Guideline on Cyber Security for Small and Medium-sized Enterprises

CFPA-E Guideline No 11:2018 S

CFPAEUROPE

Foreword

The Security Commission of the Confederation of Fire Protection Association Europe (CFPA-E) has developed common guidelines in order to achieve similar interpretation in the European countries and to give examples of acceptable solutions, concepts and models. The CFPA-E has the aim to facilitate and support fire protection and security aspects across Europe.

The market imposes new demands for quality and safety. Today fire protection and security aspects form an integral part of a modern strategy for survival and competitiveness.

The guidelines are primarily intended for the public. They are also aimed at the rescue services, consultants, safety companies and the like so that, in the course of their work, they may be able to help increase fire safety and security in society.

These guidelines have been compiled by the Guidelines Commission and are adopted by all fire associations in the CFPA-E.

These guidelines reflect best practice developed by the countries of CFPA-E. Where the guidelines and national requirements conflict, national requirements must apply.

Content

1 Introduction

1.1 General

The success of an enterprise is not only based on competitive products and services. Today, use of state-of-the-art IT to cope with operational, logistic, and technical business processes as well as the access to the internet are indispensable, as well, to compete internationally. However, digitisation and data networking involve new risks to be considered in the enterprise's risk management. Well-organised information security reduces the number of critical points and risks and, consequently, restricts potential damage to the enterprise.

Well-established protection standards are available to avert "conventional" dangers. These are in particular the guidelines for security systems provided by independent test- and certification institutions of the individual country. The Guidelines at hand are tailored to the needs of small and medium-sized enterprises (SME) to establish and maintain adequate information security.

Besides the requirements described in these guidelines, national regulations have to be observed.

1.2 Scope

These Guidelines define minimum requirements for information security and are applicable to small and medium-sized enterprises (SME), administrative divisions, associations, and other organisations.

1.3 Application Information

These Guidelines are written to be used as part of a certification process. It can be taken as basis for a certification by a certification body possessing relevant and appropriate knowledge.

Realisation of the requested actions requires expert knowledge and experience in the field of information security. Should the user lack of adequate knowledge and experience, it is highly recommended to co-operate with a qualified service provider in this field (ask for certified consultants according to e.g. ISO 27001.

1.4 Validity

These Guidelines are valid from 01.08.2018.

2 References

These Guidelines incorporate dated and undated references to other publications. These references are cited at the appropriate places in the text, and the publications are listed hereinafter. Subsequent amendments to or revisions of dated guidelines shall become valid only with publication by amendment of these Guidelines. To undated references the latest published edition referred to applies.

BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise
(IT Basic Security – Methodology; German rule; adequate alternative national rules may be used instead)

BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz
(Risk Analysis Based on IT Basic Security; German rule; adequate alternative national rules may be used instead)

BSI-Standard 100-4 Notfallmanagement
(Emergency Management; Business Continuity Management; a German rule; national rules may be used instead)

EN 50173 series Information Technology – Generic Cabling Systems – Part 1: General Requirements

EN 50174 series Information Technology – Cabling Installation

EN ISO 9001 Quality Management Systems – Requirements

EN ISO 22301 Societal Security – Business Continuity Management Systems – Requirements

ISO 31000 Risk Management – Principles and Guidelines

ISO/IEC 27005 Information Technology – Security Techniques – Information Security Risk Management

VdS 2007 Anlagen der Informationstechnologie (IT-Anlagen), Merkblatt zur Schadenverhütung (Information Technology Installations, Leaflet for Loss Prevention)*; German quick guide; adequate alternative national leaflets may be used instead)*

3 Glossary

Administrative access: Access enabling a user to manage an IT system, i.e. the user gets extensive rights on an IT system.

Administrator: An administrator is responsible for setting up, operating, monitoring, and maintaining of an IT system or network.

Active network component: Network components featuring an own logic, such as hubs, switches, repeaters, bridges, media converters, gateways, firewalls, etc. Normally, an active network component requires power supply. An active network component is an IT system.

Authenticity: Genuineness, verifiability, and reliability.

Authentication feature: A feature used by the inquiring instance to prove its identity. Authentication features could be knowledge (e.g. password or PIN), property (e.g. smart card or token), or biometric characteristics (e.g. fingerprint or iris).

Availability: Probability that a system meets particular requirements at a particular time or within a particular period of time. Availability of information is given if information can always be used as intended.

Business continuity management (BCM): Comprehensive management process to systematically prepare for coping with any damage aiming at continuing with key business processes even in case of emergency, during crises or disasters, or should this be impossible of restarting them as fast as possible.

Case of emergency: Situation in which the processes or resources of an enterprise do not work as intended. The damage resulting therefrom is unacceptably high. A case of emergency cannot be handled as a part of the routine business.

Cloud computing: Technology allowing access to a shared pool of configurable IT resources, via a network.

Connection: Channel, through which data can be exchanged.

Confidentiality: Characteristic of a message that this is intended for a restricted circle only. Confidentiality of information is given if only the circle intended is able to read or respectively to interpret it.

Critical connection: Channel that meets the requirements in clause 9.3.

Critical IT system: IT system that meets the requirements in clause 9.3.

Critical mobile data carrier: Mobile data carrier that meets the requirements in clause 9.3.

Data: Character structures representing information which can be interpreted on the basis of common understanding.

Data access: Data communication between an accessing entity and an IT system.

Data line: Physical medium through which data can be exchanged.

Emergency operation level: Definition of the functions an IT system shall ensure to maintain emergency operation.

Employee: Individual with a contractual relationship to the enterprise and holding one or several positions in the enterprise.

Endangerment: Threat plus weak point.

Fault: Situation in which the processes or resources of an enterprise do not work as intended. The resulting damage is to be considered minor. A fault can be cleared as a part of the routine business.

Function: Bundle of tasks to achieve part of the company objective.

Catastrophic damage: Damage to which applies any of the criteria below:

1. Effect to life and limb
2. Persons are severely hurt or lose their lives
3. Effect on key business processes
4. Key business processes grind to a halt and any return to normal operation (within an acceptable period of time) is impossible
5. Effect on key values of the enterprise
6. Key values of the enterprise get lost or are destroyed and re-establishing them (by means of the enterprise) is impossible
7. Effect on legal compliance
8. Breach of law, agreements, or standards and the liability resulting therefrom ruins the enterprise or the people responsible
9. Extent of loss
10. The enterprise does not have enough resources to resolve the damage

Hazard: Potential damage to an object to be protected.

Information: Sense and meaning the receiver interprets of received data.

Information security: Protection of information as to the existing safety requirements (e.g. confidentiality, availability, or integrity).

Information security process: Embedding of activities into the organisational structure to establish, maintain, and develop the information security.

Information security representative (ISR): Person in charge of the tasks acc. to clause 4.3.

Information security team (IST): Team performing the tasks acc. to clause 4.4.

