Finantsinspektsioon

# REQUIREMENTS FOR THE ORGANISATION OF THE INFORMATION TECHNOLOGY AND INFORMATION SECURITY OF THE SUBJECT OF FINANCIAL SUPERVISION

This advisory guide was instated by decision no. 1.1-7/19 of the Management Board of the Financial Supervision Authority on 23 January 2017 and Resolution No. 1.1-7/43 of the management board of the Financial Supervision Authority of 12.02.2018 pursuant to subsections 57 (1) and (3) of the Financial Supervision Authority Act.

CONTENTS

# 1. General provisions and terminology

## 1.1. Competence

1.1.1. In accordance with subsection 3 (1) of the Financial Supervision Authority Act (hereinafter FSAA), the Financial Supervision Authority conducts state-level financial supervision in order to protect the interests of clients and investors in maintaining their resources, and thereby support the stability of the Estonian financial system by increasing the stability, transparency, and functioning of the finance sector, while impeding systemic risks and the use of the finance sector for criminal purposes.

1.1.2. In accordance with subsection 57 (1) of the FSAA, the Financial Supervision Authority has the right to issue guides of an advisory nature in order to explain acts pertaining to the legislation of the finance sector, or to provide direction for the subjects of the Financial Supervision Authority.

## 1.2. Purpose and area of implementation

1.2.1. The purpose of this guide (hereinafter *guide*) is to implement minimum requirements for the organisation of information technology and information security of companies in the finance sector – thereby increasing the sector's efficiency – and to minimise systemic and operational risks.

1.2.2. This guide regulates the organisation of information technology and information security arrangements for entities established as the subjects of financial supervision in subsection 2 (1) of the FSAA, with the exception of the technical arrangements of credit agents, insurance agents, small fund managers without an activity license, investment agents, and payment agents.

1.2.3. This guide describes minimum requirements for the organisation of information technology and information security, as determined by the Financial Supervision Authority, for the subjects of supervision. In preparing the recommendations and requirements of this guide, the recommendations of internationally recognised standards ISO/IEC 27001 and ISO/IEC 27002 have been used.

1.2.4. In the implementation of this guide's requirements, as well as the development of respective solutions for any specific subject of supervision and the nature of the subject's business activities, the company's effect on the finance sector as a whole and the magnitude of risks and effects of their realisation all need to be considered.

1.2.5. When implementing this guide, legal requirements and guidelines from other guides issued by the Financial Supervision Authority need to be considered. In the case of special legal requirements, one must first consider the requirements specified in the legislation.

1.2.6. In the implementation of this guide, the „fulfil or explain" principle must be followed, according to which the subject of supervision must, if needed, be able to explain why they do not fulfil, or fulfil partially, some part of this guide.

1.2.7. The organisation of information technology and information security of companies in the finance sector must ensure appropriate support for business processes. A company's IT systems must correspond to the availability, integrity and confidentiality demands stemming from their business practice and external requirements. The particular application of this guide within a company depends primarily on the complexities of the processes involved and the magnitude of consequences.

1.2.8. In the implementation of this guide, and in the case of problems with its interpretation, one must proceed from the principle of reasonableness, considering the guide's objectives, and operate in good faith and with the due diligence expected from subjects of supervision.

## 1.3. Terminology

1.3.1. **Audit trail** – an element of information confirming the occurrence of an important event; a visible trail or piece of evidence that allows for information found in a testimony or report to be traced to its initial source.

1.3.2. **Company** – for the purposes of this guide, an entity considered as subject to financial supervision pursuant to subsection 2 (1) of the FSAA. This guide does not consider as subjects of supervision: credit agents as specified in subsection 21 (1) of the CCIA, insurance agents as specified in subsection 174 (2) of the IAA, small fund managers without an activity license as specified in § 453 of the IFA, investment agents as specified in subsection 119[1] (1) of the SMA, payment agents as specified in subsection 59 (1) of the PIEMIA.

1.3.3. **Information asset** – information, data and tools required for the processing thereof, which can either belong to the company or be stored under bailment (e.g. personal data).

1.3.4. **Owner of the information asset** – a company employee who approves security measures and grants access rights pertinent to the information asset, and monitors the functioning of information security measures.

