

2.1 Inadequate planning of security boundaries

If security boundaries of the general AD DS structure (AD domains in the so-called AD forest) are not consciously and carefully planned, all domains in the forest and objects therein, including all accounts and IT systems, might be compromised as a result of an attack due to the trust relationships between the domains.

2.2 Profusion or weakness of trust relationships

Trust relationships between AD domains and forests enable granting access to an account to the resources of another AD domain or AD forest. If the necessity and type of trust relationships between the AD forests and AD domains is not evaluated regularly and the control procedures are inadequate, then this could create problems with access rights as well as data leaks.

2.3 Lack of security functions in legacy systems

Using older operating systems as (primary) domain controllers or a domain functional level (DFL) that is not updated prevents the implementation of modern security functions and increases the danger of using insecure default settings.

2.4 Excessive roles and operating redundant services in a domain controller

Every additional domain controller service (except AD DS and its indispensable supporting services, such as DNS) adds security vulnerabilities to the central infrastructure components, incl. configuration errors. Excessive roles and additional security vulnerabilities may be abused (e.g. for making unauthorised copies of or changes to data).

2.5 Insufficient supervision and documenting of delegated privileges

When an organisation fails to form AD groups and delegate the related privileges systematically according to a plan, the users will receive access rights that exceed the extent that is necessary. Excessive access rights may be abused.

2.6 Insecure authentication

The legacy mechanisms of AD authentication, such as NT LAN Manager (LM) and NTLMv1, are not secure today. An attacker may be able to acquire privileges and abuse them without having to know, guess, or otherwise crack user passwords.

2.7 Administrative accounts that have excessive rights or are insecure

The administrative accounts of the suppliers of application software often receive domain administrator privileges for testing and implementing their products, despite these rights being too extensive for the task.

2.8 Re-used administrative passwords

It is possible to log into a system through a local account even if it is not connected to a domain. If the same credentials are used in several systems, the system administrator can log into other systems as well. This increases the danger that an attacker could receive domain credentials with more privileges from a system and abuse them.

2.9 Insecure storage of passwords

Passwords are stored in an AD DS database (ntds.dit) located in a domain controller. Depending on the domain controller, an MD4 hash function without salt may be used, which does not meet modern cryptography requirements. A weak hash function allows to conduct dictionary attacks, and for this reason, preventing unauthorised access to passwords stored in AD DS is of critical importance. Due to the popularity of AD DS, many different attack tools have been created for exposing passwords.

2.10 Insufficient security of domain controllers

A copy of the central database of AD DS (ntds.dit) is available from all domain controllers. It might also become available to unauthorised users due to insecure backup processes. An attacker gaining possession of a central AD DS database might lead to the attacker finding out passwords and the data in the domain being compromised. A similar threat exists when a virtual domain controller is installed in a physical virtual server with insufficient security. Administrative accounts of virtualisation might also have full access to AD DS.

2.11 Using an account with AD administrator privileges in domain clients

When accounts with excessive privileges are used for logging into or using services in servers located in a domain or in client computers, it might be possible to extract access data for a privileged account from the login data stored in a server when attacking the specific server (such as through the Local Security Authority Subsystem - LSASS memory). As a result, compromising one server or client in a domain may lead to compromising the entire domain, and potentially, the entire AD forest.

2.12 Adding computer objects to a Windows domain without supervision

When AD DS relies on default settings, a user of the domain may be able to add new computers to the domain without needing the administrative privileges of the domain for it. New IT devices might have access privileges or functions enabled, which an attacker might be able to use for attacking other components in the domain.

2.13 Exploiting privileges granted to applications

When software applications are used for adding AD DS accounts (such as Microsoft Exchange), an attacker might be able to exploit vulnerabilities in an application; for example, create users with extensive privileges, and thereby attack the entire AD DS structure (Microsoft Exchange vulnerability CVE-2019-0686, PrivExchange).

3 Measures

3.1 Life cycle

Planning

APP.2.2.M1	Planning AD DS
APP.2.2.M3	Group policies for work with Windows

Implementation

APP.2.2.M5	Improving the security of a domain controller
APP.2.2.M8	Configuration of a secure channel in Windows
APP.2.2.M9	Secure authentication in AD DS

Operation

APP.2.2.M6	Secure configuration of trust relationships
APP.2.2.M7	Secure management of Active Directory
APP.2.2.M16	Hardening AD DS accounts

APP.2.2.M17 Restricting the use of administrative accounts of an AD DS forest

APP.2.2.M18 Limiting new AD computer objects being added to a domain

Emergency response

APP.2.2.M12 Backup of domain controller data

Additional advanced measures

APP.2.2.M15 Transferring domain management to a separate AD forest

APP.2.2.M19 Secure use of virtualised domain controllers

APP.2.2.M20 Segmentation of organisational units

APP.2.2.M21 Multilayer AD DS structural model

APP.2.2.M22 Temporal restrictions on the use of administrative accounts

APP.2.2.M23 Regular analysis of access privileges and possible attack vectors

3.2 Key measures

APP.2.2.M1 Planning AD DS [responsible specialist]

a. As a minimum, the structure of AD DS corresponds to the functional level of an AD forest and domains of Windows Server 2016.

b. A needs-based and role-based concept of AD rights and the procedure for the delegation of rights have been established.

c. When planning AD DS, the following has been documented:

- the AD structure and the distribution of AD domains into AD trees and AD forests;
- the use of the Active Directory Federation Service (ADFS) and trust relationships;
- the concept for implementing group policy;
- the distribution of users and computers according to domains.

d. The following decisions have been made for each domain:

- the necessary AD objects and their hierarchy;
- security settings that depend on the types of computers and users;
- group policy;
- need-based AD data access subjects and interfaces;
- trust relationships that are generated automatically and other trust relationships.

e. For each AD object, the following data is documented:

- name and location in the AD tree;
- purpose;

- administrative access privileges for the AD object;
- configuration of object inheritance;
- connection to the group policy.

APP.2.2.M3 Group policies for work with Windows

a. The implementation of configuration settings (including security settings) to object groups takes place in accordance with the documented group policies.
b. The parameters of Group Policy Objects (GPO) are determined based on the group policy implementation concept that was prepared when planning AD. Exceptions are documented.
c. Need-based access restrictions have been established for all GPOs.
d. Each object group of the Organisational Unit (OU) only includes objects with a similar policy.
e. Access to the configuration of group policy is limited according to necessity.
f. The configuration of group policy determines (see also 'Example of group policy security settings' in the auxiliary materials) the following:

- the password policy;
- the policy for blocking accounts;
- the Kerberos policy;
- the surveillance policy;
- granting user rights;
- the configuration of security mechanisms;
- using Security Compliance Manager (SCM).

APP.2.2.M5 Improving the security of a domain controller

a. Default accounts of a domain controller (DC) are protected by sufficiently strong passwords and used only as emergency accounts.
b. DCs are protected with security controls both on the level of the operating system and AD.
c. The size assigned to DC logs complies with policies and guidelines regarding logging and identification of information security events.
d. Only domain managers may log into domain controllers locally. Regular users are blocked from any activity in domain controllers.
e. Aside from standard services necessary for a DC (such as Active Directory, Kerberos, and DNS), the DC does not provide application services (such as DFS, DHCP).
f. The domain controller does not share files into common use.

g. The domain controller is not used as a workstation computer (using the internet and external data carriers is prohibited).
h. Launching other operating systems is blocked in the domain controller.
i. Backup copies of the domain controller are made regularly.
j. A recovery plan has been prepared for the domain controller. One of the recovery options allows booting the domain controller in an AD recovery mode (Directory Services Restore Mode (DSRM)).
k. The AD recovery mode is protected with a suitable password. In this mode, operations can only be conducted based on the four eyes principle.
l. The domain controller is protected from unauthorised restarts.

APP.2.2.M6 Secure configuration of trust relationships

a. Trust relationships between AD domains and AD forests are regularly analysed.
b. When a domain does not require two-way trust with other domains in the same AD forest, the domain is relocated to a separate AD forest.
c. Data on privileges is subjected to filtration and anonymisation in trust relationships between the domains.
d. To increase the security of trust relationships, access is filtered based on security identifiers (SID).
e. The most essential configuration parameters of AD are regularly updated, including as a minimum:

- group policy objects;
- trust relationships;
- the structure of domain controllers;
- the topology for duplication;
- database characteristics;
- security updates installed into a domain controller;
- backup data carriers.

APP.2.2.M7 Secure management of Active Directory [responsible specialist]

a. Service administrator accounts are managed only by the members of service administrator group.
b. Before adding an account to a predetermined AD DS account group, the specialist checks whether all privileges granted to the group are required for activities related to the account.
c. Administrators are added to the Schema-Admins group only temporarily for the duration of changing the schema. After changing the schema, members are removed from the group.

d. Privileged user accounts not part of domain administrator groups (e.g. Domain Admins) are created only with a time limit and when it is justified.
e. Domain-based groups are not used for regulating data access in a global directory, only global or universal groups are used for this.

APP.2.2.M16 Hardening AD DS accounts

a. AD DS default accounts have complex and unique passwords.
b. Integrated guest accounts have been closed.
c. The access rights of the Everyone group have been restricted based on need.
d. Privileged accounts belong in the Protected Users group.
e. Service accounts belong in the Managed Service Accounts group.
f. Access to AdminSDHolder, an AD object, is restricted.
g. Accounts are only deleted after the deadlines for checking the history of the account use and logs have passed.

APP.2.2.M17 Restricting the use of administrative accounts of an AD DS forest

a. The use of administrative accounts of an AD forest and domains which have extensive access privileges is only allowed in the necessary IT systems.
b. Accounts in the Schema Admins, Enterprise Admins, and Domain Admins groups can only log into a domain controller.

APP.2.2.M18 Limiting new AD computer objects being added to a domain

a. AD computer objects (computers and other IT devices) can be added to a domain only by the users of the respective administrative accounts.

3.3 Standard measures

APP.2.2.M8 Configuration of a secure channel in Windows

a. Windows has a secure and encrypted data communication channel (Secure Channel) for the transmission of sensitive data that is configured according to the security requirements and group policy parameters.
b. The use of a secure channel is activated in all client systems of the domain.

APP.2.2.M9 Secure authentication in AD DS

a. If possible, the AD environment uses the Kerberos authentication protocol with the security settings AES128_HMAC_SHA1 or AES256_HMAC_SHA1.
b. Insecure authentication via LM and NTLMv1 has been blocked. When the use of Kerberos is not yet possible due to legacy systems, then the system transfers to at least NTLMv2 first, and a plan is prepared and deadlines set for the implementation of Kerberos.
c. SMB traffic between domain controllers and domain controllers and domain client computers has been signed. Using the SMBv1 protocol is blocked.
d. Anonymous access to domain controllers has been blocked.
e. LDAP sessions are signed and a Channel Binding Token (CBT) has been adopted.

APP.2.2.M12 Backup of domain controller data

a. Separate service management accounts have been created for backing up the data of a domain controller; its rights are valid in only one domain. The number of group members of the backup administrators is limited to a minimum.
b. Access rights to a container object for storing privileges (AdminSDHolder) are regulated as strictly as possible (see also APP.2.2.M7 Secure management of Active Directory).
c. The data of domain controllers is backed up regularly.
d. Data backed up from domain controllers is protected with security controls equal to the ones that have been established to protect domain controllers.
e. The functioning of the data backup and recovery procedures of the domain controllers is checked regularly. When recovering domain controllers, duplication of data from another domain controller is preferred to a backup copy.

3.4 Advanced measures

APP.2.2.M15 Transferring domain management to a separate AD forest (C-I-A)

a. Domain management accounts and IT systems are located in a separate AD forest
- with one-way trust (the work environment trusts the administrative environment).

b. For an accurate management of privileges and for logging privileged operations, additional technologies are used (e.g. Privileged Access Management, or PAM).

APP.2.2.M19 Secure use of virtualised domain controllers (C-I-A)

a. Virtualised domain controllers are located in a physical host that is separate from other virtual IT systems.
b. Virtual machine, IT systems involved in virtualisation, and administrative accounts of the virtualisation layer are located in a separate AD forest from the virtualised domain controller.

APP.2.2.M20 Segmentation of organisational units (C-I-A)

a. Organisational units (OUs) requiring independence due to information security or other reasons are located in separate AD forests.

APP.2.2.M21 Multilayer AD DS structural model (C-I-A)

a. The structure of an AD forest is divided between layers on different levels based on the protection requirements of the IT systems and applications.
b. All accounts of an AD forest, IT systems, and applications are located in the AD forest layer resulting from the scope of the required authorisation.
c. Higher-level accounts have no right to log into the resources on the lower level.
d. Lower-level accounts have no control over the accounts and resources of a higher level.

APP.2.2.M22 Temporal restrictions on the use of administrative accounts (C-I-A)

a. The authorisations required for administrative operations are given to administrative accounts only based on verified needs and for a limited period.

APP.2.2.M23 Regular analysis of access privileges and possible attack vectors (C-I-A)

a. The organisation assesses regularly whether the AD DS authorisation structures and the access privileges of accounts are appropriate as well as their scope. If the installation of an IT system update may impact access privileges in the AD DS, then the same assessment is conducted after the IT system update as well.
b. Authorisations granted to applications integrated with the AD DS (such as Microsoft Exchange) are limited to the least necessary level.
c. The organisation analyses attack vectors jeopardising the security of the AD domain or the entire forest due to taking over an AD DS account, and limits their likelihood.
d. Activities involving accounts critical to security are monitored from the point of view of possible attacks.

APP.2.3 OpenLDAP

1 Description

1.1 Purpose

To present measures for the secure use of a directory service that is based on OpenLDAP and for the proper protection of processed information.

1.2 Responsibility

The IT department is responsible for implementing the OpenLDAP measures.

1.3 Limitations

The module is based on version 2.4 of OpenLDAP. General security recommendations for a directory service are presented in module APP.2.1 Directory service in general.
The implementation of OpenLDAP must comply with the following modules: ORP.4 Administration of identity and rights, OPS.1.1.3 Patch and change management, CON.3 Data backup concept, OPS.1.2.2 Archiving, OPS.1.1.5 Logging, and OPS.1.1.2: IT systems management.
Administrative processes (such as data backup, logging, and patch management) are discussed only to the extent in which they are related to the peculiarities of OpenLDAP.

2 Threats

2.1 Missing or inadequate planning for OpenLDAP

When the backend systems or related parameters are chosen incorrectly, they affect the functions enabling OpenLDAP in undesirable ways.

2.2 Inadequate separation of the autonomous and online access to OpenLDAP

Online access to OpenLDAP uses the LDAP protocol; in case of an autonomous system, the database files are accessed directly. Erroneous use of the autonomous and online access modes creates various error situations. For example, the database could become incompatible with OpenLDAP after recovery so it becomes unusable.

3 Measures

3.1 Life cycle

Planning

APP.2.3.M1	Planning the implementation of OpenLDAP

Implementation

APP.2.3.M3	Secure configuration of OpenLDAP
APP.2.3.M4	Secure configuration of the OpenLDAP database
APP.2.3.M5	Secure configuration of the OpenLDAP access rights
APP.2.3.M8	Limiting the attributes of OpenLDAP
APP.2.3.M9	Partitioning and duplication of OpenLDAP
APP.2.3.M11	Limiting the operational environment of OpenLDAP

Operation

APP.2.3.M6	Secure authentication in OpenLDAP
APP.2.3.M10	Updating OpenLDAP securely

3.2 Key measures

APP.2.3.M1 Planning the implementation of OpenLDAP

a. When planning OpenLDAP, client applications are taken into consideration that are going to be used and need to be supported in the future.

b. When planning OpenLDAP, the following is considered as a minimum:

- the selection of the version of OpenLDAP and its requirements;
- requirements applying to performance;
- configuration and integration of applications (such as an address book) with OpenLDAP;
- backend systems (such as a database) that are necessary for the functioning of OpenLDAP and their limitations;
- the choice of the configuration method (static or web configuration);
- overlay limitations and ensuring the correct order of overlays.

APP.2.3.M3 Secure configuration of OpenLDAP

a. The configuration of the slapd server (whether using the slapd.conf configuration file or the slapd-config web configuration) is done securely and only authorised users have the administrative rights necessary for configuration.
b. The values of the OpenLDAP configuration settings (directives) are checked and adjusted if necessary before their initial enforcement.
c. The backend systems and overlays of OpenLDAP are taken into account during configuration.
d. Suitable limitations to time and volume are set for the search queries of OpenLDAP.
e. After each change, the configuration of the slapd server is checked and documented.

APP.2.3.M4 Secure configuration of the OpenLDAP database

a. Only accounts for this particular purpose have access to the slapd server and database files.
b. The default settings of the database used by OpenLDAP are adjusted according to the protection requirements.

APP.2.3.M5 Secure configuration of the OpenLDAP access rights

a. Each operation of the user in the access control list is covered with a relevant directive which links the user with the authorised target objects and the extent of user rights.
b. When determining the access control lists, the fact that the database directives of OpenLDAP overwrite global directives is taken into account.

APP.2.3.M6 Secure authentication in OpenLDAP

a. In order to differentiate between the users of a directory service, authentication of the users is required and anonymous access is restricted with the disallow bind_anon configuration directive.
b. Authentication data between a slapd server and a communication partner is encrypted.
c. Servers and client computers save passwords only in a hashed format by using an algorithm that can withstand cracking to a sufficient degree.

3.3 Standard measures

APP.2.3.M8 Limiting the attributes of OpenLDAP

a. In order to limit the attributes of OpenLDAP and guarantee the uniqueness of the values and the integrity of reference attributes, overlays are used.

b. The attribute limitations that are set with the help of the OpenLDAP overlays are only implemented to user data.

APP.2.3.M9 Partitioning and duplication of OpenLDAP

a. Security requirements have been taken into account when sectioning and duplicating OpenLDAP.
b. Partitioning a directory service into sub-trees is planned and implemented in accordance with measure APP.2.1.M8 Partitioning a directory service.
c. Data synchronisation between servers is achieved through duplication. The duplication mode is chosen according to network connection and availability requirements.

APP.2.3.M10 Updating OpenLDAP securely

a. Before installing a new version, it is analysed to determine whether and how the new version affects the functioning of the implemented backend systems, software dependencies, and overlays. After the installation of a new version, backend systems and overlays are tested to make sure that they are functional.
b. The functioning of the scripts created by the administrators themselves is checked before a new version is installed in the production environment.
c. After OpenLDAP is updated, its configuration and access rights are checked.

APP.2.3.M11 Limiting the operational environment of OpenLDAP

a. The configuration files and databases that are necessary for the operation of a slapd server are limited to an operational directory.
b. When a slapd server is located in a container, additional security controls from module SYS.1.6. Containerisation are implemented.
c. If the slapd server is located in a separate server, the server uses sufficient hardening measures.

3.4 Advanced measures

There are no advanced measures in this module.

APP.3 Network services

APP.3.1 Web applications

1 Description

1.1 Purpose

Describing measures for the safe operation of web applications and online services as well as the protection of data that is processed.

1.2 Responsibility

The IT department is responsible for the implementation of the measures of the module 'Web applications'.
Additional responsible persons: The procurement department, the head of information security.

1.3 Limitations

The general measures for acquiring software are presented in the module APP.6 Software in general.
Measures regarding the security of a web server, including editing web content and emergency management, are described in the module APP.3.2 Web server.
The development of web applications is explained in the module CON.10 Web applications development.
The logging of web applications is discussed in the module OPS.1.1.5 Logging.

2 Threats

2.1 Inadequacy of logging security events

Insufficient logging of security events in a web application makes it impossible to identify security events later and to find out why they occurred. Attacks (for example, unauthorised configuration changes of web applications) might remain undetected. Insufficient logging also complicates the identification and elimination of vulnerabilities.

2.2 Excessive disclosure of background information in a web application

Websites and data that are generated and transmitted through web applications could contain information about the background systems (such as data on the IT components and the versions of

operating systems). This information could simplify targeted attacks on a web application for an attacker.

2.3 Misuse of a web application with automated solutions

The automation of the use of web application functions could enable an attacker to make numerous attack attempts in a short span of time. For example, repeated logins facilitate guessing the valid combinations of usernames and passwords (a brute-force attack). If a web application provides feedback about the existence of a username, lists of valid usernames can be compiled. Repeated access to resource-heavy functions (such as complex database queries) can be used for a denial-of-service attack on the application level.

2.4 Deficiency of the authentication and session management of a web application

Certain functions of a web application can only be used by authorised users. If an attacker manages to determine the session identifier of an authorised user due to inadequate session management, they can gain access to the protected functions and resources of the web application. In case of a session fixation attack, the attacker first allows the web application to set the session ID and then pass it to an authorised user (for example, via an email link). If an authorised user uses the link and then uses the session ID sent by an attacker for authentication in the web application, the attacker can also use the web application with the help of the known session identifier in the security context of the user that was attacked.

3 Measures

3.1 Life cycle

Operation

APP.3.1.M1	Authentication of web applications
APP.3.1.M14	Protection of confidential data
APP.3.1.M22	Inspection and penetration testing of web applications

Implementation

APP.3.1.M4	Limiting the use of data and content
APP.3.1.M7	Protection against the automated use of web applications
APP.3.1.M11	Secure connection with backend systems

APP.3.1.M12 Secure configuration of web applications

APP.3.1.M21 Secure HTTP configuration of web applications

Planning

APP.3.1.M8 Secure architecture for a web application

Acquisition

APP.3.1.M9 Procedure for acquiring web applications

Additional advanced measures

APP.3.1.M20 Web application firewalls

3.2 Key measures

APP.3.1.M1 Authentication of web applications

a. Access to web application resources is possible only via the authentication of the users.
b. The methods of authentication are secure and their selection is documented.
c. The authentication data of the user of the web application can only be saved in the client computer on the basis of an unequivocal permission of the user of the web application.
d. The number of allowed unsuccessful login attempts is set in the web application. After exceeding the number of unsuccessful login attempts, the user is restricted from accessing the application for the pre-determined period.

APP.3.1.M4 Limiting the use of data and content

a. The web application only delivers data and content to users as intended and permitted.
b. The uploading function of the web application files and the launching rights of the files are restricted. The user is only able to save files in the pre-determined location.
c. The redirection functionality for users is limited in the web application.
d. Web application forwarding destinations are in a trusted domain. When a user leaves a trusted domain, the user is informed.

APP.3.1.M7 Protection against the automated use of web applications

a. Web applications are protected against unauthorised automated access.
b. Where RSS feeds or other automated functions are available on the web application, they are taken into account when setting up the security mechanisms.

APP.3.1.M14 Protection of confidential data

a. Confidential data is protected with sufficiently strong encryption during transmission. Even in the event of connection malfunctions, an unencrypted channel is not used instead of an encrypted channel.
b. No sensitive data is stored or temporarily buffered on the client's computer.
c. Confidential data on the forms is not stored in the browser in the form of cleartext.
d. The web application's access data is protected on the server by sufficiently strong encryption. Only password hash is stored in the server out of all password data.
e. The source code of the web application is protected against unauthorised access.

3.3 Standard measures

APP.3.1.M8 Secure architecture for a web application [procurement department, the head of information security]

a. When planning web applications, security aspects are taken into consideration. When planning the security mechanisms of a web application, their future capability is also taken into account.
b. The network architecture has multiple layers. The security mechanisms of the web, application, and data layers are separated.
c. The design of the software architecture takes into account which security mechanisms are implemented for which components, how the web application is integrated into the existing infrastructure, and which encryption functions and procedures are used.
d. The software architecture of the web application supports and connects the business processes of an organisation.
e. The software architecture of the web application, with all components and dependencies, is documented. The documentation also identifies the non-application components that are necessary for the application to work.