Information technology (IT): Generic term for information and data processing and transmission including the hardware and software required to this end.

Integrity: Correctness (intactness) of information and/or correct functioning of data processing.

Interface: Part of an IT system required for communication. These are not only Ethernet and wireless LAN adapters, but also other components, such as e.g. ISDN boards, modems, USB ports, NFC and infrared interfaces, SD slots, or keyboards.

IS guidelines: Guidelines on information security, see chapter 6.

IT infrastructure: All persistent equipment and organisation required for the operation of applications software.

IT manager: Head of IT department and responsible for the management of information technology.

IT outsourcing: Outsourcing of IT tasks to legally independent service providers.

IT resource: Operating resource designed for electronic data processing. These are e.g. IT systems, personnel, data carriers, connections, as well as any data and information.

IT system: Technical systems designed for data processing and composed as a closed functional unit. Typical IT systems are e.g. servers, clients, printers, mobile phones, smartphones, telephone equipment, laptops, tablets, and active network components.

Key business process: Business process, which is decisive to fulfil the company's tasks. This can be, e.g. an added value process or a process to maintain or improve competitiveness.

Mobile data carrier: Data carrier the use of which is characterised by mobility. Typical mobile data carriers are e.g. memory sticks and cards as well as external hard disks or storage media, such as CD-ROMs, DVDs, and diskettes.

Mobile IT system: IT system the use of which is characterised by mobility. Typical mobile IT systems are e.g. notebooks, smartphones, tablets, or digital cameras.

Network component: Technical system serving the transmission of data. We distinguish between active and passive network components.

Network transition: Interface between two different networks. Here, the networks may differ in the physical media of transmission, the protocols used, or the administrative sovereignty.

Passive network component: Network components without an own logic, such as cables, patch fields, outlets, plugs, etc. Normally, a passive network component does not require any power supply.

Personnel: Internal and external employees.

Physical access: Possibility to physically interact with an IT system or a network.

Policy guidelines: Document issued by the top management that defines the company objective and priority as well as the responsibilities to achieve it.

Position: Position of an employee in the company hierarchy.

Procedure: Defined execution of a process (or a single activity being part of the process).

Process: System of activities, which uses any means to convert inputs into results.

Process manager: The one who is responsible for the content of one or several business processes. This person keeps track of the resources required for such business processes as well as of the corresponding requirements.

Process of high loss potential: Process, the malfunction or breakdown of which would cause a catastrophic damage.

Project manager: The one who is responsible for proper project implementation.

Resource: Operating material which is the property of the enterprise or at its disposal.

Risk: An endangerment assessed on the basis of its probability of occurrence and its extent.

Role: Ensemble of expected conduct and responsibilities assigned to a position.

Security incident: Unwelcome event with adverse effects on the information security, which could lead to huge damage. The company shall define what kind of incident is a security incident.

Server: Central IT system to establish functional and infrastructural network services.

System software: Firmware, operating system, and system-oriented software. System software manages the internal and external hardware components of an IT system.

Task: Permanently effective order given to an actor to perform defined actions.

Threat: Potential occurrence of damage.

Top management: Top management level, such as the members of the managing board, the managing directors, or the heads of authorities.

Weak point: Condition allowing the local and/or temporal coincidence of a threat with an object to be protected.

4 Organisation of Information Security

Information security is dynamic and different from enterprise to enterprise. To get a definition of the security level aimed at in an enterprise, to realise this, and to adapt it to current requirements and endangerments – all with the least possible expenditure – a corresponding process (information security process) is to be established.

4.1 Responsibilities

The responsibilities for the information security process SHALL be assigned definitely and consistently.

4.1.1 Assignment and Documentation

The following SHALL be documented for each responsibility being part of the information security process:

- Objectives to be achieved
- Resources to which responsibility applies
- Tasks to be fulfilled to achieve objectives
- Authorisations connected to the responsibility to meet the obligations
- Resources available to meet the obligations of the responsibility
- How to meet the obligations of the responsibility and by which position(s)
- Positions required to meet the obligations of this responsibility

4.1.2 Separation of Functions

The assignment of responsibilities being part of the information security process SHALL observe the principle of separation of functions. Conflicting responsibilities SHALL NOT be assigned to one single person or business unit.

If functions cannot be separated or an inacceptable high expenditure is required to do so, other measures SHALL be taken, such as supervision of activities, monitoring, or management control.

If functions cannot be separated, this SHALL be explicitly stated (e.g. highlighted and substantiated) in the documentation of the distribution of functions.

To prevent gaps of competences or overlapping responsibilities in the information security process, the information security representative (ISR) shall review the corresponding regulations once per year.

4.1.3 Resources

To take the responsibilities in the information security process, the corresponding personnel SHALL be released from other work duties as far as required (see clause 4.1.1).

4.1.4 Delegating Tasks

Persons in charge of information security MAY delegate tasks to other people. However, the responsibility still lies with them and, consequently, they SHALL verify the result of delegated tasks.

4.2 Top Management

Members of the top management SHALL commit to take the following responsibilities:

- Assume overall responsibility for information security
- Assume responsibility for the information security process
- Implementation of the guidelines for information security (IS guidelines)
- Provision of the resources of technology, finance, and human labour required for information security
- Implementation of the information security into the structures, hierarchies, and work processes of the enterprise

4.3 Information Security Representative (ISR)

The top management SHALL assign the responsibilities of an information security representative (ISR) to an employee.

The latter SHALL take the following responsibilities:

1. Initiating, planning, establishing, and controlling the information security process
2. Preparing practical suggestions for improvement
3. Backing the top management in preparing the IS guidance document (see chapter 5) and in its yearly review and amendment
4. Backing the top management in central issues of information security
5. Preparing all IS guidelines and performing yearly reviews and amendments
6. Investigating in security-relevant events
7. Initiating and controlling awareness rising and general trainings
8. Being the contact person in projects with effects on data processing as well as for the introduction of new software and IT systems to provide for an adequate observance of security-relevant aspects
9. Reporting to the information security team (IST) once per year on the status quo of information security in the enterprise, in particular on any risks and security incidents
10. Being the central contact person for information security

4.4 Information Security Team (IST)

The top management SHALL appoint an information security team (IST).

The following business units and/or positions SHALL be in the team in person or by proxy:

1. Top management
2. ISR
3. IT manager
4. Personnel
5. Data protection representative (if any)

The team SHALL support the ISR in the following activities:

1. Preparing the IS guidance document and all IS guidelines
2. Performing yearly reviews of the IS guidance document and all IS guidelines
3. Coordinating and controlling the information security measures in the entire enterprise
4. Identifying new endangerments

4.5 IT manager

The top management shall assign the tasks of an IT manager to an employee.

IT managers SHALL perform the following tasks:

1. Establishing the IS guidelines in their area of responsibility by taking adequate technical and organisational measures
2. Agreeing upon all measures with the ISR, which they consider to be taken to improve and maintain information security in their area of responsibility, as well as the corresponding planning, coordination, and realisation

4.6 Administrators

The responsibilities of an administrator SHALL be assigned to at least one employee.