1.3.5. **Information security** – the protection of information to ensure:

- confidentiality – the protection of information from unauthorised access;
- integrity – the protection of information from counterfeiting and unauthorised change;
- availability – the timely and sufficiently systematised accessibility of information and services.

1.3.6. **Information security measures** – activities, processes and tools enacted by the company to manage, measure, and diminish risks, and to prevent and avoid security incidents, and minimise the damage they may cause.

1.3.7. **Information security policy** – a written document stating the company's goals pertinent to information security and general rules set to achieve them.

1.3.8. **Incident** – an unwanted event which results (or may result) in the violation of information security or damage to the company's activities.

1.3.9. **Encryption** – the transformation of information to disguise its contents, prevent unauthorised use or prevent unnoticed change.

1.3.10. **Log** – a chronological journal of events, which is stored as a data file for subsequent revision and analysis.

1.3.11. **Multi-factor authentication** – authentication using at least two independent authentication factors.

1.3.12. **Major incident** – an incident to which at least one of the following conditions apply:

- > 25% of the usual service is influenced or likely to be influenced;
- > 25% of customers are influenced or likely to be influenced;
- the incident has notable financial effects
- the incident has escalated to the highest level of management and the company has enacted its continuity plan
- the incident has caused or may cause major harm to the company's reputation;

Or to which at least three of the following conditions apply simultaneously:

- > 10% of the usual service is influenced or likely to be influenced;
- > 10% of customers are influenced or likely to be influenced;
- the incident has caused an interruption in the service lasting more than 2 hours;
- the incident has escalated to the highest level of management;
- the incident has affected other service providers or a relevant infrastructure;
- the incident has caused or may cause major harm to the company's reputation

1.3.13. **Sensitive information** – information, the confidentiality and integrity of which needs to be protected in accordance with the decision of the competent body within the company, as its disclosure, change, destruction or loss would result in major harm.

1.3.14. **Secured area** – the area in which critical infrastructure components are placed, and the protection of which involves special security measures.

1.3.15. **Key management process** – activities pertaining to cryptographic keys and related security measures, enacted throughout the lifetime of the key.

## 2. Documentation and arrangements

### 2.1. IT strategy

2.1.1. A company's IT activities must be based on a strategy derived from the business goals and strategies instated by its management (IT strategy). In forming an IT strategy, the type of technical support needed to achieve the company's business goals must be considered, as well as whether existing IT solutions would allow for desired business outcomes to be met. The company's strategic plan needs to be sufficiently detailed to allow for the setting of concrete development

plans, and determining of priorities and investments pertaining to IT projects.

2.1.2. The IT strategy must be regularly updated, and upon changes in the company's business strategy or developments in information technology, accordingly complemented. The company's business, IT and information security side must be involved in the process of planning the IT strategy.

## 2.2. Information security policy

2.2.1. A company's general principles of information security must be specified in a security policy and approved by its management. The goal of the security policy is to determine the company's strategic approach to the organisation of information security.

2.2.2. As a minimum, the information security policy must contain the following provisions:

- the definition of information security, as well as the goals and principles guiding the activities that influence information security;
- both general and specific obligations, as relegated to concrete roles for the management of information security;
- processes used to handle derivations and exceptions.

On a lower level, the information security policy must be supported by topic-specific policies, which include action plans, standards, procedures, and guides supporting the enactment of information security.

2.2.3. A company's employees and relevant external parties must have an awareness and understanding of the information security policy and derivative documents implemented within the organisation, as well as the role and responsibility of employees in ensuring information security. In the case of an important change in the information security policy, employees and relevant external parties must be notified. When hiring a new employee, the effective security policy, derivative documents, and their role and responsibility in ensuring information security must be introduced.

2.2.4. Stemming from the company's field of activity, business and IT strategy, as well as risk tolerance, appropriate principles for the revision of its information security policy, incl. frequency, must be established. The company must regularly revise its information security policy, and every major change in the company's business activity or IT organisation must, if necessary, be followed by supplementing its security policy.

## 2.3. Internal rules and procedures

2.3.1. Timely, appropriate and adequate internal rules must be enacted within a company, which ensure the confidentiality, availability, and integrity of data in, among other things, the development, maintenance, and use of the information system, and ensure that data is processed in accordance with valid legislation and the best practices.

2.3.2. The company must ensure the timeliness and relevance of its internal rules. When making changes in the information system, relevant procedures must also be revised and users notified of the performed changes.