APP.3.1.M9 Procedure for acquiring web applications [procurement department]

a. Requirements for the products have been established and an assessment scale agreed to acquire web application components.
b. In addition to the general aspects of acquiring software, the following is taken into consideration when acquiring web applications:

- validation of the input and coding the output of the web application;
- secure authentication procedures;
- secure session management;
- the use of secure cryptographic mechanisms;
- the management of user access rights;
- secure data storage in a server;
- the sufficient logging of events;
- the availability and installation of security patches;
- protection against web attacks.

c. If a service provider develops a web application, the implementation of the security requirements of the service provider and the organisation's access to the source code are guaranteed.

APP.3.1.M11 Secure connection with backend systems

a. Access to backend systems is only possible through the determined interfaces and systems and with the minimum necessary rights.
b. Data traffic between the users and web applications or applications and other services or background systems is regulated with security gateways.
c. The data traffic of external connections is encrypted and takes place only between authenticated destinations.

APP.3.1.M12 Secure configuration of web applications

a. Web application is configured in such a way that its resources and functions can only be accessed through pre-determined secure communication channels.
b. In the web application, access to unnecessary resources and functions is blocked and unnecessary HTTP methods are deactivated.
c. Cookie settings are configured to secure and SameSite. Session key cookies are configured to httponly.
d. When configuring, the following properties of a web application may be set and restricted:
- use of character encoding and automatic translation;
- disclosure of excessive security information in error messages and response messages;
- storing configuration files outside a root folder;
- permitted number of unsuccessful access attempts.

APP.3.1.M21 Secure HTTP configuration of web applications

a. To protect against clickjacking and cross-site scripting, a web application is configured with X-FRAME-OPTIONS: deny in the HTTP response header.
b. The web application supports the Content Security Policy (CSP) of the browser.

APP.3.1.M22 Inspection and penetration testing of web applications [head of information security]

a. The security of the web applications is checked and tested regularly.
b. The results of inspections and penetration testing are documented. They are considered confidential and stored in a safe manner.
c. Any deviations are handled and the results are reported to the head of information security.

3.4 Advanced measures

APP.3.1.M20 Web application firewalls (C-I-A)

a. Web application firewalls (WAFs) are used for the filtration of data on higher protocol levels.
b. The configuration of a web application firewall is adjusted to the web application to be protected.
c. After updating a web application, the configuration of web application firewall is checked and changed if necessary.

APP.3.2 Web server

1 Description

1.1 Purpose

To present measures for the protection of a web server and the data that is accessible through the web server.

1.2 Responsibility

The IT department is responsible for compliance with the web server measures.
Additional responsible persons: The compliance manager, the responsible specialist, the administrative department.

1.3 Limitations

The security aspects of the server that hosts the web server software are discussed in the modules of the module group SYS (IT Systems) (see also SYS.1.1 Server in general, SYS.1.3 Linux and Unix server, or SYS.1.2.2 Windows Server 2012).
The integration of a web server into the network architecture and protecting it with a firewall are presented in the modules NET.1.1 Network architecture and solution and NET.3.2 Firewall.
The module APP.3.1 Web applications describes the dynamic content and the additional functions of HTML.
The secure management of cryptographic keys is covered in the module CON.1 Cryptography concept.
Whenever external services are used for a web server, measures from the module OPS.2.1 Outsourcing are implemented.
The event logging of a web server is described in the module OPS.1.1.5 Logging.

2 Threats

2.1 Loss of reputation

If the attackers manage to manipulate a website and rearrange or deface it, it could damage the organisation's reputation. Publishing erroneous information (e.g. a misleading product description or politically motivated statement) could bring about the loss of the public reputation of the organisation.

2.2 Web server manipulation

An attacker who has gained access to a web server can manipulate files there, change the configuration of the web server and the web content, launch additional services, and install malware. An attacker might replace the files meant to be downloaded by the users with files that contain malware, for example. When the web server of the organisation is used for spreading malware, it could lead to the decline of the trustworthiness of the web server in reputational services and the unavailability of the web pages to users.

2.3 Distributed denial-of-service attack

An attacker can use a manipulated server for a distributed denial-of-service (DDOS) attack. In case of a distributed denial-of-service attack, the web server could be partially or completely incapacitated. In this case, the website is only barely usable or completely inaccessible for users. For many organisations (those with an online store, for example), this type of failure becomes business-critical quickly.

2.4 Leak of confidential data

Many web servers still use outdated encryption procedures, such as RC4 and SSL. Insufficient authentication and weak encryption might lead to attackers being able to eavesdrop on and alter the data exchange between the client computers and servers or between servers.

2.5 Violation of legislative requirements

The violation of legislative requirements (primarily data protection ones) could cause financial and reputational losses. There is also the danger of violating copyrights with the contents of the web server (e.g. when using images without permission).

2.6 Inadequate elimination of web server malfunctions

Malfunctions that occur during the web server operation affect the availability of the web server. The transmission of the web server content is interrupted, the operations of the user are not completed, and the security mechanisms could stop working. If the root causes are not dealt with consistently, then the problems with data security are going to continue.

3 Measures

3.1 Life cycle

Implementation

APP.3.2.M1	Secure configuration of the web server
APP.3.2.M2	Protection of web server files
APP.3.2.M20	Appointing a contact person

Operation

APP.3.2.M3	Security of file uploads and downloads
APP.3.2.M4	Event logs
APP.3.2.M5	Authentication
APP.3.2.M11	Encryption with TLS
APP.3.2.M12	Procedure for handling errors and error messages
APP.3.2.M13	Limiting access for bots
APP.3.2.M14	Integrity control and protection from malware
APP.3.2.M16	Penetration testing and inspection

Planning

APP.3.2.M7	Legality of publishing web content
APP.3.2.M8	Implementation plan for the web server
APP.3.2.M9	Security policy for the web server

Acquisition

APP.3.2.M10	Suitable web host

Additional advanced measures

APP.3.2.M15	Excess
APP.3.2.M18	Protection from denial-of-service attacks

3.2 Key measures

APP.3.2.M1 Secure configuration of the web server

a. After the installation of the web server, a secure baseline configuration has been created and documented.
b. The web server process is run with a user account that has minimal rights.
c. If the support from the operating system exists, the web server is run in an encapsulated environment. If the operating system does not support encapsulation, each web server is run in a separate virtual server or in a physically standalone server.
d. Web server services do not have excessive write permissions.
e. Superfluous modules and functions of the web server are deactivated.

APP.3.2.M2 Protection of web server files

a. Web server files (primarily scripts and configuration files) are protected from unauthorised reading and modification.

b. Web applications have access only to files in the required directory tree (in the web root folder). Resources outside the web root folder cannot be linked or connected to. The functions that present directories have been deactivated.
c. Files, the changing of which is prohibited, have write protection.
d. Confidential data is forwarded and saved in an encrypted manner.

APP.3.2.M3 Security of file uploads and downloads

a. Files published in the web server are checked for the absence of malware before publishing.
b. The published documents are cleaned before publication from residual data.
c. Downloaded files are saved in a separate location.
d. Volume limits have been set to files that are uploaded to the server by the users and the existence of sufficient storage room has been taken into account.

APP.3.2.M4 Event logs

a. As a minimum, the following events are logged in the web server:
- successful access to resources;
- failed access to resources due to incomplete privileges, absent resources, and server errors;
- general error messages.

b. Log data is analysed regularly.

APP.3.2.M5 Authentication

a. An encrypted connection is used for the authentication of client computers in the web server (see also APP.3.2.M11 Encryption with TLS).
b. When authenticating with a password, the password information is kept in the server in encrypted form and protected from unauthorised access.

APP.3.2.M7 Legality of publishing web content [responsible specialist, Compliance Manager]

a. The publication of contents for outside parties through a web server complies with data protection regulations.
b. When the web contents are published, copyright is taken into account.

APP.3.2.M11 Encryption with TLS

a. The web server allows the encryption of all connections with TLS. TLS and the HTTPS protocol are used for the protection of data communication in external networks.
b. In case of the HTTPS connection, the HTTPS is used without exception.

3.3 Standard measures

APP.3.2.M8 Implementation plan for the web server

a. A plan has been prepared for the implementation of the web server which documents the purpose of using the web server, the data to be presented, the target group of users, and the process of integration into the existing IT infrastructure.
b. Responsibilities for the technical management of the web server and the web content have been assigned to specific persons.

APP.3.2.M9 Security policy for the web server

a. A security policy for the web server, stipulating the measures and persons responsible for the information security of the web server, has been established and documented.
b. The security policy of the web server describes, among all else:

- acquiring information about known security vulnerabilities;
- the implementation of security controls for the web server;
- the procedure for handling security incidents.

APP.3.2.M10 Suitable web host

a. The organisation has concluded an agreement with an external service provider which stipulates the manner of providing the hosting service, the service level, and the security-related obligations of the parties.
b. The service provider has implemented technical and organisational security controls to protect their own IT system.
c. The service provider is obligated to react immediately to any technical problems that have occurred in the IT systems and when the client systems are jeopardised.

APP.3.2.M12 Procedure for handling errors and error messages

a. The name, version, and configuration of the software components of the web server are not revealed in the HTTP data and error messages.
b. The web server only forwards error messages about the application that are necessary to inform the user.
c. In the event of errors and malfunctions, the web server switches to a secure safety mode.

APP.3.2.M13 Limiting access for bots

a. Access of search robots to web content has been restricted with a robot exclusion protocol.
b. Technical measures are implemented to protect the web server content from bots (see also APP.3.2.M5 Authentication).

APP.3.2.M14 Integrity control and protection from malware

a. In order to detect unauthorised changes, the integrity of files and web contents is checked regularly.
b. The presence of malware in files is checked regularly.

APP.3.2.M16 Penetration testing and inspection

a. The security of the web server is checked with regular penetration testing and regular inspections.
b. The results of the tests and the inspections are documented and kept confidential.
c. The identified nonconformities are handled and the results are reported to the Head of Information Security.

APP.3.2.M20 Appointing a contact person [administrative department]

a. The organisation has appointed a contact person for solving web problems.
b. The organisation has published contact details for outside users for reporting web problems.

3.4 Advanced measures

APP.3.2.M15 Excess (A)

a. Web servers and their connections with other IT systems and the internet have been duplicated.

APP.3.2.M18 Protection from denial-of-service attacks (A)

a. The web server is constantly monitored to detect any denial-of-service attacks.
b. Measures for the prevention and alleviation of denial-of-service attacks have been implemented.

APP.3.3 File server

1 Description

1.1 Purpose

To present specific measures for running the file server securely.

1.2 Responsibility

The IT department is responsible for compliance with the file server measures.
Additional responsible persons: User.

1.3 Limitations

The general aspects of server security are discussed in the module SYS.1.1 Server in general and in the modules SYS.1.3 Unix server or SYS.1.2.2 Windows server 2012 of the module group SYS (IT Systems).
The security measures for storage systems and storage networks are presented in the module SYS.1.8 Storage solutions. This section also does not cover file server services (e.g. Samba).
The correct management of access rights (see also ORP.4 Administration of identity and rights) and functional data backup (see also CON.3 Data backup concept) are essential for ensuring the file server security.

2 Threats

2.1 File server malfunctions

If data or services are not available to users and applications due to a file server malfunction, it has a significant impact on the business processes of the organisation. This causes financial damage to the organisation and affects the activities of other organisations as well. If the disaster management

concept does not provide for a fast recovery of the file server, it prolongs the disruption time and the related costs even more.

2.2 Underdimensioned file server

When the network connection of the file server is slow or the storage volume of the file server is insufficient, it is difficult to guarantee the required availability of the data. As an additional threat, the employees might prefer to save their data in local computers. If several working copies of data are kept, then this might jeopardise the confidentiality and integrity of data. There is no certainty about which operations where conducted with the data last and who is the owner of the data.

2.3 Inadequate control of stored files

When the file server is not protected sufficiently from malware, an attacker might install malware there undetected. This enables unauthorised viewing or manipulating of the data that is kept in the file server. If there are many devices and applications that have access to the data in the file server, malware might spread very quickly to the entire organisation.

2.4 Absence or inadequacy of the concept of access rights

When the access rights and shared use of files is not sufficiently planned or implemented, it is possible to take advantage of the data access vulnerabilities to gain unauthorised access to the file server. An attacker can read, change, delete, or copy data.

2.5 Unstructured data management

If there is no procedure for data management or the employees do not comply with it, data is saved in the file server in a non-observable and uncoordinated manner. This causes misspending of storage resources caused by the high volume of data, unauthorised access to data (e.g. when files are kept in directories or file systems which are accessible to unauthorised persons) or the creation of unapproved file versions.

2.6 Loss of data stored in the file server

When a file server is placed in an easily accessible location, immediate access to its components and the data stored in the server becomes possible. An attacker could remove the hard disk or take it with them. A smaller network-attached storage could be stolen along with the data saved in it.

2.7 Ransomware

In case of ransomware infection, the data in IT systems is encrypted and the perpetrators promise to decrypt it after a ransom is paid. However, even after paying a ransom, the recovery of the data is not certain. Data that was added after the last backup could be lost due to the ransomware attack. If the data is not backed up, a ransomware attack could end the activity of the organisation in the worst-case scenario.

3 Measures

3.1 Life cycle

Implementation

APP.3.3.M2	RAID system
APP.3.3.M3	Antivirus programs
APP.3.3.M8	Structured data management

Planning

APP.3.3.M15	Preliminary analysis of the file server

Acquisition

APP.3.3.M6	Procedure for acquiring a file server
APP.3.3.M7	Selecting a suitable file system

Operation

APP.3.3.M9	Secure storage management
APP.3.3.M11	Implementation of quotas

Additional advanced measures

APP.3.3.M14	Use of error correction codes
APP.3.3.M12	Encryption of datasets
APP.3.3.M13	Duplication in another location

3.2 Key measures

APP.3.3.M2 RAID system

a. The organisation has analysed whether and which RAID system would be practical in the file server. The decision not to use a RAID system is documented along with the reasons.

b. The maximum length of recovery time of RAID and data has been determined.
c. In case of using hardware RAID, the RAID controller is duplicated in the server and hot-swappable hard disks are used.

APP.3.3.M3 Antivirus programs

a. When saving data in a file server, the data is checked for malware.

APP.3.3.M15 Preliminary analysis of the file server

a. A preliminary analysis has been conducted to implement a file server which determines the necessary functionality and limitations for the purpose of the server.
b. The storage volume of the server has enough reserves; the planned speed of data exchange and connectivity correspond to the purpose of the server.
c. A workstation is not used as the file server.

3.3 Standard measures

APP.3.3.M6 Procedure for acquiring a file server

a. In order to acquire a file server, a specification of requirements for the file server has been prepared for comparing the products.
b. The file server software and the services run on it have been selected based on the main goals for using the file server (e.g. file sharing, media streaming, disk image backups).
c. When acquiring a file server, its performance, storage volume, data exchange speed, and the potential number of users are taken into account.

APP.3.3.M7 Selecting a suitable file system

a. The criteria for evaluating the suitability of file systems is presented in the specification of requirements for the file server.
b. The journalling function has been applied to the file system to reverse or initiate transactions.
c. The file system has a defence mechanism for preventing file changes by several users or applications simultaneously.

APP.3.3.M8 Structured data management [user]

a. A specific directory structure has been developed for storing the data.
b. The users are aware of the procedure for storing data, including which data is saved locally and to which file servers.
c. The program data and work files are kept in separate directories.
d. Compliance with the requirements of structured data management is checked regularly.

APP.3.3.M9 Secure storage management

a. Accounts are kept of the file server resources.
b. The storage components are checked regularly to see whether they function in predetermined ways. Suitable backup components are available in case of malfunctions or running out of memory.
c. If a hierarchy of data storage (first-, second-, and third-level storage) has been established, the management procedures for (semi-)automatic storage have been prepared.
d. The functioning of the automatic data storage is checked regularly.
e. Security events of the data storage (unauthorised access attempts, changing access rights) are logged.

APP.3.3.M11 Implementation of quotas

a. File server quotas (storage limits) are set for the users. As an alternative solution, the user is warned about running out of disk space and the write permission is given only to the system administrator.

APP.3.3.M14 Use of error correction codes

a. A file system that enables error detection or error correction methods is implemented (such as ZFS). When acquiring a file server, the need for additional space is taken into account.
b. When using error codes, it is taken into account that detecting and correcting such errors only works to a limited extent.

3.4 Advanced measures

APP.3.3.M12 Encryption of datasets (C-I-A)

a. All data stored in a file server is encrypted on the level of hardware or the file system. In case of hardware encryption, only certified products are used.
b. The antivirus software is capable of checking encrypted files as well.

APP.3.3.M13 Duplication in another location (A)

a. In case of a need for high availability, the data is duplicated into several devices and to different locations.
b. A suitable duplication mechanism is chosen for the duplication of data.
c. Time services with sufficient accuracy are used.

APP.3.4 Samba

1 Description

1.1 Purpose

To present measures for the secure use of Samba protocols and methods and the protection of Samba data.

1.2 Responsibility

The IT department is responsible for the compliance with the Samba measures.

1.3 Limitations

The security controls of the Linux server that runs Samba are presented in the modules SYS.1.1 Server in general and SYS.1.3 Linux and Unix server.
The security controls of printing, file, and directory services that are implemented through Samba are described in the modules SYS.4.1 Printer and multifunction printer, APP.3.3 File server, APP.2.1 Directory service in general, and APP.3.6 DNS server, APP.2.2 Active Directory, and APP.2.3 OpenLDAP.
Access rights management is covered in the module ORP.4 Administration of identity and rights.

2 Threats

2.1 Eavesdropping on the insecure connections of Samba

If insecure protocols are used for sending files between Linux servers, Windows servers, and clients, Samba data connections can be intercepted and it is possible to eavesdrop on them. An attacker can use the authentication and user data collected in this manner to steal the sensitive information of the organisation.

2.2 Insecure default settings of Samba

If the security of the configuration is not increased after installing a Samba server and Samba is run in the smb.conf default settings of the configuration file, it could cause significant security issues.

2.3 Unauthorised use or management of Samba

The use or management of Samba by unauthorised users enables access to confidential data, allows its manipulation, or cause service malfunctions of Samba. Configuration tools, such as the Samba Web Administration Tool, often fail to pay sufficient attention to the use of security mechanisms. For this reason, weaker security mechanisms are implemented or they are completely absent (for example, they do not support HTTPS).

2.4 Incorrect management of Samba

When the system administrators are not sufficiently familiar with the extensive functionality of Samba, the selection of Samba components, and its configuration settings, the configuration errors of DNS or user rights management could enable unauthorised persons to access the server resources. In addition, incorrect management could cause interruptions in the IT systems and business processes.

2.5 Data loss in Samba

The Windows and Unix file systems have different properties. For this reason, it is not guaranteed that the access rights of Unix are preserved in Windows. This might result in data loss caused by enabling unauthorised access. Due to the differences in the systems, ADS and DOS attribute data might be lost. If this information is used in the IT systems, the differences in the operating systems might cause malfunctions in the business processes.

2.6 Loss of data integrity in Samba

When using Samba, it is important to maintain the integrity of the Samba databases of important usage data that is kept in the TDB format (Trivial DataBase). If the operating system cannot run these databases with sufficient capacity, the Samba services might be prone to malfunctions.

3 Measures

3.1 Life cycle

Planning

APP.3.4.M1 Samba server implementation plan

APP.3.4.M4 Avoiding NTFS functions in the Samba server

Implementation

APP.3.4.M2 Secure basic configuration of the Samba server

APP.3.4.M3 Secure configuration of the operating system of the Samba server

APP.3.4.M5 Secure access settings of the Samba server

APP.3.4.M6 Secure configuration of Winbind in the Samba environment

APP.3.4.M7 Secure configuration of DNS in the Samba environment

APP.3.4.M8 Secure configuration of LDAP in the Samba environment

APP.3.4.M9 Secure configuration of Kerberos in the Samba environment

APP.3.4.M12 Training of Samba server administrators

Operation

APP.3.4.M10 Secure implementation of external programs in the Samba server

Emergency response

APP.3.4.M13 Regular backups of the important system components of the Samba server

Additional advanced measures

APP.3.4.M15 Encryption of Samba data packets

3.2 Key measures

APP.3.4.M1 Samba server implementation plan

a. Before the implementation of a Samba server, the following is decided and documented:

- the tasks that the Samba server is going to perform;
- the operating mode of Samba;

• the authentication process;
• the characteristics of the Samba operational environment;
• the necessary Samba and other components.

b. The following Samba components have been thoroughly tested:
• cluster solution CTDB (Cluster Trivial Database);
• AD (Active Directory) services for the Linux and Unix systems;
• AD authentication procedure;
• VFS (Virtual File System) modules and the order of implementing them;
• IPv6 protocol in Samba.

APP.3.4.M2 Secure basic configuration of the Samba server

a. The security of the settings that regulate access and affect server capacity has been increased during configuration.
b. Samba is configured to connect to secure hosts and networks only.
c. Any changes to configuration, the persons making the changes, and the reasons for such changes are documented.
d. The correctness of syntax is checked after each change.
e. No additional software (such as SWAT) has been installed.

3.3 Standard measures

APP.3.4.M3 Secure configuration of the operating system of the Samba server

a. The databases in TDB formats are not kept in a partition that uses the ReiserFS file system.
b. In case of shared use (Netlogon), unauthorised users cannot change files in common use.
c. The operating system and the file system of the Samba server support the access control list (ACL) of the file system.
d. The SMB message signing settings comply with the security policy of the information network.
e. Kerberos is used for avoiding the abuse of the vulnerabilities of NT LAN Manager (NTLM) or NTLMv2 and an excessive network load.

APP.3.4.M4 Avoiding NTFS functions in the Samba server

a. If the NTFS ADS data flows are used due to the Samba server, then before sending the file system objects, their contents are checked for important ADS information.

APP.3.4.M5 Secure access settings of the Samba server

a. In order to map the DOS attributes in the Linux file system, extended attributes of the file system are used instead of the Samba default parameters.
b. Access to the Samba service ports is only allowed from an internal network.
c. The access rights and log data of the Samba server are checked regularly.

APP.3.4.M6 Secure configuration of Winbind in the Samba environment

a. If user accounts are not created for the users of the Windows domain in the operating system of the server, then winbind is used for converting the domain usernames into Linux usernames. At that, conflicts with the local Linux users and domain users is avoided.
b. PAMs (Pluggable Authentication Modules) are used for supporting authentication.

APP.3.4.M7 Secure configuration of DNS in the Samba environment

a. When implementing Samba as a DNS server, its configuration should be tested before the implementation.
b. DNS is configured according to the usage scenario of Samba.

APP.3.4.M8 Secure configuration of LDAP in the Samba environment

a. If the Samba users are managed with LDAP, it is carefully planned and implemented with the help of access control lists (ACL).

APP.3.4.M9 Secure configuration of Kerberos in the Samba environment

a. In order to authenticate with Samba, MIT or Heimdal Kerberos KDC (Key Distribution Centre) have been implemented along with the configuration file adjusted for Kerberos.
b. When authenticating with Kerberos, the central time server is located in the local domain controller. The time queries of the NTP service are only made available to the authorised clients.
c. The encryption mechanisms of Kerberos tickets are sufficiently strong.

APP.3.4.M10 Secure implementation of external programs in the Samba server

a. Samba initiates only verified and trustworthy external programs.

APP.3.4.M12 Training of Samba server administrators

a. The administrators of the Samba server have completed a training on specific topics related to Samba, such as the authentication of users, user rights models in Windows and Unix as well as NTFS access control lists and ADS.

APP.3.4.M13 Regular backups of the important system components of the Samba server

a. The system components and backend systems necessary for the recovery of the Samba server are included in the data backup concept for the entire organisation.
b. The backup also includes all TDB files.

3.4 Advanced measures

APP.3.4.M15 Encryption of Samba data packets (C-I)

a. The Samba data packets are encrypted with the methods in the newer versions of the SMB protocol (starting from SMB v3).

APP.3.6 DNS server

1 Description

1.1 Purpose

To present measures for the secure use of the internal and external DNS servers of the organisation.