Administrators SHALL take the following responsibilities:

1. Implementing technical measures in the information security process in coordination with the IT manager
2. Preparing proposals to improve the information security

4.7 Superiors with Staff Responsibilities

Superiors with staff responsibilities SHALL ensure for the personnel under their authority that the technical and organisational information security measures taken are implemented.

4.8 Personnel

The personnel SHALL take over the duties below:

1. Observing and implementing any information security measure and regulation which concerns the personnel or their activities
2. Giving notice of faults, security incidents, and cases of emergency

4.9 Project Managers

Project managers SHALL consult the ISR in any project with effects on information processing to provide for an adequate observance of security-relevant aspects.

4.10 Suppliers and Other Contractors

The enterprise SHALL oblige the suppliers and any other contractors to observe or implement all information security measures and regulations concerning them if they have access to critical information (see clause 9.2) or use non-public areas of the information technology (IT) in the enterprise.

5 Guidance Document on Information Security (IS Guidance Document)

The guidance document on information security (IS guidance document) is the central document for the entire information security process. This specifies the objectives to be achieved by the top management and defines responsibilities as well as authorities.

5.1 General Requirements

The top management SHALL adopt the IS guidance document and announce this officially.

Once per year the top management SHALL review the IS guidance document how up-to-date it is and initiate updating if required.

Every time after updating the IS guidance document, it SHALL be announced promptly. The IS guidance document SHALL always be available as amended.

5.2 Contents

The IS guidance document SHALL meet the following requirements:

1. It defines objectives and the relative importance of information security in the enterprise.
2. It defines all positions for the information security process and points out the corresponding tasks.
3. It points out to the consequences of any non-compliance.

6 Guidelines for Information Security (IS Guidelines)

To support the IS guidance document and make it concrete further information security specifications are required, which have to be collected in single documents, the so-called IS guidelines.

6.1 General Requirements

The ISR SHALL draw up any IS guideline and the top management SHALL put it into force.

Once per year the ISR SHALL review each IS guideline how up-to-date it is and initiate updating if required.

For drawing up and amending IS guidelines, all legal, statutory, and contractual requirements SHOULD be found out and implemented accordingly.

Any update of the IS guidelines SHALL be promptly announced to the target groups.

This SHALL be made so that the target group really hears about it and understands it, e.g. during a training.

IS guidelines SHALL be implemented in an enterprise or the top management SHALL set it aside.

6.2 Contents

Each IS guideline SHALL meet the following requirements:

1. It specifies for whom it is compulsory.
2. It gives the reasons for its preparation and defines its objectives.
3. It does not violate any other IS guidance document or any other guideline.
4. It points out to the consequences of any non-compliance.

6.3 Rules for Users

Arrangements SHALL be made for the use of IT; these are compulsory for all users (incl. all management levels) as well as for all IT.

The following arrangements SHALL be made:

1. General terms of use
    a. Any retrieval or publication of data protected by copyright without prior consent is prohibited.
    b. Any retrieval or publication of data which is applicable to criminal prosecution or unethical is prohibited.
2. Private use
    a. It is defined whether the private use of IT is permitted.
    b. Should the private use of IT be permitted, such use is designed to the advantage of the enterprise.
3. Basic rules of conduct
    a. Only allowed hard- and software is installed, used, and run in the IT infrastructure.
    b. It is prohibited to install an own network transition; only the network transition as established by the enterprise is allowed to be used.
    c. The safety devices installed in the IT infrastructure shall not be uninstalled, deactivated, deliberately bypassed, or reconfigured.
    d. Access codes shall not be published.
    e. Information shall not be encoded or protected against reading access on one's own authority; the technical procedures explicitly released by the enterprise to suit this purpose shall be used.
4. Flow of information in absentia
    a. It is defined whether new messages directed to an absent user will be routed onward.
    b. It is defined whether and when access to the data of an absent user is allowed.

5. Check for improper use
    a. Mechanisms to check for improper use are defined and communicated to the people concerned.

The enterprise SHOULD allow exceptions of the above rules in reasonable cases.

The ISR SHALL approve such exceptions in advance and this SHALL be documented together with the reasons given for this.

6.4 Rules for Suppliers and Other Contractors

Arrangements for using the IT SHALL be made; those are compulsory for all suppliers and other contractors that use non-public areas of the IT or the IT infrastructure of the enterprise.

The following arrangements SHALL be made:

1. General terms of use
    a. Any retrieval or publication of data protected by copyright without prior consent is prohibited.
    b. Any retrieval or publication of data which is applicable to criminal prosecution or unethical is prohibited.
2. Private use
    a. Any private use of IT is prohibited.
3. Basic rules of conduct
    a. Changes of safety devices as well as the installation of network transition (such as remote maintenance access or VPN access) are coordinated with the ISR in advance.
    b. It is prohibited to disclose access codes.
    c. It is prohibited to encode information or protect it against reading access on one's own authority; the technical procedures explicitly released by the enterprise to suit this purpose shall be used.
4. Access to non-public IT
    a. Access to non-public IT is subject to coordination with the ISR in advance.
    b. If IT systems of the service provider access to the non-public IT, the latter is protected by fundamental safety measures; the enterprise defines the minimum requirements for this.
5. Integration of IT systems
    a. Before an IT system is integrated in the IT infrastructure of the enterprise, an administrator releases this system for integration.
6. Handling business data
    a. Generally, the enterprise stores its business data in its own IT infrastructure; the data shall not be transferred to other IT systems or data carriers.
    b. A competent administrator allows in advance the use of mobile data carriers.
    c. Mobile data carriers are tested for malware just before using them in the IT.
    d. Mobile data carriers holding business data of the enterprise are generally treated confidentially; they are not passed on or kept so that other people could access them.
7. Check for improper use
    a. Mechanisms to check for improper use are defined and communicated to the people concerned.

The enterprise SHOULD allow exceptions of the above rules in reasonable cases.

The ISR SHALL approve such exceptions in advance and this SHALL be documented together with the reasons given for this.

6.5 Other Rules

Other specific IS guidelines SHALL be drawn up within the scope of these Guidelines:

1. Mobile IT systems (see clause 10.4)
2. Mobile data carriers (see clause 12.1)
3. Data backup (see clause 16.1)
4. Faults and breakdowns (see clause 17.1)
5. Security incidents (see clause 18.1)

The ISR SHALL determine the need of further IS guidelines once per year.

7 Personnel

The personnel is a central factor for the implementation and maintenance of information security. Therefore, the personnel management shall also allow for the information security requirements.

7.1 Prior to Recruiting

If a position in the enterprise, which is relevant for information security, is to be filled, the enterprise SHALL ensure that the applicant has the necessary professional aptitude and is trustworthy as required.