### 2.4. Management of investments

2.4.1. For optimal management of funds spent on technology and information security, investments must be managed through a periodical budgeting process.

2.4.2. The management must analyse information technology and information security arrangements at least once a year. It is recommended that the purposeful use of IT resources in support of business strategies be regularly revised, and that the budget for the next period be confirmed.

## 3. Staff

### 3.1. IT organisation

3.1.1. An IT organisation of appropriate size and competency must exist within a company to provide processes with sufficient technical support. If IT-related expertise is outsourced, it is necessary to determine the fields in which outsourcing can be used, as well as who and in which way will be managing the service.

3.1.2. Appropriate procedures for hiring IT personnel, which allow for the assessment of candidates for relevant positions, must be enacted within a company. In addition to specialised competency, the need to work with sensitive information and the company's sphere of activity must also be considered.

3.1.3. A company's IT organisation must have a clearly defined structure and tasks, as well as resources needed to fulfil its obligations. Skills, rights, responsibilities and obligations required from employees must be clearly defined and regularly revised.

3.1.4. Development and managerial functions must be separated within a company. If the separation of these duties is not possible, additional controls must be instated to decrease risks, considering that an employee must not perform the inspection or supervision of their own work.

3.1.5. A company must pick and determine central IT employees and enact additional controls to minimise excessive dependence on them.

### 3.2. Information security organisation

3.2.1. Common responsibility for ensuring information security lies with a company's management board. A person directly responsible for information security – information security manager – must be separately designated within the company. The creation of a separate position may prove expedient depending on the organisation's size and the complexity of its activities. An information security manager must be directly subordinated to a level within the company which allows for their tasks to be fulfilled. It is recommended that responsibility for coordinating information security is assigned to one member of the management board.

3.2.2. For the incorporation of the business side of a company into questions relating to information security, the assembly of an information security steering committee, which should include the managers of all important business factions or functions, as well as the information security manager, is recommended.

3.2.3. Through enacting an information security manager and IT risk management functions, the company must, at a minimum, ensure the following:

- the identification and classification of information assets, and the functioning of information security processes (incl. IT risk management);
- the determining of owners of information assets;
- the determining of the existence of relevant documentation pertaining to information security and its enactment;
- the correspondence of information security organisation to the information security policy, internal regulations and external demands through the enactment of appropriate organisational, physical and IT security measures;
- regular notification, but no less than once a year, of the company's management of the correspondence of the company's security levels to internal and external requirements and of the efficiency of enacted IT security measures;
- the briefing of the management of notable information security incidents and their solutions;
- the consideration of security concerns in developing or updating information systems;
- the operation of continuity and restoration processes relating to information systems;
- the notification of employees of security rules, and counselling pertaining to information security related topics. Also, if needed, training employees to raise general security awareness.

## 3.3. Employees

3.3.1. Mechanisms must be enacted within a company for the background checks of employees hired to responsible positions (e.g. employees having special privileges in the company's information systems). In addition to specialised expertise, the need to work with sensitive information and the company's field of activity must also be considered.

3.3.2. Prior to granting users access to information assets, their awareness of the organisation's policy and procedures (incl. security requirements and other operational mechanisms), as well as the functional use of IT tools must be ensured. To raise security awareness, it is recommended to organise regular trainings in the company, which would involve all employees (incl. the management) and which would introduce above all the information security policy of the company, the importance of information security, the obligations and procedures related to information security, as well as security requirements, notifying of incidents, etc.

3.3.3. Contracts concluded with employees must, among other things, stipulate the obligation to store confidential information, and the responsibility that violating this obligation would entail even after the employee has left the company.

3.3.4. An employee's rights, obligations and responsibilities must be stipulated in information security guidelines and other related internal regulations.

3.3.5. The confidentiality requirements, security roles and responsibilities stipulated within an organisation's information security policy must be specified for each employee. The responsibility of each staff member for ensuring information security in fulfilling work tasks must be clearly expressed in the organisational culture, as well as the contracts and agreements made with employees.

### 3.4. Use of an external service provider

3.4.1. A company is responsible for the functioning of services outsourced to an external service provider to the same extent as it would be if they were providing it themselves. Guidelines and regulations for outsourcing services have been stipulated in the Financial Supervision Authority's guideline "Outsourcing Requirements for Supervised Entities".