1.2 Responsibility

The IT department is responsible for the implementation of DNS server measures.
Additional responsible persons: Administrative department.

1.3 Limitations

When implementing a module, the measures of the module SYS.1.1 Server in general and either SYS.1.3 Linux and Unix server or SYS.1.2.2 Windows Server 2012, depending on the operating system of the DNS server, should also be applied.

2 Threats

2.1 Malfunction of the DNS server

In case of DNS server malfunctions, other servers of the clients of the organisation can no longer resolve addresses. Connections between servers cannot be established and external IT systems (such as mobile employees, clients, and business partners) also do not have access to internal servers of the organisation. Significant business processes could be disrupted.

2.2 Insufficient capacity of the DNS server

If the DNS server cannot process queries with sufficient capacity, the access times of internal and external services might be extended, the availability of services be interrupted, and an attacker would find it easier to overload the DNS server with a denial-of-service attack.

2.3 Inadequate planning of the implementation of DNS

The inadequate implementation of DNS might create security vulnerabilities which could be instrumental in the success of any attacks against the DNS server. When the firewall rules that enable DNS network traffic are too lenient, it could facilitate unauthorised access to the DNS server. However, if the rules are too restrictive, trustworthy clients cannot send queries to the DNS server, which interrupts the use of services (such as email, FTP, etc.).

2.4 Incorrect domain information

Human error could lead to semantically and/or syntactically incorrect domain information. An error occurs when the wrong IP address is linked to a host name, the necessary data is not entered, or forbidden characters are used, for example. If name resolving is implemented inconsistently, it could lead to errors in the services that use this data, depending on which source is used for the DNS resolving.

2.5 Incorrect configuration of the DNS server

When default settings are not changed or errors have been made during configuration, it could create security vulnerabilities in the DNS server or interruptions in the functioning of the server. If the DNS server is configured to accept recursive queries from the intranet without any restrictions, it could affect the availability of the server significantly due to a larger load. A configuration error of the DNS server makes the server vulnerable to a DNS reflection attack.

2.6 DNS manipulation

DNS spoofing (DNS cache poisoning) is used for creating a situation where the server under attack saves the erroneous connections between the IP addresses and names. This means that the fact that the DNS servers save domain information in a cache for a certain period is exploited. When queries are submitted to a manipulated DNS server, it sends forged data in response. The client device saves the response in its cache, 'poisoning' it as well. If a DNS resolver submits a query about a manipulated address, it is only presented to some other DNS server after the time to live (TTL) of the data has ended. So it is possible that the manipulated DNS information is stored for a long time even if the errors are already fixed in the DNS server that was attacked first.

2.7 DNS hijacking

DNS hijacking (DNS redirection) is a method of attack which is used for directing the communication between the DNS servers and resolvers through the IT system of an attacker. Such man-in-the-middle attacks allow an attacker to eavesdrop on and record the communication between servers. A much larger threat is an attacker being able to change the traffic of both communication partners at will. If a query from the DNS resolver of the client's IT system is sent to a DNS server after a DNS hijacking attack, an attacker can change links between the names and IP addresses for a small number of query submitters and under limited conditions. DNS spoofing can also be combined with other types of attacks (particularly phishing).

2.8 DNS amplification attack

In case of a DNS amplification attack, such a large amount of queries is sent to the server that they overload the network connection of the DNS server itself. In order to send a large amount of queries at the same time, the queries are usually created by a botnet. An overloaded DNS server can no longer answer queries.

2.9 DNS reflection attack

A DNS reflection is a denial-of-service attack that is not targeted at the DNS server that the queries are sent to, but instead at the sender of the queries. This attack takes advantage of the fact that certain attacks create a relatively large amount of response data. At that, it is possible to achieve more than a hundred-fold gain. Due to the number and volume of response, the network or computer is burdened to its maximum capacity. The targets of an attack could be various technical IT components. A DNS reflection attack is facilitated by external network DNS resolvers.

3 Measures

3.1 Life cycle

Planning

APP.3.6.M1	Implementation plan for DNS
APP.3.6.M8	Domain name management
APP.3.6.M11	Sufficient dimensioning of the DNS server
APP.3.6.M17	Implementing the DNSSEC extension

Emergency response

APP.3.6.M2	Duplication of the DNS server
APP.3.6.M9	Emergency plan for the DNS server

Implementation

APP.3.6.M3	Separate DNS servers for internal and external queries
APP.3.6.M4	Secure basic configuration of the DNS server
APP.3.6.M6	Security of dynamic DNS updates
APP.3.6.M13	Limiting the visibility of domain data
APP.3.6.M14	Separating DNS servers

Operation

APP.3.6.M7	DNS server monitoring
APP.3.6.M15	Log data analysis
APP.3.6.M16	Correct placement of a DNS server in the P-A-P architecture
APP.3.6.M18	Increasing the security of a zone transfer

Acquisition

APP.3.6.M10	Server that is suitable for use as a DNS server

Disposal

APP.3.6.M19 Secure decommissioning of the DNS server

Additional advanced measures

APP.3.6.M20 Feasibility check of the emergency plan

APP.3.6.M21 Hiding the primary DNS server

APP.3.6.M22 Connecting the DNS server with several suppliers

3.2 Key measures

APP.3.6.M1 Implementation plan for DNS

a. When planning the implementation of DNS, the following is decided and documented:

- the structure of the DNS service;
- the domain information to be protected;
- the manner of integrating DNS servers;
- user roles related to the DNS services.

APP.3.6.M2 Duplication of the DNS server

a. The DNS advertiser is duplicated with another DNS server.

APP.3.6.M3 Separate DNS servers for internal and external queries

a. The DNS advertiser and the DNS resolver are in physically separate servers.
b. The internal IT systems use the internal DNS resolvers of the organisation for reverse resolving.

APP.3.6.M4 Secure basic configuration of the DNS server

a. The DNS server that services the internal network is configured to only process queries from the internal network. Random source ports are used for sending queries.
b. If the DNS servers that send erroneous domain information are known, access to them is restricted.
c. A DNS advertiser is configured to handle queries from the internet iteratively.
d. Forwarding zone information is only permitted between the primary server and secondary server(s) and limited based on IP addresses.
e. The version number of the DNS server is concealed.

APP.3.6.M6 Security of dynamic DNS updates

a. The domain information in the internal DNS servers can only be changed by authorised IT systems.
b. The type of domain information that can be changed by the IT systems has been determined.

APP.3.6.M7 DNS server monitoring

a. The DNS server is constantly monitored to detect malfunctions or anomalies.
b. The DNS server load is monitored to increase the capacity of hardware in case of an overload.
c. As a minimum, the following security events are logged in the DNS server:
- unsuccessful DNS queries;
- EDNS (Extension Mechanisms for DNS) errors;
- invalid and unsuccessful zone transfers.

APP.3.6.M8 Domain name management [administrative department]

a. The organisation's domains are registered regularly and extended in a timely manner.
b. An employee has been appointed as the person responsible for the management of the internet domain names.
c. The organisation maintains control of its registered domain names even when a service provider is used for domain management.

APP.3.6.M9 Emergency plan for the DNS server

a. An emergency plan has been prepared for the DNS server which complies with the existing emergency plans and the sustainability plan of the organisation (see also DER.4 Emergency management).
b. The emergency plan includes a procedure for backing up master and configuration files, which is integrated into the existing data backup concept of the organisation.
c. The emergency plan also contains the DNS server recovery plan.

3.3 Standard measures

APP.3.6.M10 Server that is suitable for use as a DNS server

a. Using the chosen DNS server solution has sufficiently justified itself in practice.
b. The DNS server complies with the valid RFC standard.
c. The DNS server supports the creation of syntactically correct master files.

APP.3.6.M11 Sufficient dimensioning of the DNS server

a. The DNS server resource guarantees sufficient capacity for fulfilling its function.
b. The DNS server is only used for running the DNS server service.
c. The network connection of the DNS server has adequate bandwidth.

APP.3.6.M13 Limiting the visibility of domain data

a. When using the same domain name, the namespace of the domain is clearly divided into public and internal parts.
b. The public part only includes the domain information that is necessary for services which are externally accessible.
c. The DNS names that are internal to the intranet IT systems which have a public IP address cannot be solved from an external network.

APP.3.6.M14 Separating DNS servers

a. The primary and secondary DNS advertisers are located in separate network segments.

APP.3.6.M15 Log data analysis

a. The log files of the DNS server and its operating system are checked and analysed regularly.
b. As a minimum, the following log data is analysed:
- the number of DNS queries;
- the number of unsuccessful DNS queries and reasons for errors;
- the ratio of unsuccessful DNS queries and their dynamics;
- the reasons for unsuccessful zone transfers.

APP.3.6.M16 Correct placement of a DNS server in the P-A-P architecture

a. The traffic between the DNS advertiser and DNS solver is filtered with the packet filters and application level gateway (ALG) of the P-A-P architecture (packet filter - application level gateway - packet filter).

b. Only DNS traffic is possible between the DNS servers.
c. If an external service provider manages the domain name, the domain information is revealed to them only to the minimum extent necessary.

APP.3.6.M17 Implementing the DNSSEC extension

a. The DNSSEC protocol extension is activated in all DNS servers.
b. Key signing keys (KSK) and the zone signing key (ZSK) are managed securely and changed regularly or when the key is revealed.

APP.3.6.M18 Increasing the security of a zone transfer

a. Transaction signatures (TSIG) are used for protecting zone transfers.

APP.3.6.M19 Secure decommissioning of the DNS server

a. When decommissioning a DNS server, the storage media of the server are deleted in a secure manner.
b. When a DNS server is decommissioned, the name and IP address of the server is deleted from all configuration files within the organisation and in these of the service providers.

3.4 Advanced measures

APP.3.6.M20 Feasibility check of the emergency plan (A)

a. The feasibility of the emergency plan is checked regularly.

APP.3.6.M21 Hiding the primary DNS server (C-I-A)

a. The external primary DNS advertiser uses a hidden master so that the server becomes invisible in the DNS zone data and inaccessible externally.

APP.3.6.M22 Connecting the DNS server with several suppliers (I-A)

a. When registering a domain name, at least two domain name servers of an external network are used (primary and secondary).
b. The primary and secondary DNS servers are located in separate networks and are connected through different service providers.

APP.4 Business applications

APP.4.3 Database systems

1 Description

1.1 Purpose

To present measures for the secure planning, creation, and operation of relational database systems and for the protection of information that is processed in the databases.

1.2 Responsibility

The IT department is responsible for the compliance with the measures for relational database systems.
Additional responsible persons: Developer, responsible specialist.

1.3 Limitations

The module does not cover the security measures for non-relational database systems. The module also does not discuss secure development of applications, database structure, and security measures regarding access. Moreover, the model does not describe security measures for the operating system and hardware of the database server; these are presented in the SYS module group modules SYS.1.3 Linux and Unix server or SYS.1.2.2 Windows Server 2012.
Additionally, the measures of relational databases from the modules ORP.4 Administration of identity and rights, OPS.1.1.3 Patch and change management, CON.3 Data backup concept, OPS.1.1.2 IT management, and OPS.1.1.5 Logging are implemented.

2 Threats

2.1 Inadequacy of system resources

When the capacity and resources of the hardware that runs the database management system (DBMS) are insufficient, the database might encounter malfunctions (e.g. it is no longer able to store

data). In addition, the system resources might be overloaded during rush hours, causing the application to work more slowly or stop functioning altogether.

2.2 Continued use of default accounts

When a database management system is first installed, the user or administrator accounts are often unprotected or protected with publicly known passwords. This means that the accounts might be abused (e.g. an attacker can log into the database management system as a user or even as a system administrator). The attacker would be able to read the configuration or stored data and manipulate or delete it.

2.3 Unencrypted data exchange

In typical settings, many database management systems do not use encryption for establishing a connection with a database. However, if the communication between applications and databases is unencrypted, the authentication data and the forwarded data can be read or manipulated.

2.4 Data loss in the database

The data might be lost from a database due to hardware and software malfunctions and human errors. As databases are usually used for storing information that is important for running applications, it could lead to a disruption in providing a service or in the entire business process.

2.5 Loss of data integrity

The integrity of data that is stored in the database system could be impaired by databases that are configured incorrectly, software errors, or data manipulation. If the loss of integrity is not noticed or is noticed too late, it could hinder the main processes of the organisation greatly.

2.6 SQL injection

An SQL injection is a widespread method of attacking databases. If an application has access to data stored in a SQL database and the input data is insufficiently validated, an attacker could initiate their own SQL commands through the rights of the administrative account which facilitate reading and manipulating data. An attacker could add new data or initiate system commands.

2.7 Insecure configuration of the database management system

Often, unnecessary functions are activated in the typical configuration of a database system which helps an attacker to read or manipulate data that is stored in the database. For example, an attacker could use an application interface that was installed during a typical installation but is not used in the organisation to manage the database management system without authentication. This way, they gain unauthorised access to the databases of the organisation.

2.8 Malware and insecure scripts

Many database management systems can automate operations with database scripts and database triggers which are launched in the context of the database (e.g. PL/SQL). Uncontrolled use of scripts and any non-compliance with the software development requirements of the organisation could jeopardise data security.

3 Measures

3.1 Life cycle

Planning

APP.4.3.M1 Security guidelines for the database system

Operation

APP.4.3.M3 Increasing the security of the database management system

APP.4.3.M13 Restrictions on linked databases

APP.4.3.M17 Organisation of data loading or migration

APP.4.3.M18 Monitoring the database system

APP.4.3.M19 Avoiding low-quality scripts

APP.4.3.M20 Regular inspection

Implementation

APP.4.3.M4 Regulating the implementation of new databases

APP.4.3.M11 Hardware dimensioning

APP.4.3.M12 Typical configuration of a database management system

APP.4.3.M16 Encryption of database connections

Emergency response

APP.4.3.M9 Database system backup

Additional advanced measures

APP.4.3.M21	Database security instruments
APP.4.3.M22	Emergency response
APP.4.3.M23	Archiving
APP.4.3.M24	Encryption in the database
APP.4.3.M25	Security audit of the database system

3.2 Key measures

APP.4.3.M1 Security guidelines for the database system

a. Based on the general information security policy of the organisation, security guidelines for the database system are prepared, which establish the requirements for the secure use of the database.
b. Persons responsible for the management of databases are familiar with the security guidelines for the database system and comply with it in their work.
c. Any deviation from the requirements of the guidelines is documented and the Head of Information Security is informed thereof.
d. Compliance with the security guidelines of the database system is checked regularly and the results are documented.

APP.4.3.M3 Increasing the security of the database management system

a. A checklist of the measures for strengthening the database management system has been prepared.
b. The implementation of the strengthening measures and their up-to-dateness is checked regularly and the checklist is adjusted if necessary.
c. The passwords of the database are not stored as cleartext.

APP.4.3.M4 Regulating the implementation of new databases

a. A procedure has been established for the creation and implementation of databases.
b. The information on the database to be implemented is documented in the agreed format.

APP.4.3.M9 Database system backup

a. The database system and its data is backed up regularly.
b. The database system is also backed up before creating a database, using the required utility.
c. The parameters for restoring a database are established based on the protection requirement of the

data (see also CON.3 Data backup concept).
d. If the volumes planned for data backup are exceeded, changing the data backup concept is considered (such as implementing incremental backup).

3.3 Standard measures

APP.4.3.M11 Hardware dimensioning [responsible specialist]

a. A database management system is installed onto hardware with sufficient resource reserves.
b. When dimensioning hardware, the presumed growth of requirements and volumes during the planned utilisation period is taken into account.
c. The use of resources is monitored. The lack of resources can be noticed and solved in good time.

APP.4.3.M12 Typical configuration of a database management system

a. A harmonised typical configuration has been prepared for the database management systems.
b. Any deviations from the typical configuration are approved by the head of information security and documented.
c. The typical configuration of the database management is checked and adjusted regularly if necessary.

APP.4.3.M13 Restrictions on linked databases

a. Only authorised persons have the right to create database links (DB links).
b. The database links are documented and they are checked regularly.
c. Private database links are preferred instead of public database links (a link can be used with the user account under which the link was created).
d. Database links are taken into consideration when backing up the database system (see also APP.4.3.M9 Database system backup).

APP.4.3.M16 Encryption of database connections

a. A database system is configured to encrypt all database connections.
b. The encryption procedures and encryption mechanisms correspond to the protection requirement (see also CON.1 Cryptography concept).

APP.4.3.M17 Organisation of data loading or migration [responsible specialist]

a. Procedures for loading data and migration thereof to a database have been prepared.
b. After loading or migrating, the integrity of the transferred data is checked.

APP.4.3.M18 Monitoring the database system

a. Important parameters, events, and states that are important for the secure use of the database management system have been defined.
b. Application-specific parameters, events, and their threshold values are coordinated with the persons responsible for the applications (see also APP.4.3.M11 Hardware dimensioning).
c. The established parameters and events are monitored; the persons responsible are notified when threshold values are exceeded.

APP.4.3.M19 Avoiding low-quality scripts [developer]

a. Quality criteria have been established for the development of database scripts (see also CON.5 Development and implementation of applications).
b. Before the implementation of a database script, functional testing is conducted and the results are documented.

APP.4.3.M20 Regular inspection

a. The implementation of security controls of each component of the database system is checked regularly.
b. The inspection verifies whether:
- the documented state corresponds to the actual state;
- the configuration of the database management system complies with the documented typical configuration;
- the database scripts are necessary and comply with the quality standard of the organisation;
- appropriate action has been taken in case of anomalies in the database management system logs (see also DER.1 Detection of security incidents).

c. The results of the inspection are documented.
d. Any deviations are handled in accordance with the established procedure.

3.4 Advanced measures

APP.4.3.M21 Database security instruments (C-I)

a. Additional security products are used for the protection of databases which enable: • preparing reports on database security • additional options for the configuration of the database and rights management • detecting and avoiding attacks (e.g. a brute-force attack on a user account, SQL injection) • supporting audits (e.g. for checking the security of a configuration)

APP.4.3.M22 Emergency response (C-I-A)

a. An emergency plan has been prepared for action in case of a database system incident and for restoring the normal status of databases.
b. The emergency plan for database management determines the procedures for emergency management, notification routes, required notification times, the necessary resources, and persons responsible (see also DER.4 Emergency management).
c. The emergency plan takes into consideration all the needs of the IT systems that depend on the database.

APP.4.3.M23 Archiving (I-A)

a. An archiving plan of the database system has been prepared for archiving the data in the database system.
b. The archiving plan establishes the methods of archiving, archiving intervals, and the storage periods for the archived data.
c. The recovery of the archived data is practised regularly and the results are documented.

APP.4.3.M24 Encryption in the database (C)

a. The data kept in the database is encrypted (see also CON.1 Cryptography concept).
b. The following factors are taken into account when encrypting a database:
- its effect on performance;
- key management processes and the feasibility of the key management measures;
- its effect on data backup and recovery;
- its effect on functionality (e.g. using sorting).

APP.4.3.M25 Security audit of the database system (C-I-A)

a. The implementation of the security controls of the database systems is audited regularly.
b. When auditing, the technical and practical aspects of the database infrastructure (such as the

directory services) and the database management system specific to the product are taken into account.

APP.4.4 Kubernetes

1 Description

1.1 Purpose

Presenting measures used for the automation and management of containerisation and for the protection of the data in the Kubernetes cluster. The Kubernetes cluster consists of the nodes which include the container runtime. The smallest object orchestrated by Kubernetes is a container or a group of containers (hereinafter referred to as the pod) installed in one operation system. Kubernetes is a de facto standard solution for the orchestration of containers in public as well as private clouds.

1.2 Responsibility

The IT department is responsible for the implementation of the security measures of Kubernetes.
Additional responsible persons: No additional responsible persons.

1.3 Limitations

The module covers the measures related to the deployment, implementation, and administration of Kubernetes, including the measures for specialised hardware components, such as CNI (Container Network Interface) and CSI (Container Storage Interface).
The measures of this module are always discussed together with the measures from the module SYS.1.6 Containerisation.
In implementing the measures, it is not important which container runtime (e.g. Docker, runC, containerd, Windows Container) is used.
The security measures of the IT services operating in the Kubernetes cluster are specified in the modules on the respective services (e.g. APP.3.2 Web server).

2 Threats

2.1 Errors in the authentication and authorisation at the control plane of Kubernetes

The control plane of Kubernetes includes the applications used for the orchestration of the Kubernetes nodes, runtimes, and clusters. Access with administrator rights (privileged access) is required for working on the control plane of Kubernetes. Privileged accesses are mostly realised through designated network ports or Unix Socket.

2.2 Loss of confidentiality of the token of a pod

Pods require tokens for communicating with the Kubernetes control plane. As a result of an attack on a pod, the token may end up in the possession of the attacker. Then, the attacker can create a connection with the Kubernetes control plane and, if there are sufficient powers, make unauthorised changes in the settings or orchestration of the control plane.

2.3 Conflict of resources caused by a pod

One pod may, as a result of a conflict of resources, overburden the node in which the pod is located or prevent the entire orchestration of Kubernetes. A conflict of resources may put to risk the accessibility of other pods from the pod in question or prevent the normal functioning of the node.

2.4 Unauthorised changes in the Kubernetes cluster

For automation via CI/CD (Continuous Integration / Continuous Delivery) tools, the tools must be granted privileged rights for operations in the cluster. The use of such privileged rights comes with the risk of unauthorised changes being made in the Kubernetes cluster. For example, a developer may install a new version of an application in the cluster which has not been tested sufficiently or which has not been properly approved for use.

2.5 Unauthorised access to a pod

All pods have the capability to communicate with one another, with the nodes in the cluster, and with other IT systems. A malware application or an attacker can use a lack of restrictions on data exchange for attacking the Kubernetes control plane or other pods or nodes.

3 Measures

3.1 Life cycle

Planning

APP.4.4.M1	Designing the partition of applications
APP.4.4.M2	Automation of the development of applications with the help of CI/CD
APP.4.4.M3	Planning the Kubernetes identity and rights management

Implementation

APP.4.4.M4	Partition of pods
APP.4.4.M6	Secure resetting of the pods
APP.4.4.M7	Partition of Kubernetes networks

Operation

APP.4.4.M5	Backup of cluster information
APP.4.4.M8	Security of the Kubernetes configuration files
APP.4.4.M9	Security of the Kubernetes service accounts
APP.4.4.M10	Security of the automation process
APP.4.4.M11	Monitoring the use of containers
APP.4.4.M12	Security of infrastructure applications

Additional advanced measures

APP.4.4.M13	Automatic configuration audits
APP.4.4.M14	Use of specialised nodes
APP.4.4.M15	Partition of applications at the levels of nodes and clusters
APP.4.4.M16	Use of Kubernetes operators
APP.4.4.M17	Certification of nodes
APP.4.4.M18	Microsegmentation
APP.4.4.M19	Guaranteeing the high availability of Kubernetes
APP.4.4.M20	Encryption of the control plane storage space
APP.4.4.M21	Periodic restarting of the pods

3.2 Key measures

APP.4.4.M1 Designing the partition of applications

a. Before the installation of applications in the operational environment, the partition of the application installed in the pod from other applications and from its testing and development environments is designed.

b. The architecture of namespaces, meta tags, clusters, and networks is defined and the need for using virtual servers is identified based on the protection requirements of applications and the

potential risks.
c. Rules are drawn up for the partitioning of the network, CPU, and read-only memory in the course of designing.
d. Applications are partitioned based on the general network architecture of the organisation and the zoning principles of the network.
e. All applications and all programs related to the applications are designed to operate in the namespace of Kubernetes.
f. Each Kubernetes cluster only includes applications with similar protection requirements and similar potential attack vectors.

APP.4.4.M2 Automation of the development of applications with the help of CI/CD

a. The automation of the development of Kubernetes applications with the help of CI/CD (Continuous Integration / Continuous Delivery) involves the entire life cycle of an application from designing to removal from use (incl. development, testing, operating, monitoring, and the installation of updates).
b. Designing CI/CD involves defining the required roles and the minimum rights/powers needed.
c. Planning the automation process involves defining how the data processes in the applications of Kubernetes will be protected.