7.2 Recruitment and Training

A procedure (see Annex A) SHALL be implemented, which provides for the items below regarding the recruitment and training of new personnel:

1. A non-disclosure agreement is signed, which also defines the obligations regarding information security after termination or change of employment.
2. New employees are briefed on the IS guidance document, on all binding IS guidelines, and on other binding information security rules.
3. New employees are trained in the relevant security mechanisms and how to handle them (see clause 8.2).
4. It get necessary access and the corresponding access rights (see clause 15) and is trained on their use.

7.3 Termination or Change of Employment

1. A procedure (Annex A) SHALL be implemented, which provides for the items below regarding the termination or change of employment:
2. The personnel, the customers, and the suppliers and other contractors are notified of changes of employment and other changes in the enterprise as far as required.
3. Access and access rights (see clause 15) of the employee are revised immediately and changed where required.

8 Knowledge

Many dangers result from missing knowledge or awareness or are at least worsened by these factors. It is therefore important that the enterprise has current knowledge in the field of information security, that the employees know their responsibilities, and that they are suited and qualified for their tasks.

8.1 Up-to-date Knowledge

A procedure (see Annex A) SHALL be implemented which appropriately notifies all relevant positions in the enterprise as well as perhaps relevant external offices of any changes in the legal and technical conditions in the field of information security.

The procedure SHALL provide for the following:

1. Reliable sources are regularly used to get information on the latest technical and legal developments in the field of information security, especially on new dangers and possible countermeasures.
2. Information is promptly analysed regarding their importance for the information security so as to recognise new vulnerability.
3. The people in charge of the corresponding field are notified of the relevant trends within a short period of time.

Interest groups and security forums SHOULD be contacted and visited so that the people in charge are up-to-date with current knowledge and have access to expert information and advice.

8.2 Awareness Rising, Education and Training

A procedure (see Annex A) SHALL be implemented, which provides for the items below:

1. The affected personnel is adequately informed about dangers in their field of operation and trained how to work with the existing safety measures.
2. The contents of the IS guidance document and of any other applicable IS guidelines are imparted.
3. It informs on any consequences for non-observance of binding constraints.

The knowledge imparted during training or any other measure to raise awareness SHOULD be tested at the end to determine the personnel's understanding.

9 Identifying Critical IT Resources

The ISR SHALL determine the critical IT resources in the enterprise and verify yearly whether the list of critical IT resources is up-to-date and adapt it where required.

Therefore, the enterprise SHOULD analyse every year within the scope of a Business Continuity Management (BCM, see clause 17) the business impact on the basis of recognised and accepted standards. Standards can differ from one country to the other (for Germany this is the BSI standard 100-4 or the international standard EN ISO 22301. Orthe management SHOULD analyse the protective needs acc. to the (e.g.) BSI standard 100-2.

Any other manner of proceeding ABSOLUTELY requires implementation of a corresponding procedure (see Annex A), which meets the requirements of the paragraphs below.

9.1 Processes

The enterprise SHALL identify and document its key business processes and its processes of high damage potential.

This documentation SHALL meet the following requirements:

1. It contains a short process description.
2. It substantiates why the process is a central process or a process of high damage potential, respectively.
3. It contains who is responsible for the process (process manager).
4. It defines the tolerable period of time when the process does not take place (maximum tolerable outage time).

The top management SHALL release the list of processes and the corresponding documentation.

9.2 Information

The enterprise SHALL determine the pieces of information to be protected especially.

Any information which can cause catastrophic damage in connection with the factors below requires special protection:

1. Unauthorised inspection, taking of notice, or disclosure (criterion "confidentiality")
2. Corruption (criterion "integrity")
3. Irrecoverable loss (criterion "long-term availability")
4. Short-term non-availability (criterion "immediate availability")

To determine critical information the key business processes and the processes of high damage potential (see clause 9.1) SHALL be examined and both, the type and the extent of information, SHALL be taken into consideration.

9.3 IT Systems, Mobile Data Carriers, and Connections

The enterprise SHALL identify its critical IT systems, mobile data carriers, and connections.

IT systems, mobile data carriers, and channels are critical if they process, store, or transmit critical information (see clause 9.2).

The maximum tolerable outage time SHALL be defined for each critical IT system, each critical mobile data carrier, and each critical connection. The maximum tolerable outage time SHALL be as short or even shorter than the shortest maximum tolerable outage time of all critical processes (see clause 9.1) that depend on the IT system, the mobile data carrier, or the connection.

To determine the critical IT systems, mobile data carriers, and connections you MAY use a top down approach (process-oriented view), a bottom up approach (system-oriented view), or a combination of both. The top down approach determines where critical information (see clause 9.2) is processed, stored, and transmitted. Whereas the bottom up approach works with an analysis of the IT systems, mobile data carriers, and connections of the enterprise whether they process, store, and transmit critical information. A combination of both approaches allows for reliable identification of critical IT systems, data carriers, and channels.

Upon identification of the critical IT systems, mobile data carriers, and connections the imperative parts of the IT infrastructure SHALL be determined. These parts of the IT infrastructure are critical too.

9.4 Custom-made Software

The enterprise SHALL identify critical custom-made software used.

Critical custom-made software is such software which is imperative to operate critical IT systems (see clause 9.3) and has been programmed especially for the enterprise or adapted to the enterprise's needs.

10 IT Systems

Data processing in an enterprise takes place electronically for the most part. Therefore, a well-structured management and protection of IT systems is required.

10.1 Inventory

An inventory listing all IT systems of the enterprise SHALL exist.

A corresponding procedure (see clause 10.2.1 and 10.2.2) to keep the inventory up-to-date and exhaustive SHALL be implemented.

The inventory SHALL contain the following information for each IT system:

1. Unique means of identification
2. Information allowing rapid localisation
3. Purpose of use

Furthermore, any particularities in installation and configuration SHOULD be included in the documentation.

10.2 Life Cycle

10.2.1 Putting into Ooperation and Conversion

A procedure (see Annex A) SHALL be implemented for putting into operation and conversion of IT systems, which provides for the items below:

1. It is determined whether an IT system is critical (see clause. 9.3).
2. The IT system inventory (see clause. 10.1) and the documentation of networks (see clause. 11.1) are updated.
3. Base protection (see clause. 10.3) is realised.
4. Default authentication characteristics (e.g. standard passwords) are changed when putting an IT system into operation or the corresponding access is deactivated.
5. The person in charge confirms in writing the operations when putting the IT system into operation.

10.2.2 Taking out of Service and Further Use

A procedure (see Annex A) SHALL be implemented for taking out of service and the further use of IT systems, which provides for the items below:

1. The IT system inventory (see clause 10.1) and the documentation of networks (see clause 11.1) are updated.
2. The IT system is examined to find stored information.
3. It is checked whether and how such information shall be saved or archived, respectively.
4. It is ensured that information stored on the IT system is archived if they shall be permanently available (see clause 9.2).
5. All information is protected against unauthorised access by e.g. reliably deleting, overwriting, removing it from the IT system or by destroying the entire IT system.
6. The corresponding person in charge confirms in writing the operations.