3.4.2. Prior to deciding to purchase goods or services, or to continue outsourcing an activity (hereinafter *outsourcing*), a company must determine the requirements for the contents, quality, and security pertaining to the goods or service, and assess associated risks, as well as potential service providers. When outsourcing, a strategy for ending the service must be specified in case the contract is cancelled.

3.4.3. A company must regularly assess risks arising from the use of an external service provider, incl. risks to security. This assessment must be performed when choosing an external service provider, concluding a contract, and negotiating the appropriate service level agreement. Depending on the nature of the service, it may be necessary to specify which security requirements the service provider is obligated to meet. If the information system is developed or administered by an external service provider, the system's minimum information security level must not be lower than the one stipulated by the service level requirements enacted within the company. The company must establish a control mechanism to ensure the assessment of an external service provider's information security capability.

3.4.4. In the contract between a company and an external service provider, the contents and scope of the service must be precisely determined. The contract must define in detail the description, security requirements, and confidentiality requirements pertaining to the service, as well as the company's right to obtain information needed to monitor the service, the service provider's obligation to immediately notify of incidents, and the grounds, conditions, and procedures for the changing, ending and cancelling (incl. timely and extraordinary) of the contract.

3.4.5. The process of communicating with an external service provider must be formalised. To monitor the service, a process must be enacted within the company for assessing the fulfilment of business requirements, contractual provisions and service level agreements by the external service provider.

3.4.6. When outsourcing a service, incl. cloud-based processing, a company is required to maintain adequate control over information containing customer data, including its transmission, location

and storage. The company's information systems must, at a minimum, be separated in a logically secure way from the information systems of a service provider's other clients.

3.4.7. A company must ensure that when using an external service provider, sufficient and necessary rights for both the company and the party conducting supervision are contractually established for the purpose of verifying and assessing the service provider's activities, and obligations to submit to such controls and cooperation. Such rights must, among other things, encompass the right to receive satisfactory information about the service provider's activities (the service provider's obligation to report), provide additional guidelines for providing the service, as well as to demand the execution of such guidelines. The company must supervise the quality and security of the outsourced service.

## 4. Information assets and risk management

4.1.1. A process for managing IT risks must be ensured by the company's management, which determines the functioning of the methodology, the duty to report, and control mechanisms pertaining to risk management. The methodology used for risk analysis must be documented.

4.1.2. The company's management must ensure general rules and the functioning of a relevant process related to the classification of information assets and determining of their owners.

4.1.3. At a minimum, the owners of information assets should have the following obligations:

- taking part in risk assessments relating to one's own information assets, and accepting its results;
- accepting residual risk and security requirements determined on the basis of risk assessments;
- with regard to IT services, the concluding and approval of service level agreements;
- ordering, prioritising and coordinating changes pertaining to one's information assets;
- regulating access rights related to one's information assets, and the supervision of authorised employees;
- setting requirements for audit trails.

4.1.4. During a risk assessments, a company must determine potential threats and weaknesses affecting its information assets, assess the probability of risk realisation, as well as the damages these risks may cause, choose appropriate measures to inhibit the effects of risk realisation, determine their profitability and decide the acceptable level of residual risk.

4.1.5. The security needs of information systems and the related controls and measures must be determined in cooperation with the owners of information assets.

4.1.6. In assessing risks, among other things, risks emerging from the company's technical solutions, processes, and external parties, as well as the results of the monitoring of information systems must be considered.

4.1.7. Based on the results of a risk assessments, security measures must be introduced, enacted and put into practice for information assets within a company.

4.1.8. Each important change in the information system or process must be followed by a risk assessment. When planning updates in IT systems, it is necessary to determine whether and how the change will affect the security of the system and process, as well as to diminish, in every way, the effects of the risks produced by the change.

4.1.9. A company must ensure the regular updating of risk assessments (at least once every year) and the continuity of the risk management process. Risks must be assessed throughout the life cycle of the information system, i.e. throughout development, application of changes, manifestation of major threats, realisation of major incidents or the increase of its quantitative amount. Based on the results of the risk assessments, the security measures of information assets and supervision must be supplemented as necessary.