APP.4.4.M3 Planning the Kubernetes identity and rights management

a. All users of Kubernetes and control plane applications are authenticated. The powers granted to the users of Kubernetes only allow them to perform the operations required for fulfilling their task.
b. The software used in the automated environment is authenticated and only the required rights are granted to the software. The authentication and authorisation processes are performed irrespective of whether the operations are executed via the customer, a web interface, or an application programming interface (API).
c. Only personalised users may perform administrative operations in Kubernetes, no anonymous operations are permitted. Only a small circle of employees can define and change automation processes.
d. Only designated managers can create or change the persistent volumes of Kubernetes.

APP.4.4.M4 Partition of pods

a. In the kernel of the operation system of a node, isolation mechanisms are used to restrict the visibility of the resource consumption of the pods (e.g. Linux namespaces and cgroups).
b. Partition of the pods includes at least process IDs, interprocess data exchange, user IDs, the file system, and the network (incl. hosting).

APP.4.4.M5 Backup of cluster information

a. Cluster information is backed up periodically. A back-up copy must at least include the following:
- persistent volumes;
- the configuration files of Kubernetes and other control plane programmes;
- the state information of the Kubernetes cluster (incl. extensions);
- the configuration databases (especially etcd);
- all infrastructure applications which are required for the functioning of the cluster and the services included therein;
- the details of the code and image registries.

b. If possible, snapshots of the operation of the applications are also backed up, but snapshots may not be the only backup method used.

3.3 Standard measures

APP.4.4.M6 Secure resetting of the pods

a. The applications of pods are reset in a special init container.
b. Resetting an application closes all ongoing processes. Other Kubernetes containers are only activated after the successful resetting of the application.

APP.4.4.M7 Partition of Kubernetes networks

a. The administration networks of the nodes and the individual networks of the control plane and application services are partitioned.
b. Only the ports required for the functioning of the pod are open in the network of pods.
c. If the Kubernetes cluster contains several applications, the network connections between the Kubernetes namespaces are blocked by default. The network connections required for operation are whitelisted as and when needed.
d. The network ports required for the management of the nodes, the operational environment, and Kubernetes (incl. extensions thereof) are only accessible from the administrative network and from

designated pods.
e. Only designated administrators have the rights to change the management and network rules of Kubernetes CNIs.

APP.4.4.M8 Security of the Kubernetes configuration files

a. The configuration files of the Kubernetes cluster (incl. the configurations of all extensions and applications) are equipped with serial numbers and explanations.
b. The access rights to the software used for the management of the configuration files are as limited as possible. The read and write permissions of the control plane configuration files are regulated especially carefully.

APP.4.4.M9 Security of the Kubernetes service accounts

a. The service account specified under the default settings is not used in pods, the rights of this account have been removed.
b. Separate service accounts have been created for the pods of different applications. The rights of the service accounts are limited to the minimum rights required.
c. Those pods which do not require a service account do not have one. Such pods use tokens for communicating with the Kubernetes control plane.
d. Service accounts with privileged rights are only used in the pods of the control plane and those pods which inevitably require a privileged account.
e. Automation applications use tokens even if a shared service account could be used to perform a similar task.

APP.4.4.M10 Security of the automation process

a. All automation software processes, incl. CI/CD and the pipelines thereof, only operate based on the minimum rights required.
b. Changing the configuration of a pod or activating a pod through automation software is only permitted for authorised users.

APP.4.4.M11 Monitoring the use of containers

a. Container activation health checks as well as the interval of conducting the checks appropriate for the respective application or service have been established and configured for the containers of pods.

b. Kubernetes is capable of closing or restarting the pods depending on the results of the health check.

APP.4.4.M12 Security of infrastructure applications

a. If images are used in automation, hard drive management, or backing up of configuration files, at least the following has been taken into consideration:

- the access rights of personalised accounts and service accounts;
- encryption of data exchange;
- encryption of data communication in all network ports;
- minimum rights necessary for the users and service accounts;
- logging of changes;
- regular backing up of the data.

3.4 Advanced measures

APP.4.4.M13 Automatic configuration audits (C-I-A)

a. Automatic audits have been established for checking the configurations of the nodes, Kubernetes, and pods with applications, which compare the actual configurations with the lists and reference values specified.
b. Rules have been drawn up for the use of auditing tools which are compatible with the Kubernetes cluster.

APP.4.4.M14 Use of specialised nodes (C-I-A)

a. There are nodes in the Kubernetes cluster for performing specialised tasks which are only used by the pods designed for fulfilling such specialised tasks.
b. The incoming and outgoing data exchange of applications with other networks is regulated by preconfigured bastion nodes.
c. The control plane nodes are located in the so-called management nodes. The entire data exchange with the control plane is led through the management nodes.
d. Those pods which are specialised on back-up services are assembled into storage nodes.

APP.4.4.M15 Partition of applications at the levels of nodes and clusters (C-I-A)

a. Applications with a very high protection requirement are placed in the separated Kubernetes cluster or in nodes which are not accessible for other applications.

APP.4.4.M16 Use of Kubernetes operators (C-I-A)

a. The tasks of critical applications and control plane programmes have been automatised by the Kubernetes operator.

APP.4.4.M17 Certification of nodes (C-I-A)

a. Nodes present security certificates to the control plan cryptographically, preferably verified with TPM (Trusted Platform Module).
b. Only those cluster nodes are accepted by the control plane which have successfully demonstrated their security.

APP.4.4.M18 Microsegmentation (C-I)

a. Communication between the pods in the Kubernetes namespace is only permitted via designated network ports. Any unnecessary data connections are prohibited by the rules established in the Kubernetes CNI.
b. The CNI rules unambiguously specify the sources and destinations of data connections, as well as the filtration of data exchange based on the name of the service, metadata, service accounts, or certificate-based authentication.
c. The criteria used for the microsegmentation can only be changed by the individuals and administrative services with appropriate powers.

APP.4.4.M19 Guaranteeing the high availability of Kubernetes (A)

a. In the event of a failure or interruption in one location, the clusters and therefore also the applications in the pod will continue to operate without any noticeable interruption or the applications can be restarted in another location within a short period of time.
b. All configuration files, images, user accounts, network connections, and other resources required for operation, incl. the required hardware, have been prepared for restarting applications in another location.
c. In order to ensure the high availability of the cluster, the Kubernetes control plane, the hardware of the clusters, pods, and applications have been divided between different locations so that a hardware

failure or a fire, for example, would not result in the loss of availability of an application.
d. Regular tests which simulate system failures are performed to check the cooperation of the cluster, pods, and applications.

APP.4.4.M20 Encryption of the control plane storage space (C)

a. The file systems with permanent information (especially etcd) and the application services of the control plane are encrypted.

APP.4.4.M21 Periodic restarting of the pods (C-I-A)

a. In the event of a higher risk of external interruptions and a very high protection requirement, regular stopping and restarting of the pods is used. The recommended maximum uninterrupted operating time of a pod is less than 24 hours.
b. The availability of the applications of the pods during a restarting process is ensured.

APP.5 Group software

APP.5.2 Microsoft Exchange and Outlook

1 Description

1.1 Purpose

To present measures for the secure use of group software solutions Microsoft Exchange and Outlook for medium and large organisations.

1.2 Responsibility

The IT department is responsible for the application of the Microsoft Exchange and Outlook measures.

1.3 Limitations

The measures presented in the module complement the measures of the module APP.5.3 Email server and client in general in the Microsoft Exchange system.

The measures concerning the server platform, operating system, and clients are presented in the modules SYS.1.1 Server in general and SYS.2.1 Client computer in general and in the modules covering operating systems.

2 Threats

2.1 Missing or inadequate procedure for implementing Microsoft Exchange and Outlook

When there is no implementation procedure for Microsoft Exchange and Outlook, mistakes in management become possible. For example, if Microsoft Exchange is integrated incorrectly with Active Directory, data could be partially or completely lost. The same applies when the databases of the email accounts are deleted in an uncoordinated manner.

2.2 Incorrect migration to Microsoft Exchange

If the migration to the new Microsoft Exchange has not been carefully planned and implemented, problems caused by changes in the configuration settings and incorrect log settings might occur. The migration errors could disturb the exchange of information within the organisation and communication with the clients and partners.

2.3 Unauthorised browser access through Microsoft Exchange

Configuration errors of Internet Information Services (IIS), the permanent component of the Microsoft Exchange server which is used for accessing email accounts via a browser, can be used by an attacker for accessing the intranet.

2.4 Unauthorised connections of other systems with Microsoft Exchange

If the connectors for the communication with external systems are not taken into account during the migration to Microsoft Exchange, the existing connectors could become incompatible with the migrated Microsoft Exchange versions. This way, emails could be lost or changed inadvertently.

2.5 Incorrect management of the access rights of Microsoft Exchange and Outlook

When the access rights of an Outlook client or the access rights to the data stored in Microsoft Exchange are assigned and managed incorrectly, it could create security vulnerabilities. If the users

are assigned excessive rights on top of the necessary ones, unauthorised access to confidential information is created.

2.6 Incorrect configuration of Microsoft Exchange

Incorrectly configured systems are the most common reason for successful attacks against Microsoft Exchange. Due to the complexity of the Microsoft Exchange system, various configuration settings and parameters influencing each other could cause various security issues.

2.7 Incorrect configuration of Outlook

Any configuration errors of Outlook, such as assigning excessive access rights to users, create various security problems. Incorrectly selected communication protocol could cause specific security vulnerabilities. In addition, compromising the private key that is used for the encryption and signing of Outlook emails is also possible. When encryption is used on the network level (such as through IPSec or TLS), the encryption mechanisms might not function if the client has been configured incorrectly.

2.8 Malfunctions and misuse of macros and program interfaces added to the Outlook

Outlook as a well-known group tool can be used for spreading malware. Malicious software that is spread through the Outlook macros enables access to data and to change or delete it.

3 Measures

3.1 Life cycle

Planning

APP.5.2.M1	Implementation plan for Microsoft Exchange and Outlook
APP.5.2.M2	Infrastructure that is compatible with Microsoft Exchange

Implementation

APP.5.2.M3	Management of access rights for Microsoft Exchange
APP.5.2.M7	The procedure for migrating Microsoft Exchange
APP.5.2.M9	Secure configuration of the Microsoft Exchange server
APP.5.2.M10	Secure configuration of Outlook

Operation

APP.5.2.M5 Microsoft Exchange backup

APP.5.2.M11 Security of Microsoft Exchange connections

APP.5.2.M12 Secure use of Outlook Anywhere, MAPI over HTTP, and Outlook Web App

Additional advanced measures

APP.5.2.M17 Database encryption of the Microsoft Exchange system

3.2 Key measures

APP.5.2.M1 Implementation plan for Microsoft Exchange and Outlook

a. As a minimum, the following has been taken into consideration when preparing an implementation plan for Microsoft Exchange and Outlook:

- the structure of the email infrastructure;
- the client and server systems that are compatible with Microsoft Exchange;
- the use of function extensions;
- the used protocols.

APP.5.2.M2 Infrastructure that is compatible with Microsoft Exchange

a. Based on the implementation plan, suitable components for the Microsoft Exchange infrastructure have been selected, a structure for the infrastructure has been created, and the order of creating the infrastructure has been determined.
b. A valid choice between cloud and local services has been made.

APP.5.2.M3 Management of access rights for Microsoft Exchange

a. A concept of access rights has been prepared and documented for the systems in the Microsoft Exchange infrastructure.
b. The IT department uses user profiles of the server to access Microsoft Exchange.
c. The typical NTFS rights are set to allow only authorised administrators and necessary system accounts access to the Microsoft Exchange catalogue.

APP.5.2.M5 Microsoft Exchange backup

a. The Microsoft Exchange data is backed up periodically.
b. The databases of Microsoft Exchange are additionally backed up before installing updates and

changing the configuration.
c. The deleted Microsoft Exchange objects are completely removed from the database only after a predetermined period has passed.

3.3 Standard measures

APP.5.2.M7 The procedure for migrating Microsoft Exchange

a. The migration stages are carefully planned and documented. The migration plan takes into consideration the differences between mailboxes, objects, security policies, the structure of Active Directory, email systems, and the functions of versions of Microsoft Exchange and Outlook.
b. The new system has been tested in a separate testing network before its installation in the operational environment. The test results are documented.

APP.5.2.M9 Secure configuration of the Microsoft Exchange server

a. The servers of Microsoft Exchange are configured on the basis of the requirements of the email security guidelines (see also APP.5.3.M6 Email security guidelines).
b. The connectors of Microsoft Exchange are configured securely. The changes in the connector configuration are documented.
c. The activity logs of Microsoft Exchange are activated.
d. Security aspects are taken into consideration when implementing functional extensions (such as Microsoft Exchange ActiveSync, port mirroring, spam filter, Outlook Web App, or data leak prevention).

APP.5.2.M10 Secure configuration of Outlook

a. Each user has their own Outlook profile with user-specific settings.
b. The user can only change the settings that are specifically allowed to be modified (e.g. setting the letter footer, activating the out-of-office function).
c. Communication with another party does not reveal too much information (such as automatic notification about opening an email) or information about internal matters (such as the organisational structure).

APP.5.2.M11 Security of Microsoft Exchange connections

a. The security mechanisms for protecting the communication with Microsoft Exchange systems are determined and documented.
b. Measures for protecting the following components have been implemented:

- administrative interfaces;
- client-server communication;
- existing WebDAV interfaces;
- communication and messaging between servers;
- public key infrastructure (PKI), which is the basis of the encryption of Outlook emails (S/MIME).

APP.5.2.M12 Secure use of Outlook Anywhere, MAPI over HTTP, and Outlook Web App

a. Outlook Anywhere, MAPI over HTTP, and Outlook Web App are configured according to the security requirements of the organisation and the security guidelines of Microsoft Exchange.
b. Access to Microsoft Exchange through the internet is only granted to specific users based on well-reasoned need.

3.4 Advanced measures

APP.5.2.M17 Database encryption of the Microsoft Exchange system (C)

a. Guidelines for the encryption of PST files and Managed Store are documented.
b. Users are trained in the use of PST file encryption and security mechanisms.
c. In order to ensure the security of emails kept in the PST file on a local computer, encryption based on a filing system (such as Encrypting File System (EFS)) or hard disk encryption (such as Windows BitLocker) are used.

APP.5.3 Email server and client in general

1 Description

1.1 Purpose

To present general measures for the secure use of an email server and email clients.

1.2 Responsibility

The IT department is responsible for the compliance with the measures of the module 'Email server and client in general'.
Additional responsible persons: User, manager.

1.3 Limitations

The module presents general measures for the protection of the email server and clients. The module does not discuss other functionalities of the group software (such as calendar and contact management) or group software that is used as a cloud service (such as Microsoft 365, Google G Suite).
The measures concerning the server platform, operating system, and clients are presented in the modules SYS.1.1 Server in general and SYS.2.1 Client computer in general and in the modules covering operating systems. Logging is explained in the module OPS.1.1.5 Logging, and backup is discussed in the module CON.3 Data backup concept.

2 Threats

2.1 Inadequate planning of the use of email

If procedures as well as regulating and technical guidelines are not followed when implementing the email service, the uncertainty caused by it could cause erroneous settings, programming mistakes, and attacks (originating from inside or outside of the organisation). When technical and organisational security controls are not implemented, the danger of being infected by malware sent via email and of successful external attacks increases.

2.2 Incorrect configuration of the email server and clients

Due to the complexity of the email infrastructure and software settings and the concurrence of several parameters, situations might arise where security-critical settings (such as encryption of individual data or limiting rights) are ignored. Ignoring security-critical parameters could cause a loss of data availability, authenticity, and confidentiality. A configuration error of an email server could cause emails to 'get stuck' in the server and the message to not reach the desired recipient. An attacker can use an email server with a security vulnerability for spreading spam. Often, email servers do not check whether the letter actually came from the server that might be presumed by the address of the sender.

2.3 Unreliability of email

Although exchanging emails is generally a convenient and fast way for users to exchange data, it is not always reliable. For example, the messages that are sent could be delayed or lost due to an email server that has been configured incorrectly or a malfunction in the communication channel. Legitimate messages could sometimes get caught in the spam filters; an email could also be lost if the sender enters the address incorrectly. At worst, confidential information could be sent to the wrong recipient by mistake. An attacker can access an unencrypted email exchange and eavesdrop on the conversations systematically.

2.4 Spreading malware

An attacker could use email for spreading malware and infecting the IT systems deliberately. Malicious code can be hidden in the contents of an email. If the client has not configured their email securely, a malicious code could be activated right after opening the letter. Another possibility for spreading malware is to hide it in a file that is attached to the email. Malware is activated right after opening the file that is added to the email. This way, an attacker could launch a ransomware attack or use the infected computers for eavesdropping on the network traffic and stealing data.

2.5 Social engineering

Social engineering that is conducted using email takes advantage of the human qualities of the employees (such as helpfulness, trust, inattention, or respect for authority) to gain unauthorised access to data or make the employee behave in the manner that the attacker wants. Often, social engineering through email is based on identity theft; an attacker has initially hijacked a correspondence and is now communicating with the other party for financial fraud. If the employees are not trained in recognising and avoiding social engineering, it increases the danger of falling victim to social engineering.

2.6 Unauthorised reading and manipulation of emails

An attacker can take over unencrypted correspondence and gain access to confidential data that way. An attacker can manipulate materials without a digital signature or add malware to emails.

3 Measures

3.1 Life cycle

Implementation

APP.5.3.M1	Secure configuration of an email client
APP.5.3.M2	Secure use of an email server
APP.5.3.M5	Procedure for replacing an email recipient
APP.5.3.M7	Training users on group software client security
APP.5.3.M9	Extended security controls for an email server

Operation

APP.5.3.M3	Backup and archiving of emails
APP.5.3.M4	Protection of the email server against spam and viruses
APP.5.3.M8	Spam treatment of the user

Planning

APP.5.3.M6	Email security guidelines

Additional advanced measures

APP.5.3.M10	End-to-end encryption and digital signatures
APP.5.3.M11	Email server redundancy
APP.5.3.M12	Monitoring blacklists
APP.5.3.M13	TLS reports

3.2 Key measures

APP.5.3.M1 Secure configuration of an email client

a. The organisation has established a secure admissible configuration for the email clients.
b. The user receives a client program with a secure configuration. The user is prohibited or technically restricted from changing the configuration.
c. Before the end user opens an attachment, the system checks attachments with an antivirus program.
d. The configuration of the client does not allow for the automatic interpretation of the code in emails that are sent in HTML format.
e. The client configuration has prohibited the automatic preview function of attachments.
f. Automatic filtering and automatic forwarding of emails is only allowed in well-reasoned instances.

g. Insecure and public networks allow connecting to an email server only through a data connection channel (such as a VPN).

APP.5.3.M2 Secure use of an email server

a. The IT department implements measures for preventing denial-of-service attacks.
b. Data connection between an email server and clients is encrypted in both internal and external networks.
c. Sending emails via insecure and unencrypted data communication channels is prohibited.
d. A written list of protocols and services allowed in a specific email server has been prepared.
e. The possibility of using an email server for sending spam has been eliminated.
f. A limit has been set to the volume of email accounts in an email server.

APP.5.3.M3 Backup and archiving of emails

a. The backup and archiving of emails takes place only based on the established procedure.
b. The data in the email server is backed up regularly.
c. The backed up and archived emails are stored securely.
d. The users have been notified about whether the data of the email client in the client computer is backed up and how it is done.

APP.5.3.M4 Protection of the email server against spam and viruses

a. A scanning program with an antivirus software is implemented on the central email server for detecting spam and malicious content in the received and sent emails and email attachments.
b. If the email scanner is not capable of decrypting the encrypted emails for scanning, compensating security measures are applied.
c. The staff and the data protection specialist have been informed of using an email scanner.

3.3 Standard measures

APP.5.3.M5 Procedure for replacing an email recipient [manager]

a. When a significant part of the employee's tasks is sending and processing emails, a replacement has been appointed for the employee for receiving emails.
b. The replacement is given access to the email account of the person to be replaced or the emails are

forwarded to the replacement but only in compliance with the valid personal data protection regulations.
c. The person to be replaced is informed ahead of time of activating the forwarding function.
d. Written guidelines have been prepared for the secure use of automatic reply function of the email. Forwarding internal information with an automatic reply function is prohibited.

APP.5.3.M6 Email security guidelines

a. The organisation has prepared security guidelines for the secure use of an email account, which are compliant with the information security policy of the organisation.
b. Users and administrators are informed about any updates or changes to the security requirements of using email.
c. Compliance with the guidelines is checked regularly.
d. As a minimum, the email security guidelines include the following to protect the users:
- what kind of access rights the email server and clients have;
- how the sent and received emails are protected;
- how the integrity of emails is guaranteed;
- how email addresses and mail lists are managed;
- whether the private use of email is allowed and how;
- how the email accounts of the employees leaving employment are managed;
- whether the use of webmail applications is allowed and how;
- how to handle email attachments;
- whether HTML mode is allowed for emails.

e. Additional guidelines have been compiled for the administrators, determining:
- how to configure the components of an email server and client;
- how other servers can access the email server;
- which workstations allow the management of the email server and how.

APP.5.3.M7 Training users on group software client security

a. The users have been trained to work with an email client in a secure manner.
b. The users have been informed about the dangers regarding the use of an email service, including the dangers related to phishing emails and emails with a forged address of the sender.
c. The users have been warned about the dangers of sending chain letters and participating in non-essential mailing lists.

APP.5.3.M8 Spam treatment of the user [user]

a. The users are obligated to ignore and delete emails from unknown senders. Responding to such emails is prohibited, as is opening links and attachments in such emails.
b. The email server has implemented a centrally managed spam filter.

APP.5.3.M9 Extended security controls for an email server

a. An email server implements the following mechanisms for checking the authenticity of the server where an email originated and for authentication: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting and Conformance).
b. The SPF SoftFile (~) parameter is only used for testing purposes.
c. DMARC is configured to reject emails in case of a failure.
d. DMARC attack detection reports are reviewed regularly.
e. The MTA-STS and/or DANE security mechanisms are implemented to protect data connection between email servers.

3.4 Advanced measures

APP.5.3.M10 End-to-end encryption and digital signatures (C)

a. The organisation uses end-to-end encryption and digital signatures to protect data exchange.
b. Protocols that ensure sufficient security are used for encryption and digital signatures (see also CON.1 Cryptography concept).

APP.5.3.M11 Email server redundancy (A)

a. Email servers are implemented with redundancy - several email servers are in use simultaneously.
b. Rules for the synchronisation of email servers have been established and implemented.

APP.5.3.M12 Monitoring blacklists (A)

a. The organisation's email servers are constantly monitored regarding them being added to public blacklists of server addresses that are suspected of sending spam.

APP.5.3.M13 TLS reports (C-I-A)

a. The organisation uses the TLS report (TLS-RPT) for discovering potential encryption malfunctions.
b. If possible, the TLS report data is shared with other relevant parties.

APP.5.4 Unified communications and collaborations (UCC)

1 Description

1.1 Purpose

To present general measures for the secure use of unified communications and collaborations (UCC). UCC solutions combine means for phone and message communication, video calls, screen sharing, group projects, and file transfers.

1.2 Responsibility

The IT department is responsible for the implementation of UCC measures.
Additional responsible persons: No additional responsible persons.

1.3 Limitations

As UCC services require secure data communication connections to function, measures from modules NET.1.1 Network architecture and solution and NET.3.2 Firewall must be implemented along with this module. The measures concerning UCC infrastructure (server platform, operating system, and clients) are presented in modules SYS.1.1 Server in general, SYS.2.1 Client computer in general, and in the modules covering operating systems. Module APP.3.3 File server addresses the secure storage of shared files. When a UCC solution in use is a cloud service, the measures from module OPS.2.2 Using cloud services are applied. E-mail services are not considered UCC services, so measures from module APP.5.3 Email server and client in general are applied to them.