10.3 Base Protection

The measures listed in the following paragraphs SHALL be taken for all IT systems provided that they feature corresponding functionality.

Should any measures not be taken despite such functionality, the resulting risk SHALL be counteracted by implementation of a risk analysis and treatment (see Annex A.2).

10.3.1 Updates

The security updates of system and application software, which are available from the manufacturer, SHALL be tested acc. to an implemented procedure (see Annex A.1), released when apt, and be installed immediately upon release.

10.3.2 Network Communication Restrictions

The network communication with IT systems (both directions) SHALL be reduced to the minimum required to maintain functionality if one of the criteria below is applicable:

1. There are weak points, which can be used through the network and which are not removed (e.g. security update cannot be installed, passwords cannot be changed, technical procedures are not safe).
2. The IT systems are especially exposed (e.g. around IT systems, which can be accessed from the internet, or in public rooms).

10.3.3 Data Logging

The data of log-on and log-out of users, faults, and information security events SHALL be recorded in data logs for each IT system.

Such data logs SHOULD be stored centrally.

Data logs SHALL be kept for 6 months unless any other obligation to preserve or delete them applies.

The clocks of all IT systems SHALL be synchronised to allow analyses of the data logs.

10.3.4 External Interfaces and Drives

External interfaces and drives which are not required for business processes SHOULD be dismounted, shut down, deactivated, or made otherwise inaccessible to users.

10.3.5 Malware

All IT systems SHALL provide protection against malware.

Suitable software SHALL be used to search on each IT system for malware daily.

Moreover, all IT systems SHOULD feature real-time protection, i.e. a programme scans all files for malware at the moment when access to them takes place.

For IT systems featuring real-time protection the interval for a complete scan for malware MAY be increased to once per week.

Detected malware SHALL be kept from starting.

The software application designed to protect against malware SHALL automatically search for and use the latest search patterns by the software house.

10.3.6 Booting from Foreign Media

It SHALL be ensured that IT systems can be booted from authorised media only.

This MAY be done e.g. with BIOS passwords or with a physical protection of the IT systems.

10.3.7 Authentication

Access to all non-public areas of the IT systems SHALL be protected by an adequate log-on procedure requesting authentication.

The log-on procedures SHALL provide for the following:

1. Systematic trying out of log-on data is made more difficult.
2. Successful and unsuccessful log-on attempts are recorded.
3. Interactive sessions are terminated or locked when the user has not made inputs within a defined period of time.
4. If a user logs on through a network, confidentiality and integrity of the log-on data is ensured (e.g. by means of corresponding authentication protocols).

To get reliable log-on procedures the items below SHALL be provided for:

1. Structured management of accesses (see clause 15).
2. Use of reliable authentication procedures.
3. Use of adequate non-trivial authentication characteristics (e.g. no passwords that can be easily guessed).

10.3.8 Access Restrictions

Adequate access restrictions SHALL be used to ensure that users are not able to act as an administrator.

Moreover, adequate access restrictions SHOULD meet the following requirements:

1. *Users have access only to information they need to do their job.*
2. *Users have writing access only to information if this is necessary to do their job.*

10.4 Additional measures for mobile IT systems

Mobile IT systems are especially exposed to dangers, such as theft, unauthorised access, or insecure networks; this requires additional measures.

The following measures SHALL be taken for all mobile IT systems to supplement clause 10.3.

10.4.1 IS Guideline

To supplement the rules laid down in clause 6 an IS guideline SHALL define how to use mobile IT systems.

The IS guideline SHALL provide for the following:

1. It is defined which enterprise information may be collected, processed, stored, and transmitted on mobile IT systems.
2. The responsibility for data backup is defined.
3. The users are informed about the specific risks of mobile IT systems (e.g. hazard by being spied out when using the systems in public, loss or theft) and are bound to take adequate countermeasures.
4. It is prohibited to pass mobile IT systems over to unauthorised third parties.
5. It is defined whether and which software applications the users may install on mobile IT systems.
6. It is defined whether and under which conditions an administrator is allowed to localise a mobile IT system.
7. It is defined whether and under which conditions an administrator is allowed to delete information stored on a mobile IT system by remote access.

10.4.2 Protection of Information

The enterprise information stored on a mobile IT system SHALL be protected against any loss of its confidentiality and integrity.

Protection of confidentiality CAN be reached, e.g. by encryption of the data carrier.

10.4.3 Loss

A procedure (see annex Annex A) SHALL be implemented, which specifies how users and administrators shall proceed after loss of a mobile IT system.

The procedure SHALL especially define how and whom to inform of the loss and which immediate reaction shall follow.

The procedure SHALL ensure that upon a loss the accesses to the enterprise stored on this device cannot be used without authorisation (e.g. immediate reset of corresponding authentication characteristics, modification of call redirections, and deletion of voice mails).

The loss of a mobile IT system SHALL be handled as security incident (see clause 18).

10.5 Additional Measures for Critical IT Systems

The following measures SHALL be taken for all critical IT systems to supplement clause 10.3.

Should any measures not be taken, the resulting risk SHALL be counteracted by implementation of a risk analysis and treatment (see Annex A.2).

10.5.1 Risk analysis and Treatment

For critical IT systems a risk analysis and treatment procedure SHALL be established (see Annex A.2).

10.5.2 Emergency Operation Level

For each critical IT system an emergency operation level SHOULD be defined.

10.5.3 Robustness

It is NOT ALLOWED to make developments or tests on critical IT systems.

On critical IT systems all network services that are not required to fulfil the task SHALL be uninstalled, deactivated, or made inaccessible by appropriate filter mechanisms.

On critical IT systems all application software that is not required to fulfil the task SHOULD be uninstalled.

All access rights and privileges of the application software on critical IT systems SHOULD be reduced to a minimum.

10.5.4 External Iinterfaces and Drives

External interfaces and drives which are not required for business processes SHALL be dismounted, shut down, deactivated, or made otherwise inaccessible to users.

10.5.5 Management of Change

Changes to be realised on critical IT systems SHALL be tested in a test environment and released before.

A mechanism SHALL exist for critical IT systems, which ensures that the original condition of the IT system will be restored after a malfunction or a breakdown of the IT system due to a change within the maximum tolerable outage time.

10.5.6 Documentation

There SHALL be documentation for each critical IT system.

With this documentation a skilled expert SHALL be able to find out the following:

1. Who is responsible for the system
2. How does administrator access to the IT system work and what are the accesses and authentication characteristics
3. Which basic design decisions were taken during the installation
4. Which changes took place
5. When did they take place
6. Who made the changes
7. Why did they take place

10.5.7 Data Backup

All critical IT systems SHALL provide for a data backup (see clause 16).

10.5.8 Monitoring

Monitoring SHALL take place to find out whether critical IT systems are operating normally.