4.1.10. The results of risk assessments and relevant reviews must be presented to the company's management.

## 5. Physical and environmental security

### 5.1. Secured areas

5.1.1. A company must chart out areas, which, from the standpoint of information security, need protection and into which only authorised persons may enter. IT tools supporting critical or sensitive functions must be located in secured areas with limited access, and they must be physically protected from unauthorised queries, damages, security risks (e.g. fire) and environmental risks.

5.1.2. Physical and logical access controls must be used for the protection of secured areas with limited access in such a way that only authorised persons can access the area.

5.1.3. Secured areas with limited access must be constantly monitored to prevent possible damages, and for quick discovery and reaction if damage has occurred.

5.1.4. It is advised to base the measures used for protecting secured areas on standards described by an independent and accredited organisation. Security measures must be considered in early planning stages, such as the choice of location, and applied during the area's construction and instalment of its contents. When outsourcing a server hosting service, the same standards must be valid in choosing a service provider and their offered solution.

5.1.5. Secured areas must not have generally understandable markings or be marked on signs.

5.1.6. The possibility of accidental physical damage to data and power cables must be avoided. For this purpose, the use of a special bearing structure for cabling, hidden with appropriate materials in commonly used spaces, is recommended. Appropriate markings should be used in junctions for electric and data cables, which, in the case of problems, allows for the quickest possible way for a cause to be determined.

## 5.2. Network security

5.2.1. A company must have a timely overview of its computer network and access schemes.

5.2.2. Network security measures must be applied to network access, as well as to the services used and the actions performed on the network.

5.2.3. A company's computer network must have sufficient logical and physical segmentation to ensure the fulfilment of enacted requirements pertaining to availability, confidentiality and integrity. Only services necessary for the fulfilment of the company's functions should be allowed into the data stream between local and external computer networks.

5.2.4. For data protection purposes, the company's computer network must use sufficiently secure network protocols and adequate and strong encryption algorithms.

5.2.5. A company must ensure the security of data upon its broadcast through a public or radio-based network. When passing confidential data through public networks, the possibility of that data becoming public to third parties must be eliminated. In the case of increased risk, the encryption of the entire information exchange occurring on the public network must be considered.

5.2.6. A company must ensure sufficient monitoring and logging of the network to discover and record weaknesses and activities possibly influencing information security. Appropriate intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be kept up to date and used to monitor network traffic and notify those in responsible positions upon the suspicion of abuse.

5.2.7. For the timely discovery and blocking of malware and viruses, necessary measures must be enacted and employee responsibilities designated. Additionally, users must immediately be notified of dangers arising from malware and viruses if an adequate information source informs that a threat to the company from viruses and malware has increased.

5.2.8. If the administration of information systems is performed using remote access, such activity must be protected using appropriate cryptographic (e.g. VPN) solutions and solutions allowing secure authentication.

5.2.9. When using wireless networking technology, necessary measures must be enacted to avoid unauthorised access to information systems.

5.2.10. A company should regularly check the computer network for possible weaknesses arising from either the internal or external environment, or after major changes in the network (adding a new system or device, changing the network's topology, changing the firewall settings, installing updates) and, if possible, conduct network infrastructure penetration tests.

## 5.3. Device security

5.3.1. A company must determine whether it allows the use of its information assets through mobile devices, considering the company's needs, risks arising from the use of such devices, and the capability of its IT department.

5.3.2. A company must determine the type of information permitted to be saved on local and mobile devices, and how it must be protected.

5.3.3. If remote access is allowed in a company's information system, appropriate security measures must be put in place to prevent the access of third persons to sensitive information.

5.3.4. Only software and configurations accepted by the company may be used in devices belonging to the company. The company must enact procedures and appropriate measures to protect devices from security risks.

5.3.5. The functionality of devices used within the company must be limited to a level necessary for fulfilling work tasks.

5.3.6. A company must ensure that if the user leaves a device inactive for a set period of time, the continued use of an information system or connection to the computer network only be possible after re-authentication.

5.3.7. If employees are allowed to use personal device for work, a company must have enacted regulations covering the use of personal devices, which precisely determine the requirements pertaining to the storage and forwarding of data, the maintenance of devices, and security. These regulations and measures used in personal devices must not diminish the level of information security enacted in the company.

5.3.8. Employees must receive sufficient instruction and security training about the previously mentioned regulations, its application, and the permissible use of personal devices.