2 Threats

2.1 Insufficient availability of UCC services

The quality of a data network directly impacts the quality and availability of UCC services. Any disturbances in a data network or internet connection lead to interruptions in a UCC session and disturbances in the video feed or user communication. When UCC services are used for the coordination of restoring critical IT systems, the interdependence of the systems could lead to disruptions in the operation of other critical IT systems. As the UCC services cannot be used without functional data communication, the data network (and other critical IT systems) cannot be restored as required. When the UCC solution in use is a cloud service, the availability of the service also depends on the actions of the service provider and the reliability of the information security measures of the latter. Authentication services utilised by users for logging into the UCC services carry a similar risk. If an authentication service does not work, the UCC services are unavailable.

2.2 Mistakes in planning the commissioning of UCC

Misjudging the number of users and the intensity of use of a UCC service could affect the quality of the service (when the number of users of the service is higher than expected) or expenses related to the service (when the number of users of the service is lower than expected). Depending on the UCC services in use, the requirements of the UCC components to the capacity and quality of the data network might be very different. The requirements for data communication in the case of voice communication in an intranet differ from the ones set to the internet connection required for the use of cloud services. If data networks do not support all of the necessary UCC services, it is impossible to use these services to the required extent. Video communication and related image processing functions require high technical capability from the client devices using it. If a client device is not sufficiently powerful for image processing, the user experience suffers significantly. In the worst case, some of the client devices of the organisation are unfit for video communication.

2.3 Incorrect settings of a UCC solution

A UCC solution is usually configured in a client computer by a user personally. Various end user devices (headsets, microphones, etc.) might require different settings. A mistake made during configuration could mean that a user cannot be seen or heard during a meeting or that the user cannot hear other participants. If a communication device in a meeting room accepts incoming communication requests automatically, confidential information might be inadvertently revealed to the other party. The use of UCC services may be disrupted when a communication device is not correctly connected with the intranet of an organisation. Unsuitable routing devices could lead to the decreased quality of a UCC service. When the participants of a meeting with many attendees are not

identified and the rights of the participants are not sufficiently restricted, conducting a meeting will be difficult. Moreover, all attendees of the meeting might have unauthorised access to the materials of the meeting.

2.4 Improper use of the administrative rights of a UCC solution

The administrator of a UCC solution has extensive options for changing the usage possibilities of the UCC solution. The improper use of administrative rights or administrative errors due to low awareness could have serious consequences. For example, an administrator could make conversations or file sharing environments with limited access available to all users of a UCC service.

2.5 Leak of confidential information

Various UCC solutions have different user interfaces. The utilisation of an application and a web interface of a UCC solution could differ somewhat. Due to negligence, a user might inadvertently share their screen containing confidential information or forget to turn off their microphone so everyone can hear a private conversation of the user. It is also possible that materials meant to be shared with the participants are accidentally made available to an unauthorised person. Many UCC solutions record conversations and other information in a cloud. Therefore, it is possible that information with a high protection requirement is stored in a server of a cloud service provider with unknown location. This could lead to a conflict with legal requirements. When adding new users to a joint file sharing environment, the fact that a new user will also be able to access all the files stored in the environment in the past is often forgotten.

2.6 Unauthorised disclosure of personal data

UCC services gather user data and create user profiles to display to other users. This could lead to a disclosure of personal data because it allows drawing conclusions about the use of working hours, professional results, and personal relationships of the individual. Even seeing the current status or availability of a user could mean an unauthorised disclosure of the personal data of the user. If someone participates in a virtual meeting from their home office, personal items of the participant or people doing something behind the attendee might be visible or the background noise of a private environment might be audible in the background of the video feed.

2.7 Issues with the resource management of a UCC solution

A UCC solution being operational could depend on the IT components of a computer being functional. Often, different UCC solutions use the same resources shared by an operating system. Frequently, a user cannot work with several UCC solutions (e.g. a phone application and a video conference application) simultaneously because one of the applications uses all the resources and blocks other applications from using them, such as a headset required for communication. Some UCC solutions have very high requirements for resources, which might lead to an overload and overheating of a client device. This is particularly true when several video conference applications run on the background at the same time.

2.8 Unauthorised takeover of the computer of a user

UCC solutions might include a function for transferring the control over the computer of a user (such as moving the cursor) to another party. At the same time, the person transferring the screen has no option for regaining control of the computer and they lose control over further activities. As a result, the participants of a conversation could be granted access to applications and data that the person transferring the screen does not want to share with others.

2.9 Use of a false identity

A malicious user can pretend to be a reliable partner and participate in meetings or video conferences by using a false identity to acquire confidential information or plan further attacks. Often, this is possible when a large number of people attends a meeting and the meeting does not start by letting all participants introduce themselves. An attacker is able to share hyperlinks with harmful content through chats. As a UCC service is a far more reliable platform for a regular user than email, the user of a UCC service is more receptive to social manipulation and social engineering, compared to an email service. An attacker may manipulate the names displayed in the communication environment, their voice, or their appearance to increase trust. For example, an attacker might pretend to be a manager to acquire confidential information or demand confidential documents directly through a chat.

3 Measures

3.1 Life cycle

Planning

APP.5.4.M1 Planning the commissioning of UCC services

Implementation

APP.5.4.M2 Network solution inspection prior to adopting UCC services

APP.5.4.M3 Testing UCC services

APP.5.4.M4 Deactivation of useless functions and services

Operation

APP.5.4.M5 Principles for assigning UCC roles and access privileges

APP.5.4.M6 Encryption of data exchange for UCC

APP.5.4.M7 Procedure for the safe utilisation of UCC services

APP.5.4.M8 Implementing a session border controller (SBC)

APP.5.4.M9 Secure configuration of UCC

APP.5.4.M10 Limiting forwarded information based on content

Additional advanced measures

APP.5.4.M11 Ensuring the high availability of UCC services

APP.5.4.M12 Adding UCC services to the disaster management plan

APP.5.4.M13 Secure management of SIP trunks

APP.5.4.M14 End-to-end encryption of UCC data communication

APP.5.4.M15 Limiting functions that use AI

APP.5.4.M16 Implementing a session border controller (SBC) in other gateways

APP.5.4.M17 Limiting the use of UCC services

APP.5.4.M18 Integration of UCC components with security monitoring

3.2 Key measures

APP.5.4.M1 Planning the commissioning of UCC services

a. The organisation has analysed the need to utilise UCC services and the organisational and technical impact of UCC services on achieving the objectives of the organisation.

b. The organisation has prepared a plan for commissioning UCC services, describing at least the following:

- objectives that the commissioning of the UCC services is meant to achieve;
- functional requirements (for the UCC solution as a whole and individual services);
- information security requirements applicable to the UCC services;
- permitted information and data specifications that may be sent through the UCC services;

• a list of the UCC services that comply with the requirements of the organisation;
• an analysis of interdependence between the UCC and other IT services;
• changes in the work processes of the organisation due to adopting the UCC services.

c. The organisation has prepared guidelines for integrating the UCC components with the IT systems and IT infrastructure of the organisation.

d. The organisation has analysed whether the UCC components should be located in a separate network segment and how to interface the UCC components with other applications.

APP.5.4.M2 Network solution inspection prior to adopting UCC services

a. When assessing the readiness to use UCC services, the following technical aspects of the network are taken into consideration:
• performance parameters specific to the UCC - permissible packet loss, jitter, and latency;
• the existence of sufficient bandwidth for video conferences;
• power over ethernet (PoE) required for the operation of stationary endpoints;
• WLAN communication option for mobile devices.

b. Before adopting any UCC services, the compliance of the network with the performance parameters specific to the UCC services is verified and a plan is prepared for eliminating any shortcomings that were identified.

c. When additional UCC services are added, the aforementioned technical aspects are reviewed again.

APP.5.4.M3 Testing UCC services

a. Before adopting any UCC services, tests are conducted to verify that the UCC components function as required without any failures.

b. End users participate in the testing of the UCC services; they will test the interaction of the UCC services with other applications.

c. Tests are repeated when UCC services are changed or new ones are added.

APP.5.4.M4 Deactivation of useless functions and services

a. The UCC services in use correspond to the defined purposes and the services are used with the least number of necessary functions.

b. When limiting the functions, the potential interactions between the components of the UCC are

taken into account.
c. If possible, the use of the following functions is deactivated or restricted:
- personal data processing and storage by a UCC component;
- access to personal data by users and the UCC service;
- access of external parties to the UCC services potentially containing sensitive information (such as texts, status of the user, shared storage space);
- sending data and files to external UCC services.

d. Log data of interpersonal conversations is collected and stored only to the least necessary extent.
e. There is a clear understanding of which users and UCC components have access to log data. If necessary, access is restricted and/or the corresponding UCC service functions are deactivated.

APP.5.4.M5 Principles for assigning UCC roles and access privileges

a. The management procedure of roles and access rights of the organisation has been updated to include roles and authorisations specific to UCC. When assigning roles, all user groups (including external) are taken into account.
b. When granting access privileges, the following aspects are considered:
- the least necessary access privileges for the intended use of the UCC services;
- the necessary access privileges for configuring the UCC services and changing settings;
- the right to activate special functions of UCC services (such as recording conversations).

c. Access rights granted to regular users have been limited to the minimum required level.
d. Only authorised users have the right to use the special functions of the UCC services.
e. Compliance with the least privilege principle of users and the appropriateness of access rights granted to users of UCC services are checked regularly. In addition, access rights are checked after any changes to the UCC services. If necessary, access rights are updated.

APP.5.4.M6 Encryption of data exchange for UCC

a. Any UCC data communication over unreliable networks (such as the internet) is encrypted.
b. When the encryption of the UCC data communication is not possible, the organisation has established clear categories of data that cannot be transferred through unified communications and collaborations solutions.
c. In the case of data exchange between various UCC solutions, it has been determined which data can be forwarded only when encrypted first (such as sending files).
d. Files containing confidential data stored in the file repository of a UCC solution (including

personal data) are encrypted with secure encryption mechanisms. The requirement for encryption applies in the internal file repository as well as for files stored in the cloud of a UCC service provider.
e. The users of a UCC solution can make sure that data communication has been safely encrypted.

APP.5.4.M7 Procedure for the safe utilisation of UCC services

a. The users know how to use UCC services safely, including chats or video conferences initiated by external parties.
b. The users have been informed of the functions of a UCC solution (such as entering a shared PIN or secure authentication of the parties) that help make chats or video conferences that they initiate safer.
c. When starting a UCC video conference or a web meeting, the following security aspects are agreed:

- selection of participants according to the content and objectives of the conversation;
- correct authentication of all participants;
- assigning moderator rights only to select users;
- procedure for recording a video conference or a conversation;
- procedure for using conference equipment in meeting rooms.

3.3 Standard measures

APP.5.4.M8 Implementing a session border controller (SBC)

a. When transmitting UCC media flows to a less trustworthy network, a session border controller (SBC) has been activated in the gateway. First and foremost, this is important when using UCC call services.
b. SBC functions as an endpoint for encryption and filters signalling and the transmission of media flows.

APP.5.4.M9 Secure configuration of UCC

a. When configuring UCC, the implementation of the following additional security controls has been considered:

- encryption of signalling and media flows in trustworthy transmission channels among all else;
- additional measures for protecting stored data and restricting access to the recordings of

conversations;

- allowing only internal users to utilise UCC services;
- blocking the forwarding of the status of users.

b. Stored data is encrypted and only authorised users have access to it after secure authentication.

c. Client computers have preconfigured messaging applications for secure use. Text-based messages are scanned with an anti-malware application to identify harmful links.

APP.5.4.M10 Limiting forwarded information based on content

a. The organisation has carefully considered whether the implementation of measures for the (automatic) evaluation of the content of a conversation and for restriction is proportionate in light of protection requirements and actual needs for data protection.

b. If necessary, content-based restrictions on information can be deactivated completely or for a specific conversation.

c. A conscious decision has been made on whether or not to allow the services of artificial intelligence (AI) and sending message content to the supplier of a cloud service when evaluating content.

d. The users of a UCC service have been informed of the content-based restrictions and analyses of the contents of chats ahead of time and they have given clear and unequivocal consent.

e. Data created when evaluating conversations is protected from unauthorised access.

3.4 Advanced measures

APP.5.4.M11 Ensuring the high availability of UCC services (A)

a. The following technical measures are implemented to improve the availability of UCC services:

- ensuring the redundancy of central servers and central services;
- using CAC (Call Admission Control) for increasing the quality of phone and video services;
- using independent UCC services without any significant dependencies.

b. When using the UCC services, the network connections between the cloud service provider and internet service provider (ISP) are designed to function in a redundant and failsafe manner.

c. When using VoIP telephone communication, the provider of the SIP service ensures the high availability of its communication networks.

d. The availability of the UCC services is constantly monitored and measured.

APP.5.4.M12 Adding UCC services to the disaster management plan (A)

a. A business impact analysis (BIA) has been conducted regarding UCC services and the UCC services to be discussed as part of an emergency concept have been selected (see DER.4.M7 Emergency concept).
b. An alternative solution has been determined for each UCC service, used when the service is not available. First and foremost, the possibility of making emergency calls has been ensured for users.
c. Detailed recovery plans have been prepared for UCC services that require more complicated settings (such as changes in network configuration or changing the routing by the supplier of a telephone service) or that depend on other services.

APP.5.4.M13 Secure management of SIP trunks (C-I-A)

a. When managing SIP trunks, the four eyes principle is applied to making the following changes:
- changes in routing configuration;
- changes in CAC (Call Admission Control) parameters;
- encryption settings (both in the intranet as well as towards the service provider network);
- changes in security settings, such as the configuration of the local storage of data.

APP.5.4.M14 End-to-end encryption of UCC data communication (C-I)

a. Media flow and signalling, which connect participants, have been securely encrypted end to end.
b. Using data communication without end-to-end encryption (for example, when the communication between different UCC solutions does not enable end-to-end encryption) is prohibited in the case of UCC services.

APP.5.4.M15 Limiting functions that use AI (C)

a. Using AI (artificial intelligence) in UCC services is deactivated or limited to a minimum.
b. If it is not possible to deactivate AI centrally, the users are obligated to turn off AI functions when starting a conversation.

APP.5.4.M16 Implementing a session border controller (SBC) in other gateways (C-I-A)

a. SBCs are also used in intranet gateways. This is particularly important in the case of UCC data communication between network segments with protection requirements.
b. SBC encryption mechanisms are applied in data communication between intranet segments.

APP.5.4.M17 Limiting the use of UCC services (C-I-A)

a. The following measures are used for restricting UCC services:
- allowing/prohibiting services based on the content of forwarded information and protection requirement;
- multifactor authentication (MFA) of users;
- blocking external users;
- deactivating the storage of metadata;
- limiting the visibility of communication data for administrators.

b. If necessary, additional technical and/or organisational security measures are used in UCC solutions (such as entering a PIN or a password every time).

APP.5.4.M18 Integration of UCC components with security monitoring (C-I-A)

a. Important UCC components (such as UCC controllers, SBCs, encryption devices) have been integrated with constant security monitoring.
b. When an organisation uses real-time automated control systems for the identification of security events and sending notifications about them, essential UCC components are also monitored.

APP.6 Software in general

1 Description

1.1 Purpose

To present measures for ensuring the security of software and data that is processed with the software, including measures for the implementation, acquisition, use, and decommissioning of software. This module considers all software products as software (such as operating systems, office software, financial software, and document management system).

1.2 Responsibility

The IT department is responsible for the implementation of the measures of the module 'Software in general'.
Additional responsible persons: Procurement department, responsible specialist.

1.3 Limitations

The module discusses the typical software processes during a generalised life cycle. The module does not apply to the software of closed systems (such as IoT and network devices). In addition to this module, the software measures from the modules OPS.1.1.3 Patch and change management, OPS.1.1.6 Software testing and onboarding, and product-specific APP modules are implemented.

2 Threats

2.1 Selecting unsuitable software

Selecting unsuitable software for the organisational needs has a negative impact on the business processes. For example, the new software might not be compatible with the existing IT systems or there may be deficiencies in the functionality or performance capacity of the software. When software does not comply with the security requirements established in the organisation, there is danger of disclosing or manipulating data that is processed with the software.

2.2 Data loss caused by a configuration error

When the software has been configured incorrectly, sensitive data could be disclosed inadvertently. For example, data is synchronised with the cloud service of a software manufacturer because the respective setting was not deactivated during configuration. Configuration errors could cause violations of legislative acts or financial or reputational losses.

2.3 Acquiring software from an unreliable source

When software or its updates are acquired from unreliable sources, a ruined or deliberately changed software copy might be received instead of the desired software. When installing such software in the organisation's computers, malware might spread and/or software might not function as expected.

2.4 Security vulnerabilities due to inadequate maintenance

Software security vulnerabilities could become apparent during the entire time that the software is used. If the security vulnerabilities are not fixed as quickly as possible, the data that is processed with the software is under threat. If the software manufacturer does not guarantee the new updates and security patches or if a maintenance agreement has not been concluded for software maintenance, an attacker might abuse the security vulnerabilities in the software for penetrating the network or stealing data.

2.5 Data losses caused by the misuse of software

When software functions are misused, the employees might delete data or render it unusable by accident. For example, when using the encryption function incorrectly, the data could still be there but it can no longer be decrypted.

2.6 Lack of resources when using software

If the existing IT infrastructure does not have sufficient resources for running a software, the availability of the software could be severely disrupted. The increased access and wait times affect the functioning of business processes negatively.

2.7 Incompatibility of the software with the needs of the user

When the functionality of the acquired software does not correspond to the actual needs (e.g. the formats are not compatible with the applications in use), the work of the organisation could be significantly interrupted. Even if the software functionality is sufficient but the user interface is not user-friendly, the users could abandon the software and look for alternative solutions. This facilitates the use of illegal software or software meant only for personal use in the organisation.

3 Measures

3.1 Life cycle

Planning

APP.6.M1	Planning the implementation of software
APP.6.M2	List of software requirements

Acquisition

APP.6.M3	Secure acquisition of software

APP.6.M7	Selecting suitable software
APP.6.M11	Managing add-ons and plugins

Implementation

APP.6.M4	Procedure for the installation and configuration of software
APP.6.M5	Secure installation of software
APP.6.M8	Secure use of installation media

Operation

APP.6.M6	Additional security functions of software
APP.6.M9	Software inventory
APP.6.M10	Security guidelines for software

Disposal

APP.6.M12	Decommissioning software
APP.6.M13	Secure uninstallation of software

Additional advanced measures

APP.6.M14	Use of certified software

3.2 Key measures

APP.6.M1 Planning the implementation of software [responsible specialist]

a. When implementing software, the following has been described:

- the purpose of using the software;
- the data that is processed with the software;
- hardware and IT systems on/in which the software is used;
- software interface and threading with existing applications;
- the need for external support when implementing and running the software.

b. When planning to implement software, aspects of information security and the security requirements that the software must comply with are taken into account.

c. In order to implement typical software, necessary approvals and persons responsible are determined who:

- prepare the list of requirements;
- select a software product;
- test the software;
- install the software product.

APP.6.M2 List of software requirements [responsible specialist]

a. Based on the results of planning the implementation of software, a list of requirements for the software has been prepared and approved.
b. The list of requirements for the software includes both functional and non-functional (including information security) requirements for the software.
c. As non-functional requirements, the following is described:

- application environment, including platform, external devices, interfaces;
- compatibility with other components, incl. supporting migration and backward compatibility;
- requirements applying to performance;
- interoperation requirements;
- reliability requirements;
- compliance with standards and internal regulations;
- usability requirements, incl. the ease, comprehensibility, and learnability of use;
- maximum cost limit;
- requirements for documentation;
- requirements for the quality of software.

d. The following is described as part of the security requirements:

- identification and authentication;
- regulating access;
- security of evidence;
- logging requirements;
- resistance to damage;
- reliability;
- secure data transmission;
- data backup;
- encryption;
- functions for ensuring data integrity.

e. The requirements for software comply with the regulations on personal data protection and other relevant legislation.
f. The list of software requirements is approved within the organisation by all the units and parties it concerns.

APP.6.M3 Secure acquisition of software [procurement department]

a. When acquiring software, the list of software requirements is complied with (see also APP.6.M2 List of software requirements).
b. Software is only obtained from trustworthy sources. The authenticity and integrity of the acquired software can be proved.
c. The software producer guarantees support and security patches for the software for its entire lifespan.

APP.6.M4 Procedure for the installation and configuration of software [responsible specialist]

a. When installing and configuring software, the following principles are followed: • the software is installed and run only to the extent of the necessary functionality; unnecessary services and functions are uninstalled or deactivated; • the software is run with minimum necessary access rights; • the software does not contain redundant data, incl. personal data.
b. The updates and security patches of the software are installed before starting to use the software in an operational environment.
c. Installation guidelines are prepared for the installation of software which include all manual installation steps, and among all else, configuration changes made during the installation.
d. Installation procedures are conducted by the authorised employees of the IT department.
e. Before installing software, the authenticity and integrity of the software package is verified by using a digital signature of the issuer of software or file hash information.
f. The typical configuration of the software and changes to it are documented.
g. Before and after installing software, a complete data backup is made for all affected IT systems.

APP.6.M5 Secure installation of software

a. Typical software is installed and configured according to the installation guidelines (see also APP.6.M4 Procedure for the installation and configuration of software).
b. Only software that is previously tested and approved for implementation is installed.
c. Installation procedures are conducted by the authorised employees of the IT department.
d. Any deviations from the guidelines are approved with the responsible employee of the IT department and the party that approves the implementation.

3.3 Standard measures

APP.6.M6 Additional security functions of software

a. In case of a high protection requirement, the sufficiency of the security functions of the implemented software is evaluated; if possible, this is done while establishing the requirements and selecting software products.
b. As a minimum, the following are considered additional security functions:

- increasing the security of log data;
- hardening the hardware and operating system for running the software;
- hardening the encryption mechanisms for data exchange;
- creating a more detailed tiering for access rights.

APP.6.M7 Selecting suitable software [responsible specialist, procurement department]

a. The available software products are analysed and compared based on the list of requirements (see also APP.6.M2 List of software requirements) by using a suitable scale of comparison.
b. If there is more than one suitable software product, the maximum number of product users, product reviews, and costs related to the product (for example, training, migration, and running) are also analysed.
c. A suitable product is selected together with the head of the unit that submitted the application based on prior assessment and product testing.

APP.6.M8 Secure use of installation media

a. A backup copy has been created of the installation media, and if possible, the backup copy is used for repeated installations..
b. The installation media is kept protected from unauthorised access. The installation media is accessible for the authorised employees.
c. If necessary, the installation files can be downloaded again from the manufacturer's repository (such as an application store).
d. A backup copy has been created of the configuration files of the software and its configuration has been documented.
e. Re-installation of software has been integrated into the data backup concept of the organisation.

APP.6.M9 Software inventory

a. The used software products are registered in the inventory list.
b. The software inventory list presents the name, licence type, number of licences, and the duration

of validity of the licence of the software.
c. The software can only be used if its use complies with the terms and conditions of the software licence.
d. In case of software products that differ from typical software, the inventory list also makes a note of the reason for using this software.
e. The software inventory list is reviewed and updated regularly. In addition, the list is updated as quickly as possible after adding new software.

APP.6.M10 Security guidelines for software

a. Requirements for the secure configuration and use of software are compiled into software security guidelines.
b. The concerned external parties and employees of the organisation comply with the software security guidelines when completing daily tasks.
c. The compliance with the software security guidelines is checked at random.

APP.6.M11 Managing add-ons and plugins

a. Only the use of the necessary add-ons and plugins is allowed for running the software for its intended purpose.
b. Unnecessary add-ons and plugins are uninstalled or deactivated.