This SHALL ensure that any breakdown of a critical IT system is detected and corresponding countermeasures are taken.

Furthermore, the resources of critical IT systems SHOULD be subject to monitoring to detect bottlenecks before they appear.

10.5.9 Standby Systems and Replacement Procedures

If a critical IT system cannot be restored within its maximum tolerable outage time, the enterprise SHALL provide for a standby system or a replacement procedure to allow further operation of the critical processes which depend on the critical IT system.

The standby system or replacement procedure SHOULD ensure the emergency operation level (see 10.5.2) of the critical IT system.

10.5.10 Critical Custom-made Software

The enterprise SHALL ensure by contractual and/or organisational regulations that it could use in future and adapt to its requirements any critical custom-made software (see clause 9.4).

11 Networks and connections

Networks and connections are designed to communicate information and to network IT systems. Therefore, adequate protection is required.

11.1 Documentation

The networks of the enterprise SHALL provide a documentation with the help of which any skilled expert can find out the following:

1. Active network components
2. Intra-network connections
3. Connections to external networks
4. Task
5. Physical medium

11.2 Active Network Components

Active network components are IT systems and SHALL be treated as laid down in clause 10.

11.3 Network Transition

The security measures required for network transition with less trusted networks or even untrustworthy networks SHALL be determined in the scope of a risk analysis and treatment procedure (see Annex A.2).

Configuration of network components implementing network interworking with less trusted or untrustworthy networks SHALL be subject to yearly reviews and SHALL meet the requirements below:

1. The following is documented for the settings with relevance for security:
    a. Who implemented it
    b. When did implementation take place
    c. What effect does it have
    d. Why is it required
2. The restrictions of communication strived for are implemented successfully.

11.4 Base Protection

The measures listed in the following paragraphs SHALL be taken for all networks provided that they feature corresponding functionality.

Should any measure not be taken despite such functionality, the resulting risk SHALL be counteracted by implementation of a risk analysis and treatment (see Annex A.2).

11.4.1 Network Sockets

Permanently unused network sockets SHALL be protected against any unauthorised use.

This CAN be realised, e.g. by a physical access restriction, by deactivation of the network sockets, or by authentication of the IT systems.

11.4.2 Segmentation

It SHALL be verified whether the networks of the enterprise should be segmented. The decision SHALL be documented.

Implementation of the segmentation SHALL provide for an as comprehensive restriction of channels as possible and for the option to log blocked connections.

11.4.3 Remote Access

Accesses via less trusted or untrustworthy networks to data and/or IT system areas of the enterprise which are closed to the public SHALL be protected.

Here, the following requirements SHALL be met:

1. Confidentiality, integrity, and authenticity of transmitted information is protected.
2. Access is designed so that only those IT systems can be reached that the corresponding user needs to do his job.

Moreover, the following requirements SHOULD be met:

1. Access takes place via a remote desktop connection which ensures that it is impossible to copy any enterprise information to the accessing IT systems.
2. The user, especially if granted with extensive access rights, is authenticated through multi-factor authentication to reduce the risk of unauthorised access.
3. Access is designed so that not only the user but also the accessing IT system is authenticated.

11.4.4 Network Coupling

Coupling of enterprise networks via less trusted or untrustworthy networks SHALL be protected.

Here, confidentiality, integrity, and authenticity of transmitted information SHALL be guaranteed.

11.5 Additional Measures for Critical Connections

For critical channels a risk analysis and treatment procedure (see Annex A.2) SHALL be established to supplement clause 11.4.

12 Mobile Data Carriers

Mobile data carriers are at particular risk due to their exposed type of use. Therefore, adequate treatment of the risks involved is required.

12.1 IS Guideline

To supplement the rules laid down in clause 6 an IS guideline SHALL define how to use mobile data carriers.

The IS guideline SHALL meet the following requirements:

1. It is defined which enterprise information may be stored on mobile data carriers.
2. The users are informed about the specific risks of mobile data carriers (e.g. loss or theft or malware) and are bound to take adequate countermeasures.

3. It is prohibited to pass mobile data carriers over to unauthorised third parties or to lend them out.

12.2 Additional Measures for Critical Mobile Data Carriers

The following measures SHALL be taken for all critical mobile data carriers to supplement clause 12.1.

12.2.1 Risk Analysis and Treatment

For critical data carriers a risk analysis and treatment procedure SHALL be established (see Annex A).

12.2.2 Protection of Stored Information

The enterprise data stored on critical mobile data carriers SHALL be protected against unauthorised inspection and modification.

Protection of confidentiality CAN be reached, e.g. by encryption of the data carrier.

12.2.3 Loss

A procedure (see Annex A.1 SHALL be implemented, which specifies how users and administrators shall proceed after loss of a critical mobile data carrier.

13 Environment

The enterprise SHALL protect its IT systems and data lines against adverse environmental impacts.

This SHOULD be based on a recognised standard, such as VdS 2007 (for Germany). Standards can differ from one country to the other.

Any other manner of proceeding SHALL implement at a corresponding procedure (see Annex A.1) which meets the requirements of the paragraphs below.

13.1 Server, Active Network Components, and Network Distribution Points

Server, active network components, and network distribution points (e.g. patch fields) SHALL be protected with appropriate measures against any damage and unauthorised physical access.

This CAN be realised e.g. by construction measures (server room) or by lockable cabinets (server and network cabinets).

The following requirements SHOULD be determined for server, active network components, and network distribution points, the fulfilment of which is ensured by appropriate construction, technical, and organisational measures:

1. *Environmental conditions (such as temperature, air humidity, dust, or smoke)*
2. *Power supply*
3. *Protection against natural hazards (fire, water, lightning, and overload)*
4. *Protection against theft*
5. *Protection against unauthorised physical access*

13.2 Data Lines

Fixed data lines SHALL be protected with appropriate construction measures against any damage.

This CAN be realised, e.g. by installing the data lines into cable ducts.

All data lines SHOULD be installed acc. to prevailing standards, such as the DIN EN 50173/4 series.

13.3 Additional Measures for Critical IT Systems

Within the scope of the risk analysis and treatment (see clause 10.5.1) the following threats shall be handled for each critical IT system:

1. Poor environmental conditions (such as temperature, air humidity, dust, or smoke)
2. Unreliable power supply and electrical equipment
3. Natural hazards (fire, water, lightning, and overload)
4. Intrusion, theft, tamper, vandalism
5. Unauthorised physical access

14 IT Outsourcing and Cloud Computing

Outsourcing of IT resources requires consideration of the enterprise's security interests.

14.1 Preparation

The top management SHALL approve any project leading to an outsourcing of IT resources.

The following parameters SHALL be documented for each project.