### 5.4. Security of storage media

5.4.1. A company must enact regulations concerning the use of storage media and its distribution within the organisation and to third parties. These regulations must specify and enact requirements for the use, storage, and secure destruction of storage media.

5.4.2. A company must specify and enact appropriate measures for the protection of storage media.

5.4.3. Appropriate technical measures (e.g. data encryption) must be enacted to protect information stored on external media.

5.4.4. When forwarding a data medium, a reliable and secure courier service, of which a precise overview can be attained, must be used.

## 6. Management of communication and operations

### 6.1. Capacity and performance management

6.1.1. A company must have enacted a process for reporting and monitoring the information system's performance. User requirements for the accessibility and performance of the information system must be regularly revised and specified. The timely fulfilment of requirements relating to the information system's performance must be ensured on the basis of monitoring the performance of the existing system and prognosis of future performance requirements.

### 6.2. Configuration management

6.2.1. A company must possess complete and regularly updated documentation relating to the installation and configuration of the hardware and software used in its IT systems. The hardware and software platform used must, if possible, be standardised.

6.2.2. To protect against weaknesses arising from the software's technology, a company must enact rules for monitoring the issuance of software updates, their testing and application. The responsibility of administering software updates must be determined for each separate software system.

6.2.3. When changing the information system's configuration, the procedure for change management, through which prior analysis, documentation, testing and coordination of installation is to be ensured, must be followed

6.2.4. Prior to installing a system or device onto the network, the manufacturer's default security settings must be modified (changing the password, closing unnecessary accounts etc.).

6.2.5. A company must enact regulations, which rule out the use of unauthorised and unlicensed software. The company must establish routine controls to discover unauthorised software and check the validity of license agreements.

6.2.6. A process for installing updates and applying security patches to the information systems' standard software and system components must be ensured within a company. New security patches should only be installed when there is conviction within the company of there being no side effects. There should be regular checks for the availability of new software patches. The company must ensure that known security vulnerabilities are minimised and that security measures are enacted according best practices known at the time.

6.2.7. After performing necessary changes, a company must ensure that the functionality of standard software and system components is brought to the lowest necessary level. In addition, unnecessary services and protocols must be closed (the protocols and services that are not directly required for fulfilling the device's main function).

### 6.3. Change management

6.3.1. When planning and executing changes within a company's information system, their effect on businesses and existing technical solutions must be determined. Different variables, which need to be evaluated and analysed, are used as a baseline for determining such effects. These variables include the following:

- effect on the IT service, system, and infrastructure;
- effect on other systems that function within the same infrastructure;
- effect on the system's security (in the case of major changes pertaining to the purchase of new hardware, software, or services, prior analysis is necessary to determine new security requirements);
- the impact of not implementing the change;
- IT and other resources needed for applying changes.

6.3.2. An action plan must be assembled for executing the changes. The performance of planned and unplanned changes must be coordinated with and approved by the owner of the respective information asset.

6.3.3. All persons involved must be notified of the details of the changes.

6.3.4. In order to diminish the probability of interruptions, errors and violations of legal requirements as a result of performing changes in the information system, the legality and verifiability of the proposed changes, while considering their goals, must be ensured. An audit trail of performed changes, which allows for later establishment of the time the changes were applied and the person performing them, as well as the nature of the changes, must be retained.

6.3.5. Planned changes in a system's software and hardware must go through prior testing. Before applying the changes, appropriate restoration procedures must be defined which could be immediately enacted to restore the system's previous state in the case of failure. It is recommended to also perform prior tests of procedures for restoring systems.

6.3.6. A company must ensure the usability and integrity of information required by an administrative act or action by an organisation conducting financial supervision in the same amount as prior to the act or action. If this requirement is not met as a result or possible result of applying changes to the information system, a motivated statement regarding the changes performed and legal protection provisions or other provisions applicable to the owner of the information asset must be presented to the organisation executing financial supervision.

### 6.4. Logs and the monitoring of information systems

6.4.1. A company's information systems must be monitored. At a minimum, monitoring must ensure the enactment of preventative measures in the security administration of the systems and the timely identification of incidents.

6.4.2. The following must be ensured through the monitoring of information systems:

- the timely identification of internal and external threats;
- identification of vulnerabilities within the information systems;
- the detection and prevention of unauthorised use of hardware and software;

- the monitoring of the information systems' configuration and device changes;
- the monitoring of the availability of information systems, devices and processes.