APP.6.M12 Decommissioning software [responsible specialist]

a. Guidelines have been prepared for the secure decommissioning of software, which include detailed steps and appoint persons responsible.
b. If the decommissioning of software brings changes to the daily tasks of the employees, they are notified well ahead of time and the employees are made sure to receive the necessary training.

APP.6.M13 Secure uninstallation of software

a. When uninstalling software, all files are removed which were created for the use of the software in the IT system and all entries related to the software to be decommissioned are deleted from the system files.
b. Any system changes made during the uninstallation are documented (manually or with special programs).

3.4 Advanced measures

APP.6.M14 Use of certified software (C-I-A)

a. When acquiring software, the sufficient trustworthiness of the affirmations of the manufacturer, supplier, or service provider about the implemented security functions is evaluated.
b. If there are several certified software products with the required functionality, the additional security mechanisms of the product and their compliance with the protection requirement are evaluated.
c. When there is no certified product on the market, the operational environment of the software is protected with additional security measures.

APP.7 Custom software development

1 Description

1.1 Purpose

To present measures for planning, acquiring, implementing, using, and decommissioning applications which are developed for the individual use of the organisation or adjusted significantly for the organisation.

1.2 Responsibility

The responsible specialist is responsible for compliance with the measures for the development of custom software.
Additional responsible persons: Procurement department, IT department.

1.3 Limitations

The module discusses the planning, ordering, implementation, running, and decommissioning of software from the point of view of the ordering entity.
Software development and related security measures from the point of view of the developer are covered in the module CON.8 Software development. In addition to this module, the measures from

the module OPS.1.1.6 Software testing and onboarding and from the product-specific APP modules are implemented for the software.

2 Threats

2.1 Inadequate stipulations in the contract with an external service provider

If a contract with an external service provider describes the activities of the parties inadequately or ambiguously, the security measures might be left unimplemented due to ignorance, missing qualifications of persons concerned, or a lack of resources. For example, the requirements for software stemming from legislative acts might not be met if the contract that is concluded with the service provider does not stipulate the development of the relevant functionality.

2.2 Insecure software architecture

If the applications have used sub-programs, modules, and protocols with a required security level that is individually lower than that of the application as a whole, the application could have significant security vulnerabilities. When the software program modules and protocols are designed for operating in an isolated environment, then connecting the software to the internet might create various security issues. If abusing a vulnerability in the software or a software error becomes apparent, the provided security mechanisms might fail to function as planned. Due to the security vulnerabilities of the software architecture, an attacker could find a way to bypass the security mechanisms.

2.3 Undocumented functions

The application could include functions that are unknown to the regular user and undocumented. Such hidden functions can be used by an attacker to bypass the existing security mechanisms meant for regular users.

2.4 Absent or inadequate security measures in the application

The absence of suitable security measures in an application makes the application data easily accessible for an attacker. The inadequacy of the security measures might be caused by the insufficient project budget or a rushed development schedule.

2.5 Inadequate control over software development

When the contracting entity cannot control whether the agreed function (including a security function) has been realised in the application, there is a danger of accepting the application along with the security vulnerabilities contained in it.

2.6 Incompetent software developer

The chosen software developer could lack the technical knowledge about the specific programming language or framework. In addition, the developer may not be capable of considering all the details regarding an IT infrastructure and operational environment. Due to a lack of sufficient experience, the developer could make mistakes which otherwise would be avoidable.

3 Measures

3.1 Life cycle

Planning

APP.7.M1	Planning a custom software development project
APP.7.M2	Establishing security requirements for software development
APP.7.M3	Determining the operating requirements for software
APP.7.M4	Establishing the requirements for custom software
APP.7.M6	Thorough documentation of the requirements for custom software

Operation

APP.7.M5	Monitoring a software development project
APP.7.M8	Involving employees in the early testing of software

Implementation

APP.7.M7	Secure acquisition of custom software

Additional advanced measures

APP.7.M9	Reliable depositing
APP.7.M10	Using a certified software developer

3.2 Key measures

APP.7.M1 Planning a custom software development project

a. A responsible party (contracting entity or developer) and a project manager have been appointed for managing and coordinating the software development project.
b. The organisation has conducted the initial analysis and established the framework conditions for the custom software, including:

- the business processes that are supported by the application;
- the processed data and its protection requirement;
- legal framework conditions;
- IT systems with which the application exchanges data;
- the necessary roles and access rights.

c. In order to conduct a development project, methods for software development and the model for project management have been approved.
d. The development project of custom software has a pre-defined result, budget, and deadline.

APP.7.M2 Establishing security requirements for software development

a. The organisation has approved the organisational and technical security requirements for the development process.
b. The development environment and its security controls are selected based on the security requirements of the software development and protection requirements of the data.

APP.7.M3 Determining the operating requirements for software [IT department]

a. The IT department has prepared a list of specifications for hardware and software required for running the custom software:

- hardware platform (including a server and storage devices);
- software (including an operating system and database);
- system resources (including requirements for the processor, RAM, and storage capacity).

b. The specification for the interface is prepared to add the software to other IT systems.

APP.7.M4 Establishing the requirements for custom software [procurement department]

a. The following requirements are established for the acquisition of custom software:

- software functionality requirements resulting from the business requirements of the organisation and legislative acts;
- software requirements (see also APP.6.M2 List of software requirements);

• security requirements for software development (see also APP.7.M2 Establishing security requirements for software development);
• technical requirements for software (see also APP.7.M3 Determining the operating requirements for software).

3.3 Standard measures

APP.7.M5 Monitoring a software development project

a. When developing custom software, the agreed and approved software development methods and the model of project management are followed.
b. The software development project includes risk and quality management.
c. Employees and external developers who participate in the risk and quality management of the development project are sufficiently qualified.
d. The required monitoring activities of the method for software development and the project management model are conducted throughout the life cycle of the custom software.

APP.7.M6 Thorough documentation of the requirements for custom software

a. The business requirements established for the application and their implementation (including work flows, dialogues, correction templates, data structures) are presented as functional requirements for the application.
b. As non-functional requirements, at least the following requirements for the application are documented:
• quality requirements (usability, trustworthiness, performance);
• requirements for the architecture and IT infrastructure for which the application is developed;
• interfacing requirements;
• documentation of the application (such as modelling in UML);
• testing requirements for the application;
• requirements for security functions.
c. The following security requirements are documented in the case of high protection requirements of the data of the application:
• requirements for the use of cryptographic mechanisms (See also CON.1 Cryptography concept);
• requirements for data backup (see also CON.3 Data backup concept);
• archiving requirements (see also OPS.1.2.2 Archiving);

• logging requirements (see also OPS.1.1.5 Logging).

d. After the installation of software changes and functional updates, compliance with the requirements is checked, and if necessary, the documentation of the software requirements is updated.

APP.7.M7 Secure acquisition of custom software

a. The developer of custom software submits a suitable software development and project management method along with the tender.

b. The public procurement documents of the software do not disclose the security architecture of the planned software too extensively.

c. The organisation has established processes and appointed the persons responsible for assessing the compliance of the submitted tenders with the procurement documents.

APP.7.M8 Involving employees in the early testing of software

a. The employees of the organisation are included in the software testing at the earliest possible stage of the software development.

b. The developer ensures that there is a sufficient time buffer for eliminating errors discovered during testing and realising improvement proposals.

3.4 Advanced measures

APP.7.M9 Reliable depositing (A)

a. In case of business-critical custom software, the necessity of insuring software against the discontinuation of software support has been decided.

b. The escrow of software source code and other essential materials has been considered. As a minimum, the escrow contract includes the following:

- the rights and conditions of handing over the deposited material;
- verification of the deposited material;
- suitable storage and protection of the deposited material;
- the procedure for updating the deposited material.

APP.7.M10 Using a certified software developer (C-I-A)

a. When developing security-critical custom software, software developers that are certified in security governance and software development are used.
b. When selecting a software development partner, the reliability of the developer's confirmations of the acquired certifications and the implemented security functions is evaluated.

APP.EE Estonian applications

APP.EE.1 X-tee data service

1 Description

1.1 Purpose

Presenting measures used for the protection of the provider or consumer of the X-tee data service. The IT systems interfaced with the X-tee security server may not endanger the infrastructure of X-tee or become vulnerable due to being interfaced with X-tee. Exchange of data between different organisations and units must also be based on clear legal bases.

1.2 Responsibility

The responsible specialist is responsible for compliance with the measures for the consumption of the X-tee data service.
Additional responsible persons: The IT department, data protection specialist.

1.3 Limitations

The measures for the owner of the X-tee security server are described in the module SYS.EE.1 X-tee security server. The agreements on the use of the security server and on the data service are based on modules CON.9 Exchange of information and OPS.3.1 Information security of the service provider. In addition to this module, the measures from the module OPS.1.1.6 Software testing and onboarding and from the product-specific APP modules are implemented for the software.

2 Threats

2.1 Misuse of the data of the data service

The X-tee data service is used to mediate and store the data of service providers as well as the consumers of the services. Any misuse, leak, or unauthorised modification of the data would affect the parties to the data service and the owners of the data (incl. private individuals).

2.2 Security server configuration errors

Errors in the communication with the owner of the security server and the resulting incorrectly configured security server may enable unauthorised access to data or restrict the access of authorised users to the data service without a cause.

2.3 Errors in the interfacing of the security server with the data service

The errors made in the interfacing of the security server and a data service may lead to data leaks and unauthorised access to the data services.

3 Measures

3.1 Life cycle

Planning

APP.EE.1.M1 Planning the use or provision of the X-tee data service

Implementation

APP.EE.1.M2 X-tee subscription contract with the X-tee centre

APP.EE.1.M3 Contracts for trust services

APP.EE.1.M15 Agreement for the consumption of the security service

Operation

APP.EE.1.M4 Management of e-seal certificates

APP.EE.1.M5 Publication of the X-tee data service with the help of the security server

APP.EE.1.M6 Consumption of the X-tee data service through the security server

APP.EE.1.M7 Agreements for X-tee data services

APP.EE.1.M8 Secure interfacing of the X-tee data service

APP.EE.1.M9 Developing and testing the X-tee data service

APP.EE.1.M10 Archiving the message log of the X-tee security server

APP.EE.1.M14 Regular reviews of the documentation of the X-tee data service

APP.EE.1.M16 Using the security server as a consumer

APP.EE.1.M17 Logging and monitoring the X-tee data service

Disposal

APP.EE.1.M11 Terminating the provision of the X-tee data service

APP.EE.1.M12 Ceasing the use of the X-tee data service

APP.EE.1.M13 Secure termination of the use of the security server

Additional advanced measures

APP.EE.1.M18 High availability of the X-tee data service

APP.EE.1.M19 Secure use of the private key of the e-seal of the organisation

APP.EE.1.M20 Using qualified e-seals

3.2 Key measures

APP.EE.1.M1 Planning the use or provision of the X-tee data service [data protection specialist, IT department]

a. The demand for and the requirements of the X-tee data service have been analysed, with at least the following issues considered:

- identifying the data exchange needs of a business process or a service;
- the legal grounds for sending/receiving/processing the data included in the composition of data exchange;
- the existence of personal data (primarily special categories of personal data) and the rules for processing such data;
- the permissibility and time limits of buffering data;
- defining the requirements for availability (incl. the volumes of using the service and the patterns of use).

b. The X-tee usage model is selected based on the analysis conducted and the capability of the organisation: either outsourcing the security server service or owning a security server SYS.EE.1 X-tee security server).

c. The content of the security server service and the performance indicators of the security server are determined based on the requirements of the business process using the data service and in cooperation with the owner of the security service: the level of the probative value of data exchange, incl. the need for qualified e-seals (see eIDAS); the accuracy (frequency) of timestamping and the permitted delay (the maximum period for which messages may remain without a time stamp);

requirements for the level of detail of the message log (full message logs, only headers logged, or no logging); the retention periods of the message log and the access rules of the message log.

APP.EE.1.M2 X-tee subscription contract with the X-tee centre [management of the organisation]

a. An X-tee subscription contract has been concluded with the X-tee centre.
b. Authorised administrative and technical contact persons are registered in the self-service environment of the X-tee centre. In the event of any changes in the authorised persons, the contact details are updated immediately.
c. The email address for receiving notices is redirected to a separate address/mailing group with more than one recipient.

APP.EE.1.M3 Contracts for trust services [management of the organisation]

a. The organisation has concluded contracts for trust services.
b. There is a procedure for reviewing the contracts. The contracts are updated, if necessary.
c. The administrative and technical authorised contact persons of the organisation are registered by the provider of trust services (timestamping service, certification centre, OCSP). In the event of any changes in the authorised persons, the contact details are updated immediately.
d. The email address for receiving notices is redirected to a separate address/mailing group with more than one recipient.

APP.EE.1.M4 Management of e-seal certificates [IT department]

a. Timely updates of the signing certificates are ensured in cooperation with the owner of the security server.
b. If a signing certificate is no longer in use, an application for the cancellation of the certificate must immediately be submitted to the trust service provider.

APP.EE.1.M5 Publication of the X-tee data service with the help of the security server

a. The technical parameters of the X-tee data service and the end points have been defined (WSDL addresses, REST, data service address(es), subsystem name, etc.).
b. The required probative value of the X-tee data service has been agreed on (i.e. the levels of the e-seal and timestamping).

c. The procedure for updating and checking the access list has been agreed on.
d. Every IT system or a logical part thereof has a separate X-tee subsystem for providing the data services.
e. Consuming the X-tee data service without the mediation of an authorised security server is blocked.
f. The owner of the security server is notified of the following:
- any changes in the list of consumers of the data service (for updating the access list);
- any significant/expected changes in the usage of the data service;
- maintenance works on the data service and the duration of the works.

g. The provider of the data service is notified of the following;
- any changes in the technical details of the security server (address, certificates);
- any maintenance works on the security server and the duration of the works;
- any circumstances concerning the provider of data services which the owner of the security server has become aware of.

h. The configuration of the services which have been removed from use (incl. end point certificates) are immediately removed from the configuration of the security server.

APP.EE.1.M6 Consumption of the X-tee data service through the security server

i. The required probative value of the X-tee data service has been agreed on (i.e. the levels of the e-seal and timestamping).
a. The security server service is only consumed in the manner agreed on with the owner of the security service and from the addresses agreed on.
b. Every IT system or a logical part thereof has a separate X-tee subsystem for using data services. The description and technical parameters of the subsystem are documented.
c. Unique message identifiers are used in the X-tee messages.
d. The unique identifier of an authenticated user or pseudonym which can be linked back to it (if required in the description of the service) is added to the X-tee messages.
e. Consuming the X-tee security server service without the mediation of an authorised information system is blocked.
f. The owner of the security server is notified of any changes in the interfacing of the information system with the security server and of any significant/expected changes in the usage stress of the data service.
g. Consumers of the security server are notified of the following:

• any changes in the technical details of the security server (address, certificates);
• any maintenance works on the security server and the duration of the works;
• any circumstances concerning the consumer of the security server which the owner of the security server has become aware of.

h. The configuration of the services which have been removed from use (incl. end point certificates) are immediately removed from the configuration of the security server.

APP.EE.1.M7 Agreements for X-tee data services

a. The provision/consumption of a data service is based on a bilateral agreement which describes the following, among other things:
• the nature of the data service;
• the legal grounds (incl. the legal grounds for using the data provided through the service, the promised goals, the details of data retention and disposal of data);
• the administrative and technical contact details and the procedure for updating the details;
• the requirements for availability;
• the X-tee identifiers of the provision and consumption of the data service;
• the characteristics or network addresses (if necessary) of the security servers used for providing and/or consuming the data service;
• the method and interval of mutual verification of secure management (e.g. sharing the respective parts of the E-ITS audit report, another certificate or audit, direct inspection).

b. Consumers of the data services are notified of the following:
• any changes in the nature of the data service;
• maintenance works on the data service and the duration of the works.

c. The provider of the data service is notified of the following;
• any significant/expected changes in the usage of the data service;
• termination of the use of the data service.

APP.EE.1.M8 Secure interfacing of the X-tee data service

a. There is a mutually authenticated TLS connection between the security server and the data service, the TLS certificates of the security server and information system of which are verified.

b. Every data service provider/consumer uses a unique TLS key. Reuse or multiple use of the key is prohibited.

c. In the event of using protocols which have not been authenticated and/or encrypted, further

security measures which ensure confidentiality and integrity are applied.
d. The data service can only be used through the authorised security server.

APP.EE.1.M9 Developing and testing the X-tee data service

a. The development and testing operations of the security server and data exchange interface are conducted in the development or testing environment.
b. It is not permitted to use the data or services of the production environment (operational environment) in the development and testing environments.
c. The security measures of the security server and data services of the development and testing environments prevent the abuse of those environments and attacks against those environments.

APP.EE.1.M10 Archiving the message log of the X-tee security server

a. There is an agreement with the owner of the security server which includes the following:
- archiving the message log in the infrastructure owner of the security server;
- or the transportation and archiving of the message log in the infrastructure of the consumer of the security server.

b. The retention periods of the message log and the procedure for accessing the logs have been defined.

APP.EE.1.M11 Terminating the provision of the X-tee data service

a. The consumers of the X-tee data service and the owner of the security server are notified before terminating the provision of the X-tee data service.
b. It is made sure that the owner of the security server has removed the configuration elements related to the respective data service (technical description of the service, access lists, the X-tee subsystem, etc.).
c. In the event of termination of the provision of the X-tee data service, the retention of the message logs based on the requirements of the business process is ensured.

APP.EE.1.M12 Ceasing the use of the X-tee data service

a. Before ceasing to use the X-tee data service, the provider of the X-tee data service is notified thereof for them to remove the access right.
b. In the event of termination of the provision of the X-tee data service, the retention of the message

logs based on the requirements of the business process is ensured.
c. The TLS keys which were used for the communication between the security server and the information system are destroyed and any further use thereof is excluded.

APP.EE.1.M13 Secure termination of the use of the security server

a. The owner of the security server is notified before ceasing to use the security server.
b. The retention of all message logs (incl. those yet to be archived) is ensured.
c. The certificates which were used in the security server are cancelled.
d. With the help of the owner of the security server, an application for the removal of any unused configuration elements (any subsystems, organisations, etc. which will remain unused) from X-tee is filed.
e. It is checked whether the owner of the security server has removed the configuration elements and keys used for the consumption of the security server.

3.3 Standard measures

APP.EE.1.M14 Regular reviews of the documentation of the X-tee data service

a. The following aspects of the X-tee data services are checked regularly:
- the need for the services;
- the validity of the legal grounds;
- whether or not the access list is updated;
- compliance with the conditions specified in the agreement for the use of the data service:
- whether or not the documentation and technical specifications published (incl. in the X-tee self-service portal) are updated.

APP.EE.1.M15 Agreement for the consumption of the security service

a. The owner of the security server and the consumer of the security server conclude an agreement for the consumption of the security server service. The agreement is based on the standard terms and conditions of the security server service, but may include further terms and conditions.
b. The agreement must include at least the following:
- authorised contact persons and the respective contact details;
- the procedure for reviewing and updating the data;
- the communication paths agreed, the authorisation checks for service requests, and the response

times;

• authorising the owner of the security server to keep and activate the keys of the e-seal of the organisation;

• if necessary, authorising the owner of the security server to communicate with the trust service provider (for applying for and, if necessary, cancelling signing certificates);

• the mutual obligation to process the data related to the security server service (incl. the data of the service, message logs) based on the protection requirement of the data (confidentiality, integrity, availability);

• the procedure for granting access to, storing, and delivering to the client the message logs and service inquiry logs;

a service level agreement on the volume, nature, and availability of the services;

• the security requirements of the authorised end points of the service provider(s) (IP addresses, technical specifications of the services) and the procedure for reviewing the requirements.

APP.EE.1.M16 Using the security server as a consumer

a. The contact details of the authorised persons provided to the owner of the security server are accurate and are updated immediately in the case of any changes.

b. The email address for receiving notices is redirected to a separate address/mailing group with more than one recipient.

c. Messages from the owner of the security server are responded to depending on the level of priority of the message.

d. Unused certificates are cancelled immediately.

APP.EE.1.M17 Logging and monitoring the X-tee data service [IT department]

a. The logs of the information system used for providing or consuming the data service are processed and retained based on the policies of the organisation.

b. The operation, resource consumption, and the metadata of the message exchange of the operation system used for providing or consuming the data service are monitored based on the goals of the organisation.

3.4 Advanced measures

APP.EE.1.M18 High availability of the X-tee data service (A)

a. In order to ensure that the X-tee data service is failsafe and/or improve the performance of the service, several copies of the service are operated, with a load balancer used to direct the traffic.
b. The copies of the data service are kept synchronised by using technical or procedural measures.

APP.EE.1.M19 Secure use of the private key of the e-seal of the organisation (C)

a. In cooperation with the owner of the security server, it is ensured that a qualified e-seal creation tool (HSM) is used to create, use, and store the private key of the e-seal used on X-tee.

APP.EE.1.M20 Using qualified e-seals (C-I)

a. In order to improve the probative value of the data exchange, the provider of the data services requires the use of qualified e-seals from the consumers of the data service.
b. The data service provider uses a qualified e-seal in responses to inquiries.

IND: INDUSTRIAL IT

IND.1 Operational technology. Process control and automation technology

1 Description

1.1 Purpose

To present organisational and conceptual measures for the secure use of operational technology (OT), including process control and automation technology and SCADA systems in an organisation.

1.2 Responsibility

The operational technology department is responsible for compliance with the security measures for operational technology and process control and automation technology.
Additional responsible persons: IT department, employees, information security manager, architect.

1.3 Limitations

The technical implementation of operational technology and process control and automation technology can vary greatly due to the differences in the purpose, components, and technologies of the system. When designing security measures in accordance with the measures of this module, these variations must be taken into account.
The module ORP.3 Increasing awareness of information security and training is implemented to raise the awareness of employees about information security. In case of process control and automation technology, measures from the modules ORP.4 Administration of identity and rights and OPS.1.1.5 Logging are also applied.

2 Threats

2.1 Damage caused by environmental factors

Under industrial conditions, the components of the operational technology and the process control and automation technology are exposed to detrimental environmental factors. Adverse environmental factors (such as extreme heat, cold, dampness, dust, vibration, corrosive substances) could significantly affect the functioning of such components. Often, several factors occur together. The lifespan of the components could be shorter in an adverse environment - they could degrade faster and malfunction earlier.

2.2 Inadequate integration of operational technology with the security structure

Due to the technical or organisational differences in the office IT and industrial control systems, the general security requirements of an organisation might be implemented insufficiently or not to their full extent in the case of operational technology. If the persons responsible for information security are not familiar with the characteristic information security and functional safety aspects of the industrial control systems, the threats related to the use of operational technology could realise.

2.3 Inadequate management of operational technology and process control and automation technology

Using standard procedures for IT management is not sufficient to compensate for all vulnerabilities of the operational technology in the case of operational technology devices. If the peculiarities of operational technology are not considered when managing changes and incidents, configuring devices, repairing malfunctions, or installing security updates, it could cause interruptions in production, financial losses, injuries, or environmental damage due to malfunctions in the

operational technology and process control and automation technology. Unauthorised changes in the relevant components could affect the security of the system in addition to its functional impact.

2.4 Inadequate access security

If a communication channel with inadequate security is used for integrating the operational technology and process control and automation technology with the central production control and ERP systems of the organisation, the channel could be used for attacking the operational technology and process control and automation technology. If the network is not separated from the office network, all attacks aimed at the computer network of an organisation immediately threaten the functionality of the process control and automation technology. In addition, it is difficult to implement intrusion prevention systems (IPS) and anti-malware in the operational technology environments because the active interference of the software in the functioning of the system could threaten the completion of work processes.

2.5 Insecure development process of applications

Rash changes and developments of the applications and supervisory programs of the operational technology could cause malfunctions in using the operational technology. An insecure development environment, faulty source code, neglecting to validate input, or insecure data communication interfaces present additional threats.