1. Which IT resources are planned to be outsourced
2. Which business, legal, and contractual conditions shall be met, in particular regarding confidentiality, availability, and integrity of the outsourced IT resources
3. If the IT resources to be outsourced are critical

If the enterprise plans to outsource IT resources, the enterprise SHALL be prepared following the steps below:

1. The competences to control the IT resources to be outsourced are built up.
2. The IT infrastructure is prepared for communication with the IT resources to be outsourced.

14.2 Contractual Arrangements

If IT resources are planned to be outsourced, a contract with the provider SHALL be entered into, which includes the requirements specified in clause 14.1 and binds the provider to fulfil them.

Furthermore, it SHOULD be ensured that any claims due to breaches of the contract can be asserted even if provider and enterprise are subject to different jurisdictions.

14.3 Additional Measures for Critical IT Resources

If critical IT resources (see clause 9) are planned to be outsourced, the requirements specified in clause 14.1 for their confidentiality, availability, and integrity SHALL be determined within the scope of a risk analysis and the following shall be stipulated by contract:

1. Services
    a. The services to be rendered by the provider are defined and it is stipulated how to assess and supervise their provision.
    b. The locations where to render the services are defined.
    c. The safety measures to be taken by the provider to protect the outsourced IT resources are stipulated.
    d. The interface between the IT infrastructure of the enterprise and the outsourced IT resources is defined and described.

2. Communication

   b. The contact persons on the part of the enterprise and on the part of the provider are designated.

   c. A non-disclosure agreement is signed.

   d. It is agreed whether and under which conditions the provider is authorised to disclose data to third parties.

   e. The provider undertakes the obligation to inform in case of security incidents which affect the outsourced IT resources.

3. Change in service and termination of the contract

   f. The provider undertakes the obligation to cooperate in case of termination of the contract or insolvency; this particularly means handing over of all IT resources belonging to the enterprise as well as the active support of any migration executed by the provider.

   g. Written documentation and reporting in case of any changes of the aforementioned items is stipulated.

   h. Consequences for any non-compliance with the services as provided for by contract are stipulated.

It SHALL be ensured that any claims due to breaches of the contract can be asserted even if provider and enterprise are subject to different jurisdictions.

15 Accesses and Access Rights

Accesses and access rights allow access to the non-public IT of the enterprise and its data. Therefore, both require a well-structured management.

15.1 Management

Procedures (see Annex A.1) SHALL be implemented to create and modify accesses and access rights as well as to reset authentication characteristics, which provide for the following:

1. The respective procedures are applied for, reviewed, and approved before starting implementation.
2. Accesses and access rights are only approved if the corresponding user requires them to do his job or if business processes require this.
3. If it is planned to assign administrator access or access rights to a user, this is substantiated and decided by the IT manager.
4. Applicant and user are notified at short notice of the realisation; if accesses are withdrawn, only the applicant shall be notified thereof.
5. Before deleting an access, the data linked with it are passed on, deleted, or backed up / archived.
6. Any procedure is documented.

15.2 Additional Measures for Critical IT Systems and Data

A list of all accesses to critical IT systems (see clause 9.3) and all rights to access critical information (see clause 9.2) SHALL be drawn up every year to verify then whether they were created following the procedures specified in clause 15.1 and whether they are required.

Any improperly created access and access right SHALL be handled as a security incident (see clause 18).

16 Data Backup and Archiving

Data can become useless or get lost. Therefore, it is required to provide for data integrity and availability by means of a data backup.

Data backup SHOULD be based on recognised and accepted standards, such as the BSI standard 100-2 allowing for the (e.g.) IT-Grundschutz (basic protection) catalogues by BSI. Standards can differ from one country to the other.

Any other manner of proceeding SHALL comply with the requirements of the paragraphs below.

16.1 IS Guideline

To supplement the rules laid down in clause 6 an IS guideline SHALL define the storage locations for enterprise data.

The enterprise data SHOULD be stored centrally whenever possible; this provides for an effective data backup.

16.2 Archiving

The enterprise SHALL review which data shall be archived to satisfy business, legal, and contractual requirements.

16.3 Procedure

For data backup, data restoration, and data archiving, procedures (see Annex A.1) SHALL be implemented which provide for the following:

1. The data backed up are protected against modification, damage, loss, and unauthorised inspection during transmission, storing, and transport.
2. The data backed up are not stored in the same fire compartment as the IT systems backed up.

Single data backups SHOULD be kept at a remote location to provide for an available data backup in case of a disaster.

16.4 Further Development

Every year the ISR SHALL verify whether any conversions of IT systems or of operational, legal, or contractual framework conditions cause an adaptation of the backup, restoration, and archiving procedures.

Necessary adaptations SHALL be implemented within a short period of time and documented.

16.5 Base Protection

The measures listed in the following paragraphs SHALL be taken for all storage locations (see clause 16.1), servers, active network components, and mobile IT systems provided that they feature corresponding functionality.

Should any measure not be taken despite such functionality, the resulting risk SHALL be counteracted by implementation of a risk analysis and treatment (see Annex 18.3A.2).

16.5.1 Storage Locations

Storage locations SHALL be backed up so that their latest completely restorable backup is not older than 24 hours.

16.5.2 Servers

Servers SHALL be backed up so that their latest completely restorable backup (system software, configurations, application software, and application data) is not older than 24 hours.

16.5.3 Active Nnetwork Components

System software and the configuration of the active network components SHALL be backed up upon any change.

16.5.4 Mobile IT Systems

The administrators SHALL define a technical backup procedure.

16.5.5 Tests

Backup and restoration procedures SHALL be tested:

1. Once per year an IT system subject to backup is randomly selected and restored in a test environment.
2. Upon any change of the backup or the restoration procedure, one of the corresponding IT systems is backed up and restored in a test environment.

The tests SHOULD be effected without any support by the corresponding person in charge of the data backup. On the contrary, another employee SHOULD effect them with the help of the existing documentation.

The test results and experience gained from them SHALL be used to revise the existing backup and restoration procedures within a short period of time.

Performance of the tests and their results SHALL be documented.

16.6 Additional Measures for Critical IT Systems

Each critical IT system SHALL provide for data backup which provides for the following to supplement clause 16.5.

16.6.1 Risk Analysis

Within the scope of the risk analysis and treatment (see clause 10.5.1), the consequences of any data loss SHALL be analysed to determine the maximum tolerable data loss as well as the maximum tolerable outage time.

16.6.2 Procedure

The procedures for data backup and restoration SHALL provide for the following:

1. Critical IT systems SHALL be backed up completely (system software, configurations, application software, and application data).
2. The maximum tolerable outage time is not exceeded.
3. Restoration within the maximum tolerable outage time is ensured if no standby system or replacement procedure is available (see clause 10.5.9).

16.6.3 Tests

Every year, the backup and restoration procedures for critical IT systems SHALL be tested acc. to 16.5.5 on a critical IT system.

17 Faults and Breakdowns

An appropriate reaction to breakdowns enables an enterprise to resume normal business quickly and to reduce the damage to a minimum.