6.4.3. A company must enact appropriate monitoring of a system's usage and access for the purpose of timely discovery of unauthorised activity, assessment of enacted measures relating to access security, and the identification of errors in the information system.

6.4.4. Unauthorised activity includes all activities with which legal requirements are violated, or the purpose or content of which is inappropriate fulfilment – or lack of fulfilment – of an administrative act or action by an organisation performing financial supervision, incl. the violation of the integrity or usability of information as compared to its state prior to the receipt of the act or performing of the action. When a relevant demand is received from an organisation performing financial supervision, a company must justify such unauthorised action in detail.

6.4.5. To set up monitoring, it is necessary to have a log of actions performed in the information system. The appropriate monitoring level for various elements of the information system must be determined on the basis of a risk assessment. A company must ensure sufficient analysis of logs to discover errors in the functioning of the system or violations of availability, integrity, or information confidentiality.

6.4.6. A company must use appropriate measures and tools to analyse logs. These measures and tools must be accessible only to authorised personnel.

6.4.7. In accordance with the security requirements pertaining to information assets, stated in legislation and determined within a company, it is necessary to determine the types of actions about which logs will be recorded and stored for set deadlines.

6.4.8. Logs pertaining to information important to the company must, at a minimum, be kept about the following actions (whether or not the action was successful or unsuccessful):

- entrance into the system;
- the viewing of information;
- the making of queries;
- addressing the system and application;
- changes and actions in the database;
- attempts to access sensitive information;
- using systems and performing actions with special (privileged) usage rights;
- unauthorised actions in the information system.

6.4.9. A log must, at a minimum, contain the performer of the action, action type, and time of its execution.

6.4.10. When saving, administering and storing a log, its unavoidability, availability, integrity and confidentiality must be ensured. It is recommended to store the media containing log files in a safe area and separately from the information processing environment being logged.

6.4.11. To ensure chronological precision, all clocks related to the process must be synchronised.

## 6.5. Backups and continuity

6.5.1. Action plans and guidelines for the organising of business continuity for the subjects of supervision have been established in the Financial Supervision Authority's guideline entitled „Requirements for Organising the Business Continuity Process of Supervised Entities."

6.5.2. A company must document and establish the procedures for making and restoring backups, which determine the organisation's requirements for the backing up of information, software and systems, as well as storage and protection of backed-up data. The scope and frequency of the backups should reflect requirements arising from the organisation's activities, security requirements pertaining to relevant information, and to how critical the information is from the standpoint of continuing its activities.

6.5.3. The backup procedure must encompass at least the following topics:

- the information which needs to be backed up;
- the scope and frequency of backing up;
- responsibility for making backups
- the amount of time that backups are stored for;
- testing the restoration of backed up data.

6.5.4. Backup copies need to be made regularly and they must be stored in a secured area, which rules out unauthorised access. This must ensure a relevant level of physical and environmental protection for copies, which corresponds to the norms enacted in the main location. One backup copy must be regularly and securely stored in a far enough location to avoid damage in the case of an emergency in the main location.

6.5.5. Backup copies must be protected from unauthorised use and data corruption. If needed, the copies must be protected with encryption.

6.5.6. The usability and integrity of backup copies must be regularly examined to ensure their usability in the case of an emergency, and verify that the backup procedure corresponds to the requirements stipulated in the company's continuity plans. In business-critical systems and services, the back-up procedure should encompass all the system data, applications, and information necessary to restore the whole system in the case of emergency.

6.5.7. A company must determine and enact a timeframe for the storage of information assets, considering legal requirements, expiration dates and the possible interest of financial supervision authorities in this information.

6.5.8. If a company's employee or member of management creates or edits work-related information on a system not belonging to or used by the company (e.g. personal device, personal mailbox with a service provider, etc.) and obligations for the immediate saving of such information are not specified by law, the company must ensure the storage of a copy of the created and edited information as soon as possible on technical solutions owned or used by the company.

## 7. Encryption

7.1.1. Depending on need and the sensitivity of relevant information, for the primary purpose of ensuring confidentiality and integrity, encryption must be used to protect information.

7.1.2. Rules must be enacted within a company about the use of encryption. These rules must state the cases in which data encryption is mandatory. The used cryptographic algorithm, encryption key lengths, and conditions for how cryptographic keys are to be managed, must also be agreed upon.