2.6 Insecure remote administration

The remote administration of process control and automation technology using public networks (mobile networks, internet) could afford unauthorised access to the components or infrastructure of the operational technology. Remote access that is configured insecurely or has inadequate monitoring capabilities allows attackers to avoid the security mechanisms of the network perimeter.

2.7 Inadequate monitoring and detection procedures

The monitoring functions of the process control and automation technology (warnings related to the process; indicators of technical parameters) need a supporting IT infrastructure to function. Lack of control over events in the network, attack attempts, and network congestion could cause malfunctions in the exchange of information with the control system. Incidents could remain undetected in time.

2.8 Insufficient testing

If changes in the operational technology and process control and automation technology are not carefully planned, coordinated, and tested in an environment resembling the actual system, the mistakes in logic or software and malfunctions in the industrial control systems could cause significant damage. An untested update that has been issued by the manufacturer could cause malfunctions in the process control and automation technology due to a wrong parameter value.

2.9 Inadequate concept of the life cycle

As the life cycle of the operational technology components is significantly longer than that of the office IT devices, the networks of operational technology and process control and automation technology may be using hardware and software components (such as operating systems) that are no longer supported by the manufacturer. When updates are no longer issued for the elimination of vulnerabilities, the known vulnerabilities can be used for attacking the systems. The same threat persists when updates are not installed or installed with a great delay.

2.10 Insecure procurement

In case of failing to provide a sufficient overview of the information security requirements when preparing a procurement for operational technology devices, the operational technology and process control and automation technology could have vulnerabilities which cannot be eliminated later. However, describing the system in too great a detail in the procurement conditions could reveal undue information about the processes and business secrets of the organisation.

2.11 Use of insecure protocols

Specific industrial automation protocols are used in the operational technology components in addition to the well-known network protocols (such as Ethernet, TCP/IP, GSM), which are not always developed with the requirements of information security in mind. Therefore, security mechanisms could sometimes be missing completely or be applicable to a limited extent only. Information could be transmitted as cleartext or without secure authentication. An attacker who has access to the network can read or change the contents of the communication and, through that, affect the processes by simulating sensor signals or forging commands, for example.

2.12 Insecure configuration

The security functions of the default configuration of the operational technology components are not always activated. A component with insecure configuration could threaten the security of the entire system (e.g. if a default password is used for access). An example of insecure configuration is the use of unnecessary services and insecure interfaces (e.g. USB and Firewire ports).

2.13 The dependence of the operational technology on the IT networks

If the operational technology and process control and automation technology are not designed to function completely separately from the rest of the network, then the disruptions in the intranet and other IT incidents affect the use of the operational technology directly. As the computer networks are generally not under the control of the user of the organisation's operational technology infrastructure, the incidents can only be solved with external help. Examples of such dependence are internet connections (cable and mobile connections), infrastructure components in public use, and cloud services.

3 Measures

3.1 Life cycle

Planning	
IND.1.M1	Integration with the security management
IND.1.M11	Secure acquisition and system development
IND.1.M12	Establishing the procedure for managing vulnerabilities
Implementation	
IND.1.M3	Anti-malware
IND.1.M4	Documenting the infrastructure of operational technology
IND.1.M5	Development of zoning principles
IND.1.M6	Managing the changes in the operational technology and process control and automation technology
IND.1.M7	Central administration of rights
IND.1.M20	Extended system documentation
IND.1.M21	Documenting the communication pathways
Operation	
IND.1.M18	Logging the operational technology and process control and automation technology

IND.1.M19	Backup copies
IND.1.M8	Secure management of the operational technology components
IND.1.M9	Restricting the use of removable data carriers and mobile devices
IND.1.M10	Monitoring, logging, and detecting incidents
IND.1.M22	Central logging and monitoring

Disposal

IND.1.M23	Disposal of operational technology components

Additional advanced measures

IND.1.M13	Emergency preparations for the operational technology and process control and automation technology
IND.1.M14	Strong authentication of the operational technology components
IND.1.M15	Supervision and monitoring of rights
IND.1.M16	Strong isolation of zones
IND.1.M17	Regular security review
IND.1.M24	Communication in the event of a malfunction

3.2 Key measures

IND.1.M1 Integration with the security management [information security manager]

a. An independent information security management system has been created for the management of the security of the operational technology and process control and automation technology or it has been integrated with a comprehensive information security management system (see also ISMS.1 Security governance).
b. Security management involves all interested parties of the operational technology and process control and automation technology.
c. The organisation has appointed a person who is responsible for the information security of the operational technology and process control and automation technology.
d. The legislative acts, guidelines, and special requirements pertaining to the operational technology are taken into consideration in the information security management.

IND.1.M3 Anti-malware

a. The following components of operational technology and process control and automation technology are checked for malware:

• external interfaces;
• connections with the intranet, internet, and partner networks;
• removable data carriers;
• maintenance, setup, and programming terminals;
• new components (such as disks, software).

b. The guidelines of the manufacturer of the operational technology components for the use of anti-malware are taken into account; if necessary, alternative protective measures are implemented.

c. The operational technology systems must not acquire known virus signature files straight from the internet.

IND.1.M4 Documenting the infrastructure of operational technology

a. Comprehensive, up-to-date, and practical documentation has been prepared for the management of the operational technology infrastructure, incl. a list of assets.

b. The list of assets includes updated information on all software, system, and network components:
• name, designation, purpose;
• location, physical security zone;
• person responsible (with contact details);
• the model, type, version, and configuration of the product, patching status of software;
• the environment/platform, interfacing data, data exchange of the product;
• network information (network map with zones, ports, protocol version);
• data of the manufacturer, licences, certificates, information exchange with the manufacturer;
• backup data, backup status;
• management and maintenance information.

c. The documentation management of operational technology and process control and automation technology is automated.

d. The protection of documents corresponds to the security requirements of the data.

IND.1.M18 Logging the operational technology and process control and automation technology

a. All changes to the components of the operational technology and process control and automation technology are logged.

b. All successful and failed access attempts to the process control and automation technology are logged.

IND.1.M19 Backup copies [employee]

a. Regular backup copies are made of the software and data of the operational technology and process control and automation technology.
b. In addition, backup copies are made before and after changing the components of the operational technology and process control and automation technology.

3.3 Standard measures

IND.1.M5 Development of zoning principles [architect]

a. When creating security zones, the objects and functions of the operational technology and process control and automation technology and their distinct protection requirements as compared to an office network are taken into consideration.
b. The networks of the operational technology and process control and automation technology are designed to withstand malfunctions and attacks.
c. The network segments of operating the system are as independent as possible. Zones for controlling industrial processes must be available even in case of a malfunction in or when separated from another zone; the required period is established in the procedure for emergency management.
d. Regular checks are conducted to discover and eliminate undocumented communication links.

IND.1.M6 Managing the changes in the operational technology and process control and automation technology

a. The organisation has established, documented, and implemented a process for changes in the operational technology and process control and automation technology.
b. When managing the changes in the operational technology and process control and automation technology, the general change management measures are implemented (see also OPS.1.1.3 Patch and change management).

IND.1.M7 Central administration of rights [information security manager]

a. The management of user access rights of the operational technology and process control and automation technology (applying for rights, management of rights, and establishing, revoking, and documenting rights) is based on the established guidelines for the management of user access rights (see also ORP.4 Administration of identity and rights).

b. Rights are granted based on the role and according to the principle of least necessity. In the case of all role and staff changes, the access rights of affected individuals are reviewed.
c. Workstation-based access rights through firewalls or access control lists of routers are considered to be the granting of user rights in accordance with the access rights management procedure.
d. The status and history of rights are documented in a reviewable manner.
e. The use of operational technology and process control and automation technology can be detected (see also IND.1.M10 Monitoring, logging, and detection).
f. Access rights are regularly checked; sanctions can be applied when rights are abused.

IND.1.M8 Secure management of the operational technology components [IT department]

a. For the initial configuration of operational technology components, a checklist has been prepared which determines based on the component:

- the deactivation of useless or insecure functions, interfaces, and other such elements;
- the activation of security functions;
- the regulation of access and authentication;
- replacing initial passwords;
- remote access and maintenance;
- synchronisation of time;
- logging.

b. Partitioned administrative networks are used for the remote maintenance of the operational technology components which implement secure protocols and secure authentication.
c. Access to the maintenance interfaces is limited to the persons with the respective rights.
d. Access is granted to only these systems and functions which are necessary for completing a specific administrative task.
e. As a minimum, the applications and communication channels which are used in the remote management of the components have the same protection requirement as the managed operational technology and process control and automation technology.
f. The authorisation, monitoring, and management of the remote maintenance and remote administration processes are regulated. Remote maintenance access is only activated for a specific instance and deactivated once the task has been completed. The maintenance activities are documented.
g. Additional access routes cannot be established for remote access.

h. Business-critical administrative proceedings requiring higher levels of security can be conducted only with several administrators cooperating.

IND.1.M9 Restricting the use of removable data carriers and mobile devices

a. Guidelines for the use of removable data carriers and mobile devices are established for the operational technology.
b. In the production environment of the operational technology, connecting removable data carriers and mobile devices is restricted; all exceptions are documented.
c. The use of data carriers and devices in the possession of service providers is allowed only with a written approval. The respective requirements have been approved in writing by the service providers.
d. Unnecessary interfaces of the operational technology components are deactivated. If possible, the use of data carriers and mobile devices is restricted in the activated interfaces.

IND.1.M10 Monitoring, logging, and detecting incidents

a. The organisation has established a procedure for the management of logs and events in the operational technology and process control and automation technology, which includes measures for the detection of security incidents, reporting them, and a plan for handling such incidents.
b. The incident handling plan is based on the general security incident handling process of the organisation (see also DER.2.1 Handling of security incidents). The plan for handling incidents includes incident classification, reporting routes, relevant structural units, event analysis and documentation, the recovery of systems, and incident follow-up.
c. The feasibility and up-to-dateness of the incident handling plan is checked regularly (at least once a year) and the plan is adjusted if necessary.
d. As a minimum, the following events are logged when using the operational technology and process control and automation technology:

- starting and restarting the system;
- important events in the operational technology platform;
- service initiation;
- logins and login attempts;
- management and maintenance operations;
- results of anti-malware programs;
- events in the network (interruptions in the connection, blocked messages, congestions);

• error and malfunction messages regarding security.

e. The system time of the operational technology components is taken from trustworthy sources; it is constantly synchronised with an external reference time and uses a standard format (time zone, daylight saving time).

f. In case of a high protection requirement, an intrusion detection system (IDS) is used in the operational technology system.

IND.1.M11 Secure acquisition and system development [information security manager]

a. Compatibility, reliability, and security requirements based on the necessary protection requirement are established and documented for the acquisition, development, and integration of operational technology and industrial control systems. These requirements are considered integral parts of tender documents.

b. Information security measures are planned in the early stages of the development of operational technology and industrial control systems.

c. Confidentiality agreements are concluded with contractual partners (developers, suppliers, or external operators).

d. Recommendations of manufacturers or integrators are observed for the safe use of operational technology components.

e. Measures for continuing with the activities of the organisation have been established for instances when an operational technology partner decides to stop providing their services (see OPS.2.3: Outsourcing).

IND.1.M12 Establishing the procedure for managing vulnerabilities

a. In order to guarantee the security of the operational technology and process control and automation technology, a procedure for the management of vulnerabilities is established. The procedure handles the software of the operational technology components, the identification of the vulnerabilities of protocols and external interfaces, and the planning of further action.

b. In order to identify vulnerabilities, the published vulnerability reports of the relevant interested parties (e.g. manufacturers and CERT) are monitored.

c. Corrective measures (e.g. security patches) are planned and implemented after assessing the identified vulnerabilities (e.g. according to the CVSS criteria).

d. For predicting and preventing the vulnerabilities of the operational technology components, the support and service life of the components are tracked.

e. In order to identify the vulnerabilities in the operational technology and process control and automation technology, regular reviews and audits are conducted.

IND.1.M20 Extended system documentation

a. The operational technology and process control and automation technology are documented in sufficient detail for their use and management.
b. As a minimum, the system documentation includes:
- the possible instances of use (for example, regular maintenance, changing and repairing components, external services);
- description of organisational peculiarities;
- guidelines for system management (including remote management);
- chronology of the changes in the components of the industrial control system.

c. All changes in the operational technology components are documented at the earliest opportunity.
d. The documentation is protected against unauthorised access.
e. The documentation is available in case of malfunctions.

IND.1.M21 Documenting the communication pathways

a. The data exchange partners, data categories, and the technical specifications of data exchange of the components of the industrial control system are documented.
b. When new components are added, the documentation on data exchange connections is updated.

IND.1.M22 Central logging and monitoring

a. The log data for the operational technology and process control and automation technology is sent to a central log system.
b. Log data is analysed regularly.
c. The potential security-critical events that are identified in the course of automatic monitoring are reported automatically to the responsible employees.

IND.1.M23 Disposal of operational technology components

a. When disposing of old or defective operational technology components, all sensitive data is deleted securely from the automation component.

b. When disposing of an automation component, all access data of users must be deleted from the device.

3.4 Advanced measures

IND.1.M13 Emergency preparations for the operational technology and process control and automation technology (A)

a. An emergency plan has been established and documented for each security zone (see also module DER.4 Emergency management) which, as a minimum, takes into account the following emergency scenarios:

- long-term interruption of the internet connection (over one week);
- complete shut-down of the office IT for a certain time (e.g. 2 days);
- temporary malfunction of the vital IT components of operational technology;
- security failure of the vital IT components of operational technology due to an attack or malware infection.

b. A procedure for backup and recovery has been developed for the operational technology and process control and automation technology, which establishes:

- the procedures for backup, recovery, and regular testing of backup copies;
- procedures for the recovery of systems;
- repair of defective components;
- need for and storage of spare parts;
- alternative communication and control options in the case of malfunctions.

c. The functioning of the emergency management of operational technology is evaluated regularly (at least once a year). For this purpose, the emergency management is tested, emergencies are simulated, and the recovery operations are practised.

d. The duplication and redundancy of the support systems (e.g. power supply, network components, management routes) necessary for the functioning of the components of the operational technology and process control and automation technology are used.

e. In case of a very high availability requirement, a backup control centre has been established in a second location which can be launched during a specific time, should the main control centre malfunction.

IND.1.M14 Strong authentication of the operational technology components (C-I-A)

a. Wherever possible, the identification and authentication of the user is required to use and maintain the components (including network devices) and services.
b. Multi-factor authentication is used for secure authentication.
c. For emergencies, local system and application accounts have been created which are stored securely.
d. When planning an authentication solution, the mutual independence of security zones is taken into consideration.
e. The configuration and changes in the authentication systems are documented and the systems are monitored regularly for the detection of incidents.

IND.1.M15 Supervision and monitoring of rights (C-I-A)

a. The organisation has prepared a list of assets which includes the current status and history of changes of the access rights of all important units of operational technology and process control and automation technology (see also IND.1.M7 Central administration of rights).
b. The list of assets allows checking the rights of a specific user in all systems, and vice versa, the rights of individual users of each system.
c. All significant administrative operations are logged (see also IND.1.M10 Monitoring, logging, and detecting incidents).
d. Logs are protected from unauthorised erasure and changes based on the principle of the separation of duties.

IND.1.M16 Strong isolation of zones (I-A)

a. In order to protect the operational technology and process control and automation technology which are hard to secure on the system and network level, interfacing systems with preventative security control functions are used.
b. The operational technology and process control and automation technology has been adjusted to a P-A-P structure (packet filter - application level gateway - packet filter) or demilitarised zone(s) are created with it for the mitigation of risks which enable virus protection, data format control, and monitoring and filtering the contents of messages.
c. Additional organisational and technical information security measures have been implemented for the prevention of deliberate or accidental bypassing of the secure perimeter (e.g. by using portable data carriers and mobile devices).

IND.1.M17 Regular security review [information security manager] (I)

a. The compliance of the security concept of the operational technology components with the security policy and the up-to-dateness of the component configuration is reviewed periodically and/or according to need when new threats emerge, for example.
b. As a minimum, the security review entails the systems which are more open to threats due to external interfaces or direct access to users.
c. The reviews include the evaluation of vulnerabilities and practical testing. When conducting penetration tests, its potential effects on the availability of the system are taken into account.

IND.1.M24 Communication in the event of a malfunction [employee] (A)

a. Alternative backup communication channels using a different technology are established for the use of the operational technology and process control and automation technology in case of a malfunction of the communication systems.

IND.2 Industrial control system

IND.2.1 Components of an industrial control system in general

1 Description

1.1 Purpose

To present the measures for the security of the industrial control systems, including the components of the process control and automation technology and SCADA (Supervisory Control and Data Acquisition), regardless of the manufacturer, architecture, purpose, and place of installation of the components.

1.2 Responsibility

The operational technology department is responsible for the implementation of the measures of the module 'Components of an industrial control system in general'.
Additional responsible persons: Employee, architect, maintenance staff.

1.3 Limitations

The measures are generalised to all components of automation. The technical measures for specific components of an industrial control system are presented in other modules of the module group IND.2 Industrial control system. The organisational measures of the operational technology are presented in the module IND.1 Operational technology and process control and automation technology.

2 Threats

2.1 Insecure configuration of the system

The default settings of a component of an industrial control system do not restrict the operational possibilities of the component. If all functions are activated in the configuration of the components of the industrial control system and the services are active even when not in use, an attacker can gain access to the device more easily. A device that has been hijacked due to a default password that has not been changed or a configuration error of the device can be used as a starting point for future attacks on the industrial control system.

2.2 Inadequate management of users and rights

Some of the components of the industrial control systems have an autonomous function for managing users and rights. If the access rights are not centrally managed, unauthorised persons could gain access to the components of the industrial control system. When there is no clear overview of the access rights, the employees could use a shared user account or the accounts of the service providers could remain active.

2.3 Inadequate logging

If only events related to the automated process are logged, important data and events regarding the components of industrial control system from the point of view of information security remain unnoticed. This makes security events difficult to detect and the incidents that have already occurred cannot be analysed at a later time.

2.4 Manipulation and sabotage of the components of the industrial control system

The various interfacing options of the components of the industrial control system bring along the danger of manipulating systems, software, and the forwarded information. An attacker could block or change the status and error messages or other measuring results in the automation components. The manipulated measurement results could lead to erroneous decisions of other components or the staff servicing the system. The manipulated systems could be used for hiding other manipulations or attacking other systems and locations.

2.5 Insecure protocols

The industrial control systems often use protocols with absent or inadequate security mechanisms. The technical information is forwarded as plaintext without an integrity control and previous authentication. An attacker who has access to the communication channels can change the content of communication or interfere with control commands and affect the operation of the devices this way. On the level of protocols, an attack is possible even if other configuration of components is secure and without vulnerabilities.

2.6 Denial-of-service attacks (DoS)

An attacker can affect the use of components of the industrial control system through denial-of-service attacks. In case of real-time processes, a short-term disturbance could cause loss of information or control over processes.

2.7 Malware

Even isolated industrial control system networks can be infected with malware. The possible infections come from interfaces with external environments and the office IT. Laptops used for maintenance and removable data carriers used for programming and maintenance of components of the industrial control system pose a great threat. Through the latter, malware can transfer even in isolated environments.

2.8 Data intelligence

The components of the industrial control system contain detailed information on the processes or operations. Even forwarded indicators (such as measuring or control signal data and control programs) can be used for deducting information that is classified as a business secret. An attacker could gain access to business secrets (industrial espionage) or intellectual property. In addition,

information about the working principles and security mechanisms of the components of the industrial control system is acquired for future attacks.

2.9 Manipulated firmware

In addition to application programs, firmware can also be altered on the components of the industrial control system. When using manipulated firmware, local interfaces (such as USB ports) can be programmed or the operation of the component can be affected through an existing network connection. A software update can be manipulated while it is being transferred from the manufacturer to the users. A purchase from an insecure source could supply an operator with a component that has firmware which is already compromised. An attacker gets an opportunity for changing and forging processes and procedures.

3 Measures

3.1 Life cycle

Operation

IND.2.1.M1	Restricting access to configuration and maintenance interfaces
IND.2.1.M2	Use of secure protocols for configuration and maintenance
IND.2.1.M7	Data backup
IND.2.1.M8	Anti-malware
IND.2.1.M11	Maintenance of the components of the industrial control system
IND.2.1.M16	External interface security
IND.2.1.M17	Secure data connection protocols

Implementation

IND.2.1.M4	Deactivation and uninstallation of superfluous services, functions, and interfaces
IND.2.1.M6	Network segmentation

Planning

IND.2.1.M13	Procedure for the commissioning of the components of the industrial control system

Additional advanced measures

IND.2.1.M18	Emergency communication
IND.2.1.M19	Security tests
IND.2.1.M20	Trustworthy program code

3.2 Key measures

IND.2.1.M1 Restricting access to configuration and maintenance interfaces

a. Only authorised employees have access to the configuration and maintenance interfaces of the components of the industrial control system.
b. The standard user accounts of the devices are blocked and the default passwords are changed (see also ORP.4 Administration of identity and rights). New passwords are stored in a secure manner.
c. Only an authorised and authenticated employee can change the configuration of the components of the industrial control system. Changes in the configuration are documented.

IND.2.1.M2 Use of secure protocols for configuration and maintenance [maintenance staff]

a. Secure protocols are used for the configuration and maintenance of the components of the industrial control system.
b. Data that is forwarded during the configuration and maintenance is protected.

IND.2.1.M4 Deactivation and uninstallation of superfluous services, functions, and interfaces [maintenance staff]

a. All superfluous services, functions, and interfaces of the components of the industrial control system are deactivated or uninstalled.

IND.2.1.M6 Network segmentation [architect]

a. The components of the industrial control system are partitioned from the office IT systems.
b. The dependencies of the work of the components of the industrial control system on network services have been documented.
c. The communication of the components of the industrial control system with other components is based on necessity and is as minimal as possible.

3.3 Standard measures

IND.2.1.M7 Data backup

a. Regular backup copies are made of the programs and data.
b. In addition, a backup copy is always made after system changes.

IND.2.1.M8 Anti-malware

a. The components of the industrial control system are protected from malware (see also OPS.1.1.4 Protection from malicious programs).
b. Anti-malware and virus signatures have been updated to the latest version.
c. When the anti-malware cannot be used on a component due to its lack of resources or real-time requirements, compensating measures are implemented (such as isolating the production network of the operational technology).

IND.2.1.M11 Maintenance of the components of the industrial control system [maintenance staff]

a. The new and approved security updates are installed during the regular maintenance of the components of the industrial control system.
b. The updates to the operating system are installed on the operational environment component only after receiving approval from the manufacturer of the component and after it is tested in the testing environment.
c. When critical security updates are released, maintenance for their installation is done at the earliest opportunity.

IND.2.1.M13 Procedure for the commissioning of the components of the industrial control system

a. The components of the industrial control systems are approved for use only when their firmware, software, and security updates comply with the current requirements.
b. The components of the industrial control systems are integrated into the processes of operation, monitoring, and information security management. First and foremost, it entails:

- the management of changes and rights;
- the management of vulnerabilities;
- anti-malware;
- operation monitoring and emergency preparedness;
- regular security reviews of the systems.

IND.2.1.M16 External interface security

a. Interfaces with external access (such as network interfaces, USB ports, and serial connections) are protected from misuse.

IND.2.1.M17 Secure data connection protocols

a. The measuring and control data is protected from unauthorised access and changes.
b. In case of real-time applications, the data is protected as needed and possible.
c. The measuring and control data that is forwarded through public networks is protected according to the requirements.

3.4 Advanced measures

IND.2.1.M18 Emergency communication [employee] (A)

a. In order to maintain operational capabilities in case of malfunctions, alternative and independent communication channels have been established.

IND.2.1.M19 Security tests (C-I-A)

a. The functioning of technical security measures is checked with regular security tests.
b. The testing is planned to take place during maintenance and is not conducted on working equipment.
c. The test results are recorded; the identified risks are analysed and handled.