To this end the enterprise SHOULD implement a BCM based on a recognised standard, such as the (e.g.) BSI 100-4 or the DIN EN ISO 22301.

Any other manner of proceeding SHALL comply with the requirements of the paragraphs below.

17.1 IS guideline

To supplement the rules laid down in clause 6 an IS guideline SHALL define how to handle faults and breakdowns.

The IS guideline SHALL provide for the following:

4. The terms "fault" and "breakdown" are clearly defined.

   This SHOULD include an enumeration of the conspicuous signals that shall lead to the message of a potential fault or a potential breakdown.

5. Every employee reports potential faults and breakdowns to an administrator.

6. Administrators give the investigation into faults and breakdowns priority. Where required this is done together with the corresponding process managers, the IT manager, and the ISR.

7. The cases are defined when notification of the top management of faults and breakdowns is required.

8. It is defined how internal and external communication of the enterprise about pressing problems with faults and breakdowns and those mastered takes place.

17.2 Reaction

A procedure (see Annex A.1) SHALL be implemented, which provides for the items below – in such order – in case of a fault or breakdown:

1. Getting a general idea of the situation.

2. Taking all measures required to protect life and limb.

3. Taking emergency measures to get the damage under control.

4. Documenting the damage.

5. Searching for evidence to secure it.

6. Repairing the damage and resuming normal business.

7. Effecting a revision of the event to determine the root causes and developing upgrade measures.

In case of minor faults or breakdowns it SHOULD be possible to terminate the procedure prematurely.

17.3 Additional Measures for Critical IT Systems

17.3.1 Plans to Resume Operation

A plan to resume operation SHALL be drawn up for each critical IT system; this shall provide for the following:

1. It contains information and the workflow in the correct order of steps to allow a skilled expert to resume the operation of an IT system within the maximum tolerable outage time to an extent that the emergency operation level is given.

2. It contains the resources required, such as the personnel and corresponding contact data, the hardware, the software, the networks, the services, the passwords.

3. It is comprehensible and clearly arranged.

4. It is kept ready even in case of emergency.

5. It is kept in a different fire compartment than the location of the IT system.

17.3.2 Interdependencies

The interdependencies of the critical IT systems SHALL be documented.

This documentation SHALL meet the following requirements:

1. It definitely specifies the sequence of the critical IT systems when resuming operation.
2. It is comprehensible and clearly arranged.
3. It is kept ready even in case of emergency.
4. It is kept in a different fire compartment than the location of the IT system.

18 Security Incidents

An adequate reaction to security incidents enables an enterprise to quickly get the damage under control and repair it. Therefore, adequate preparation for security incidents is required.

18.1 IS Guideline

To supplement the rules laid down in clause 6 an IS guideline SHALL define how to handle security incidents.

The IS guideline SHALL provide for the following:

1. The term "security incident" is clearly defined.

   This SHOULD include an enumeration of the conspicuous signals that shall lead to the message of a potential security incident.

2. Every employee reports potential security incidents to the ISR.
3. The ISR gives the investigation into security incidents priority. Where required, this is done together with the corresponding process managers, the IT manager, and the administrators.
4. The cases are defined when notification of the top management of security incidents is required.
5. It is defined how internal and external communication of the enterprise about pressing problems with security incidents and those mastered takes place.

18.2 Detection

The enterprise SHOULD implement measures to detect potential security incidents, such as:

1. Intrusion Detection Systems (IDS)

2. Integrity checks and check sum basis

3. Sensor systems (honeypots)

4. Monitoring of the access to especially sensitive data

5. Recording and analysing logs

18.3 Reaction

A procedure (see Annex A.1) SHALL be implemented, which provides for the items below - in such order - in case of a security incident:

1. Getting a general idea of the situation.
2. Taking all measures required to protect life and limb.
3. Taking emergency measures to get the damage under control.
4. Documenting the damage.
5. Searching for evidence to secure it.
6. Repairing the damage and resuming normal business.

7. Effecting a revision of the event to determine the root causes and developing upgrade measures.

In case of minor security incidents it SHOULD be possible to terminate the procedure prematurely.

Annex A Procedures, Analyis, Treatments

A.1 Procedure

The enterprise SHALL plan, control, and permanently improve the procedures requested in these Guidelines.

This SHOULD take place within the scope of a quality management and based on a recognised standard, such as the DIN EN ISO 9001.

Any other manner of proceeding SHALL comply with the following requirements:

1. It is defined who shall be responsible for accomplishment.
2. Procedures are defined in a way that the corresponding target group can access them and understands them; they are documented and published.
3. Procedures are improved when any deficiencies in realisation, adequacy, and effectiveness turn out.
4. Every year, the realisation, adequacy, and effectiveness of one third of the procedures is subject to review. The procedures to be reviewed are selected randomly. If the yearly review reveals that more than half of the procedures subject to review show deficiencies, all procedures will be reviewed.

A.2 Risk Analysis and Treatment

The enterprise SHALL carry out the risk analyses required in these Guidelines and treat any detected risk promptly and adequately.

This SHOULD take place within the scope of a risk management and based on a recognised standard, such as the BIS standard 100-3, the ISO/IEC 27005, or the ISO 31000.

Any other manner of proceeding ABSOLUTELY requires implementation of a corresponding procedure (see Annex A.1), which meets the requirements of the paragraphs below.

A.2.1 Risk Analysis

A risk analysis SHALL meet the following requirements:

1. The documentation lays down how to proceed with risk identification and assessment.
2. This manner of proceeding guarantees that any threat or weak point can be detected reliably.
3. Risk assessment takes place on the basis of potential damage to the enterprise and its probability of occurrence.
4. The result of the risk analysis allows prioritisation when treating the risk.

A.2.2 Risk Treatment

Identified risks SHALL be treated promptly and with priority; this is provided for by defining, documenting, and implementing appropriate measures to prevent, reduce, or transfer risks (e.g. by effecting an insurance).

Implementation SHALL be verified and checked for effectiveness.

If risks cannot be treated adequately, the top management SHALL accept them and document this.

A.2.3 Repetition and Adaptation

Risk analyses SHALL be reviewed for up-to-dateness and repeated if required.

Moreover, risk analyses SHALL be revised promptly upon occurrence of one of the conditions below:

1. The object of the risk analysis has substantially changed (e.g. hardware, software, or configuration of an IT system).
2. The intended use of the object has substantially changed.
3. The danger has increased (e.g. a new danger has emerged or an existing danger has increased considerably).

Annex B Partners and Institutions

1. VdS Schadenverhütung GmbH
   This document is based on the *VdS Guidelines for Information Security, Cyber Security for Small and Medium-sized Enterprises (SME), Requirements* and was kindly supported by it's publisher, VdS.
2. Bundesamt für Sicherheit in der Informationstechnik, BSI
   Federal Office for Information Security; it's goal is to promote IT security, it's the first and foremost the central IT security service provider for the federal government in Germany. It's tasks may be taken over by specialised providers of other countries as well.