IND.2.1.M20 Trustworthy program code (I-A)

a. Firmware updates and new control programs are only installed after checking the integrity and authenticity of the updates.

IND.2.2 Programmable logic controllers

1 Description

1.1 Purpose

To guarantee the security of programmable logic controllers (PLC) regardless of their manufacturer, purpose, architecture, or location.

1.2 Responsibility

The operational technology department is responsible for the compliance with the programmable logic controller measures.

1.3 Limitations

The general measures for the security of components of the industrial control system is presented in the module IND.2.1 Components of an industrial control system in general. The measures for the functional safety automation are described in the module IND.2.7 Safety automation. The organisational measures for the operational technology are presented in the module IND.1 Operational technology. Process control and automation technology.

2 Threats

2.1 Inadequate documentation

If the documentation of the programmable logic controllers is insufficient, important interfaces and security functions could be missed. If the documentation does not describe the usable functions, ports, and administration of rights in sufficient detail, vulnerabilities could remain uncorrected. In case of inadequate documentation, problems could arise when an employee working with the logic controllers leaves employment.

3 Measures

3.1 Life cycle

Operation

IND.2.2.M1 Complete documentation of programmable logic controllers (PLC)

IND.2.2.M3 Synchronisation of time

3.2 Key measures

3.3 Standard measures

IND.2.2.M1 Complete documentation of programmable logic controllers (PLC)

a. Control programs and the configuration of a logic controller are archived after every change.
b. The changes in the configuration and replaced components are documented.

IND.2.2.M3 Synchronisation of time

a. The synchronisation of system times is centralised and automatic.

3.4 Advanced measures

There are no advanced measures in this module.

IND.2.3 Sensors and actuators

1 Description

1.1 Purpose

To guarantee the security of smart sensors or a group of devices functioning as sensors regardless of their manufacturer, purpose, architecture, or location.

1.2 Responsibility

The operational technology department is responsible for the compliance with the measures for sensors and actuators.
Additional responsible persons: Maintenance staff.

1.3 Limitations

The general measures for the components of the industrial control system are presented in the module IND.2.1 Components of an industrial control system in general. The module does not discuss wireless sensor networks (see also SYS.4.4 Device in the internet of things (IoT) in general). The general security measures for the operating and control systems are described in the module IND.1 Operating and control technology.

2 Threats

2.1 Inadequate security requirements during the acquisition of products

When the information security does not receive sufficient attention due to inadequate risk awareness and additional costs during the acquisition of sensors, they could contain vulnerabilities, the elimination of which would be very expensive at a later time.

2.2 Incorrect calibration

If the sensors are calibrated incorrectly or unauthorised access to the calibration of sensors is possible, the sensor data might be unreliable and the sensors might send incorrect measuring results.

3 Measures

3.1 Life cycle

Implementation

IND.2.3.M1 Correct selection and installation of sensors

Operation

IND.2.3.M2 Calibration of sensors

Additional advanced measures

IND.2.3.M3 Avoiding wireless connection

3.2 Key measures

IND.2.3.M1 Correct selection and installation of sensors [maintenance staff]

a. When choosing and acquiring sensors, the trustworthiness of the manufacturer and the suitability of the sensors with the environmental conditions (temperature, dust, vibration, corrosion, etc.) are taken into account.
b. The sensors are installed according to the manufacturer's requirements.

3.3 Standard measures

IND.2.3.M2 Calibration of sensors [maintenance staff]

a. The sensors are calibrated regularly and the calibration is documented.
b. Unauthorised access to calibration is blocked.

3.4 Advanced measures

IND.2.3.M3 Avoiding wireless connection (C)

a. In case of a higher protection requirement, wireless networks (such as a Wireless Local Area Network (WLAN), near-field communication (NFC), or Bluetooth connection) are not used.
b. Unnecessary communication interfaces are deactivated.

IND.2.4 Robot devices

1 Description

1.1 Purpose

To present the security measures for electronically controlled semi-automatic or fully automatic robot devices (such as numerical control machine tools) regardless of their manufacturer, purpose, architecture, or location and the place of installation.

1.2 Responsibility

The operational technology department is responsible for the compliance with the measures for robot devices.

1.3 Limitations

The measures are meant for the robot devices which do not offer access to their internal configuration to the organisation. The general measures for the components of the industrial control system are presented in the module IND.2.1 Components of an industrial control system in general. The general organisational security measures of the operational technology are presented in the module IND.1 Operational technology. Process control and automation technology.

2 Threats

2.1 Malfunction or interruption caused by inadequate maintenance

If robot devices are not maintained regularly, the devices stop working correctly or malfunction. Failures and the unstable operation of robot devices could endanger employees and hinder production.

2.2 Deliberate manipulations

If the robot device interfaces are insufficiently protected, an attacker might be able to manipulate the parameters of the devices through local programming interfaces or a network. This way, the processed parts could be deliberately damaged or an entire product series be made defective. An attacker could also damage the device itself.

3 Measures

3.1 Life cycle

Operation

IND.2.4.M1	Remote maintenance security by the manufacturer
IND.2.4.M2	Procedure for operating the device after the end of the warranty period

3.2 Key measures

IND.2.4.M1 Remote maintenance security by the manufacturer

a. Central remote maintenance guidelines have been established, which determine which remote maintenance solutions are used, the protection measures for the data communication, and the monitoring measures for remote maintenance.
b. When remote maintenance is provided for robot devices, the person doing the maintenance does not have access to the other systems or robot devices of the organisation.
c. The procedure for using data that is stored in a robot device has been coordinated with the maintenance provider.

IND.2.4.M2 Procedure for operating the device after the end of the warranty period

a. A procedure for the secure use of the robot device after the end of the warranty period has been established.

b. A support service agreement with the supplier of the robot device has been concluded.

- There are no standard measures in this module.

3.3 Standard measures

3.4 Advanced measures

There are no advanced measures in this module.

IND.2.7 Safety automation

1 Description

1.1 Purpose

To present information security measures for the construction of a system of automated safety devices. In the context of this module, automated safety devices are sensors, actuators, safety-instrumented programmable control devices (logic system), application software and the associated programming devices, configuration consoles, and visualisation devices.

1.2 Responsibility

The operational technology department is responsible for the compliance with the measures for safety automation.
Additional responsible persons: Information security manager, architect, maintenance staff.

1.3 Limitations

The module complements the modules IND.1 Operational technology. Process control and automation technology and IND.2.1 Components of an industrial control system in general from the point of view of safety automation. The security of IT systems used for maintenance and administration as programming devices and visualisation devices is presented in the module SYS.2.1 Client computer in general.

2 Threats

2.1 Logic system manipulation

The manipulation of the application program of the logic system could disrupt the integrity of the automated safety devices. Unlike standard components of operational technology, the threat to humans, environment, and technical systems resulting from the manipulation of a component of a safety automation system could be far greater.

2.2 Inadequate monitoring and identification procedures

If the indicators of the operational statuses of the automated process, warnings related to the monitoring of the status (e.g. when exceeding the maximum load level), and technical parameters (temperature, position of valves) can be manipulated, it could have very severe consequences, including risk to human life and health. Lack of systems for identifying attacks and inadequate monitoring of automated safety devices makes manipulation possible. In the absence of monitoring, attacks cannot be detected in time.

3 Measures

3.1 Life cycle

Implementation

IND.2.7.M1	Registration and documentation
IND.2.7.M7	Segmentation of safety automation systems; its independence from the environment

Operation

IND.2.7.M2	The use of hardware and software components for specific purposes
IND.2.7.M3	Logic system security
IND.2.7.M5	Incident management of the safety automation devices
IND.2.7.M8	Secure forwarding of technical data to safety automation devices
IND.2.7.M9	Security of data and signal connections
IND.2.7.M10	Presentation of simulated or bridged variables; alarms
IND.2.7.M11	Managing the security of integrated systems

Planning

IND.2.7.M4	Linking information security with functional safety management
IND.2.7.M6	Protecting the integrity of safety automation technology

Additional advanced measures

IND.2.7.M12 Guaranteeing the integrity and authenticity of application programs and configuration data

3.2 Key measures

IND.2.7.M1 Registration and documentation [architect, maintenance staff]

a. The hardware and software components that belong in an automated safety system, their data and connections are documented.
b. The documentation of a safety automation system includes the following:
- the specification of signals used for data connection;
- the type of data;
- the protocol and direction of data exchange;
- security information (authentication, certificates, encryption);
- sub-units and positions responsible for the planning, implementation, maintenance, monitoring, inspection, and change processes of the safety automation system.

c. The documentation is updated in case of changes and checked at least once a year.

IND.2.7.M2 The use of hardware and software components for specific purposes [maintenance staff]

a. Software and hardware components that belong and are used in safety automation systems are not used for any other purpose.

IND.2.7.M3 Logic system security [maintenance staff]

a. The security mechanisms of the logic system are activated. If this cannot be done or the protection requirement is higher, organisational measures are added.
b. Only authorised persons can change the application programs of logic systems and approve the installation of the system.
c. Safety automation components are protected from unauthorised physical access.
d. Programming devices are connected to the system only when necessary and based on the session.

3.3 Standard measures

IND.2.7.M4 Linking information security with functional safety management [operational technology department]

a. The processes, rights and obligations related to the information security of the safety automation system are clearly established and integrated with the management process of functional safety.
b. The safety automation devices are managed according to the legislative requirements and safety standards.

IND.2.7.M5 Incident management of the safety automation devices [information security manager]

a. An incident handling plan for the safety automation systems has been established, determining the necessary roles and obligations.
b. As a minimum, the incident handling plan takes into consideration the following scenarios:
- interruptions in the communication of the safety automation system; security failure of a communication partner;
- the security failure of a sensor, actuator, or a logic system (e.g. malware in the maintenance console).

c. Action in case of incident scenarios is practised regularly.

IND.2.7.M6 Protecting the integrity of safety automation technology [architect, maintenance staff]

a. Possibilities for accidental and unauthorised changes to the specification, implementation, and technical parameters are blocked.

IND.2.7.M7 Segmentation of safety automation systems; its independence from the environment [architect, maintenance staff]

a. Safety automation devices are protected from detrimental environmental effects (including erroneous or congestive data).
b. A procedure for using substitute values is established for instances of losing the connection or data exchange with the environment.
c. The process changes that could affect the safety automation system are made through the functional safety management.

IND.2.7.M8 Secure forwarding of technical data to safety automation devices [architect, information security manager, maintenance staff]

a. Technical and organisational measures are applied for the protection of the authenticity and integrity of data forwarded to the safety automation devices.
b. Personal use of work devices is prohibited.
c. Forwarding data with removable data carriers is restricted (see also CON.9 Exchange of information).

IND.2.7.M9 Security of data and signal connections [architect, information security manager, maintenance staff]

a. Measures for ensuring the security of one-way connections have been implemented (such as a unidirectional security gateway).
b. Data and signal connections which need feedback (two-way) are protected. In case of two-way connections, the following measures are implemented depending on the necessity and physical protection:

- the communication partner of the safety automation system proves security with a security or risk assessment;
- the forwarded data is encrypted; the communication partner is authenticated;
- connections are always initiated from the environment of the safety automation system;
- data traffic is limited to the designated ports and addresses;
- the contents of the messages are monitored to detect potential anomalies.

IND.2.7.M10 Presentation of simulated or bridged variables; alarms [architect]

a. The variables which are simulated with a substitute value or bridged externally are monitored and the values are constantly and unambiguously reported to the user.
b. The value limits of these variables are defined and an alarm is activated when the limit is reached.

IND.2.7.M11 Managing the security of integrated systems [architect, maintenance staff]

a. A strategy is developed for the use of safety components in integrated systems.
b. Common use does not create security risks for the safety systems; the secure common-use components are sufficiently separated from the insecure ones.

3.4 Advanced measures

IND.2.7.M12 Guaranteeing the integrity and authenticity of application programs and configuration data [architect] (I)

a. Only such safety automation devices are acquired which have sufficient integrity and authenticity control mechanisms developed by the manufacturer.
b. The integrity and authenticity control mechanisms of the logic system or the configuration data and application programs of sensors and actuators related to it are activated and securely configured.
c. Integrity malfunctions are identified and reported automatically.
d. Software issued in a downloadable format is protected from manipulation. Firmware and its updates are received from the manufacturer in a signed form.
e. The programming and management devices of the safety automation system are not used for other purposes (are not connected to a network).
f. If necessary, compensatory security measures are implemented, such as segmenting the safety automation system to a demilitarised zone.

IND.3 Operational technology networks

IND.3.2 Remote maintenance of operational technology components

1 Description

1.1 Purpose

Presenting the measures for the secure remote management of operational technology (OT) components. Operational management and industrial control systems usually consist of the hardware and software components of different manufacturers and authorised maintenance personnel require remote access for the maintenance thereof.

1.2 Responsibility

The operational technology department is responsible for the implementation of the remote maintenance measures of the operational technology components.

Additional responsible persons: The IT department, architect, maintenance personnel, data protection specialist, employee.

1.3 Limitations

The module only includes measures which take into consideration the specifics of operational technology. Due to the peculiarity of a specific operational technology system, the measures applied to an OT component may differ from those described in this module.
Operational technology systems are also subject to the general remote maintenance measures from module OPS.1.2.5: Remote maintenance and the secure network architecture measures from module NET.1.1 Network architecture and solution.
This module does not cover the regular use and remote monitoring of industrial control systems (ICS) in an operating environment (e.g. activating or stopping processes).
The measures for the secure use of industrial control systems are presented in modules IND.1 Operational technology and industrial control systems and IND.2.7 Safety automation.
Further measures from the following modules are applied, depending on the organisation of remote maintenance of operational technology components: OPS.1.1.5 Logging, OPS.2.3: Outsourcing, OPS.2.2 Using cloud services, APP.3.1 Web applications.

2 Threats

2.1 Insufficient documentation of remote maintenance access rights

Employees of the organisation, manufacturers of the components, and external partners require access to the operational technology components of the organisation. In practice, various different technical solutions are used to grant remote access, and therefore, there is a risk of making mistakes in the management of access rights. Compared to the office computer network, the process of managing the access rights to operational technology systems is often significantly less efficiently regulated and documented.

2.2 Dependence of the operational technology network of the computer network of the organisation

Operational technology systems, unlike the computer network of the organisation, require real-time information and uninterrupted data communication connections. Merely a short-term operational disruption may cause critical errors in the ICS.

2.3 Insufficient requirements for the individuals responsible for remote maintenance

The general security requirements for the administration of the computer network of the organisation are often inappropriate for the operational technology network, as the requirements for the service are insufficiently restricted. The requirements for the configuration and change management which are suitable for the computer network may not be detailed enough for use in operational technology networks.

2.4 Lack of control over remote maintenance operations

The individuals responsible for providing remote maintenance must have the required prior knowledge about the system maintained. External partners have often not been informed sufficiently of the safety and security requirements of specific operational technology systems.

2.5 Access to an operational technology component from an insecure network segment

Access to the operational technology network from any networks or network segments which are not required for operation or management puts to risk the security of the operational technology system. Different segments of the intranet of the organisation are also not at the same level of reliability. Malware spreading in the network segment of the devices of end users may spread from there into the operational technology network. Operational technology components may not be as efficiently protected against malware as the end devices which are equipped with anti-malware.

2.6 Insufficient back-up options for remote access

In order to register potential errors of operational technology components, there must always be access to the OT components. Thus, a back-up solution is needed for the operational technology networks in the event of a failure of the main technological solution. Such an alternative remote maintenance access may be vulnerable to an attacker. For example, a GSM modem installed directly in the operational technology network as a back-up solution may be in conflict with the security policy established at the organisation.

2.7 Insecure execution of remote maintenance solutions

Components of an operational technology system are often created by different manufacturers. Several different remote maintenance solutions are required for the remote maintenance of a

decentralised system. Different access solutions that are preferred by different manufacturers and that are based on different technologies make the management of remote maintenance and ensuring security complicated for an operational technology department.

2.8 Technological underdevelopment of the remote maintenance solution

Due to the long life cycle of operational technology systems, it is common for one system to be used for a decade or more. The access systems used for remote maintenance no longer receive security updates due to their age.

3 Measures

3.1 Life cycle

Planning

IND.3.2.M1	Designing the remote maintenance of operational technology components
IND.3.2.M4	Agreements for external remote maintenance

Operation

IND.3.2.M2	Consistent documentation of the access rights of OT components
IND.3.2.M3	Checking access rights for the remote maintenance of OT and managing exceptions
IND.3.2.M6	Security of remote maintenance solutions in the operational technology network
IND.3.2.M7	Decoupling IT systems from an operational technology network
IND.3.2.M8	Controlled initiation of a remote maintenance session
IND.3.2.M9	Secure transmission of files in the course of remote maintenance
IND.3.2.M10	Monitoring and inspecting remote maintenance
IND.3.2.M11	Central administration of the OT user accounts

Implementation

IND.3.2.M5	Coordination of maintenance procedures with the IT department

Additional advanced measures

IND.3.2.M12	Special solution for the remote maintenance of operational technology
IND.3.2.M13	Expanded logging of remote maintenance operations
IND.3.2.M14	Technical inspection of a remote maintenance session

3.2 Key measures

IND.3.2.M1 Designing the remote maintenance of operational technology components [architect]

a. There is an organisation-wide procedure for ordering and performing the remote maintenance of operational technology (OT) components.
b. The procedure for remote maintenance of OT takes into consideration the following aspects:
- legal requirements, including the protection of personal data;
- technical specifications of OT components and recommendations from manufacturers;
- security requirements arising from the separation of networks;
- requirements for interfacing and data communication connections;
- requirements for the availability of remote maintenance;
- special requirements arising from environmental conditions;
- compatibility with existing systems.

c. The procedure for remote maintenance is observed by all employees of the organisation and external partners concerned.
d. All technical solutions used for remote maintenance are documented centrally.
e. In the case of any new OT components, the requirements for information security are agreed on with the supplier in advance.
f. If possible, standard and uniform solutions are used for the remote maintenance of all OT components.

IND.3.2.M2 Consistent documentation of the access rights of OT components [IT department, maintenance personnel]

a. The remote maintenance access rights of the operational technology systems are managed consistently.
b. The remote maintenance access rights are documented. The documentation is organised similarly to the documentation of the remote accesses to the IT systems of the computer network.
c. In the event of the remote maintenance solution integrated into the OT system, any unnecessary system accounts are deactivated. All deactivated accounts are also documented.

IND.3.2.M3 Checking access rights for the remote maintenance of OT and managing exceptions [IT department]

a. Compliance of the remote maintenance solutions of the operational technology components and the related access rights with the procedure for the remote maintenance of operational technology (see IND.3.2.M1 Designing the remote maintenance of operational technology components) is checked regularly.
b. Procedures have been established for the approval and confirmation of exceptions to the procedure for the remote maintenance of the operational technology.

IND.3.2.M4 Agreements for external remote maintenance

a. The terms and conditions of performing remote maintenance have been agreed on with all external parties (manufacturers of OT components, integrators, and providers of maintenance service). The agreements ensure that external users only use access to the remote maintenance of OT in a controlled and coordinated manner.
b. The organisation has defined which external users may be granted access and to which extent. Moreover, employees have been appointed who are authorised to monitor and check the activities of external maintenance personnel.
c. When performing remote maintenance, the security of people working with OT is ensured.
d. An operational technology specialist of the organisation may perform the remote maintenance of OT components if the respective authorisation has been granted to them.

IND.3.2.M5 Coordination of maintenance procedures with the IT department [IT department, architect]

a. The operational technology department has coordinated all interfaces, systems, and technical parameters of the systems used for remote maintenance with the IT department and other relevant units of the organisation.
b. All external roles, procedures, and obligations of the operational technology department which are required for performing remote maintenance (incl. applying for authorisations for use) have been defined.

IND.3.2.M6 Security of remote maintenance solutions in the operational technology network [IT department]

a. If remote access is gained to an operational technology component through a device or server in the computer network, the operational technology department is responsible for the configuration

and access rights of at least one security component required for such access.
b. If possible, standardised, centrally managed authentication solutions are used for the remote maintenance of the operational technology components.
c. If the remote maintenance access system of an OT component is not centrally managed by the organisation, the accesses are protected by a further security mechanism which is not part of the typical (default) remote access solution.

3.3 Standard measures

IND.3.2.M7 Decoupling IT systems from an operational technology network [architect]

a. Remote accesses to any OT component have been decoupled from the operational technology network. Before starting a remote maintenance session, the IT system used for remote access is decoupled from other networks. A new session is created for remote maintenance.
b. The tools and applications of remote maintenance are installed in the maintenance computer in advance.
c. The IT system of remote maintenance supports different user accounts.
d. A jump server or an application layer gateway (ALG) located in a demilitarised zone (DMZ) are used for remote maintenance.
e. If possible, the operational technology department is responsible for the decoupling of remote access and manages the respective DMZ.

IND.3.2.M8 Controlled initiation of a remote maintenance session [employee]

a. All remote maintenance sessions are coordinated with the system owner appointed by the organisation operating the operational technology system. Only then will the responsible specialist of the operational technology department activate the remote maintenance access. Prior coordination of remote maintenance sessions with the owner of the system is needed in the case of scheduled maintenance performed within the maintenance periods agreed in advance, as well as in the case of emergency remote maintenance.
b. A remote maintenance session lasts for a limited period of time. The responsible specialist of the operational technology department may decide on the time and duration of a remote maintenance session at their own discretion (see IND.3.2.M3 Checking access rights for the remote maintenance of OT and managing exceptions).
c. External remote maintenance accesses are only created from the inside out (initiated from the

operational technology network).
d. The ports opened for remote maintenance cannot be accessed from unreliable networks.

IND.3.2.M9 Secure transmission of files in the course of remote maintenance [architect, IT department]

a. Procedures which include security measures have been established for the secure transmission of files in the course of the remote maintenance of OT (e.g. for sending configuration files, system updates, or instructions).
b. Upon transmitting files, the files are checked to detect potential malware.
c. Files can only be transmitted between previously authenticated users. The transmission of files is not automatic, but a permission is required to initiate a transmission.
d. Any transmission of files is logged.

IND.3.2.M10 Monitoring and inspecting remote maintenance [employee]

a. Remote maintenance of OT does not harm production processes or OT systems and devices.
b. Remote maintenance does not pose a direct or indirect risk to the individuals who use operational technology systems or are in the vicinity of the devices.
c. If there is a risk of potential bodily harm or material damage, all remote maintenance operations are validated based on the four eyes principle.
d. A specialist of the operational technology department who is monitoring remote maintenance operations on site can interfere with the course of remote maintenance or halt a remote maintenance session if necessary.

IND.3.2.M11 Central administration of the OT user accounts [IT department]

a. The remote maintenance of operational technology components is only conducted from the user accounts of the operational technology department or the user accounts registered in the centrally managed directory service.

3.4 Advanced measures

IND.3.2.M12 Special solution for the remote maintenance of operational technology [architect] (C-I-A)

a. A special remote maintenance solution of the OT components is used for remote maintenance, which is independent from the computer network and IT architecture of the organisation. All other options for remote access to the operational technology components have been deactivated or blocked.
b. A separate Internet connection independent from the computer network of the organisation is used for the remote maintenance of the operational technology components.

IND.3.2.M13 Expanded logging of remote maintenance operations [architect, data protection specialist] (C-I)

a. The remote maintenance operations of the operational technology systems can be monitored fully and immediately.
b. In addition to the events and session data, the content of remote maintenance operations is also logged.

IND.3.2.M14 Technical inspection of a remote maintenance session [architect, data protection specialist] (C-I-A)

a. All operational-level operations, i.e. manually or automatically issued commands, can be prevented technically, if necessary.
b. The automatic monitoring solution of the OT remote maintenance sessions activates an alarm in the case of a violation of specific technical rules, as well as in the case of any abnormalities in the pattern of use (e.g. a sudden increase in the volume of data communication).