7.1.3. The key management processes enacted in the company should determine the functioning of the following actions:

- generation of encryption keys;
- distribution, storage, changing and destruction of encryption keys;
- replacement of encryption keys if they become, or are suspected to have become public;

## 8. Management of access rights

### 8.1. Management of access rights

8.1.1. A company must enact a policy or procedure which encompasses all the phases of the access rights' life cycle, incl. the initial registration of users, changing of access rights, and the final un-registering of users, or the revoking or stopping of user rights.

8.1.2. The access rights policy or procedure must determine all possible access locations: the work computer, data network, operating systems, applications and databases, mobile and remote access to information assets, the access of temporary and external users to the information system etc.

8.1.3. Everyone who uses information assets must be identified and authorised. Depending on the sensitivity level of the information asset, the level of identification and authorisation, as well as relevant rules, must be determined.

8.1.4. Access rights and other workflow regulations need to be set up in a way which allows the company to identify the user of an information asset with adequate confidence. It must be possible to individually identify a company, its employee or member of management, having used the information asset, as pertaining to each performed action.

8.1.5. A company must determine and enact a procedure for verifying access rights. The correspondence of documented access rights to those actually issued must be regularly confirmed. The correspondence of rights granted to a user for their actual work-related needs must also be regularly confirmed. If access rights no longer relevant, or for which there are no users, are discovered during this process, they must be removed.

8.1.6. Access to data and information must be limited only to persons for whom it is needed for work-related duties. The granting of access rights must be consulted with the owner of the information

asset. This requirement also applies to the so-called technical users of an information system. Access rights must be documented and based on the will of the owner of an information asset. The methodology for documenting access rights must ensure a clear overview of their management process and the access rights currently in effect.

8.1.7. Employees and external service providers must be stripped of access rights to information and data processing tools upon the cessation of a business relationship, contract or agreement. In the case of changes in the relationship, contract or agreement, access rights must be modified accordingly. Special attention must be devoted to the timely deactivation of access rights upon an employee's departure or the termination of relations with a service provider. If there is erosion of trust, access rights to information systems must be revoked before the employee or external service provider is officially notified of their contract having been terminated. If an employee is away for a longer period of time, revoking access rights until their return should be considered.

8.1.8. Unique usernames must be determined for system administrators as well. If the technology in use allows, individual accounts for each administrator for everyday system administration should be created in addition to the built-in administrator account. Copies of codes and passwords in common use and related to administrative rights need to be stored securely.

8.1.9. Stricter rules must be enacted for administrative or privileged accounts as compared to accounts of regular users (incl. requirements for the validity and complexity of authentication measures, logging of actions, procedure for changing authentication data for commonly used accounts after an employee leaves).

## 8.2. Authentication

8.2.1. A company must enact rules for the use of appropriate authentication measures (e.g. password, PIN, smart card, biometric access measures etc.).

8.2.2. Special care must be devoted to monitoring the outside use of services on a company's internal network. Before opening a remote access service and granting appropriate access rights, the identity of the external user must be determined for the use of a specific service and the performing of specific actions. Depending on the nature of the service, multi factor authentication should be considered for its users.

8.2.3. The management of passwords must be coordinated with the owners of an organisation's information assets, and its terms must be known to all employees able to access them. At a minimum, password management must include information about the following – the procedure for creating passwords and notifying the users of passwords, the frequency and conditions for changing a password, storage of passwords, the user's responsibility, and rules for managing the passwords for users with special privileges.

8.2.4. A company must enact rules for choosing and managing passwords. Passwords given to users within an information system must, at a minimum, be at a level of complexity which will, in all likelihood, rule out brute-force cracking.

8.2.5. Classified authentication information must be kept confidential. In addition, it must be ensured that classified authentication information not become known to other employees or third parties (e.g. passwords may only be stored in an encrypted form, the password of an individual user may not be in common use).

8.2.6. Users must be notified of their responsibilities for the secure use of passwords. The user whose password was used to gain access to the information system is responsible for the actions performed.

## 9. The development and acquisition of systems

9.1.1. When developing or acquiring IT solutions, functional and non-functional requirements, incl. serviceability, performance, reliability, monitoring, security and compatibility with existing systems, must be specified.

9.1.2. The development of an information system must be based on a company's needs. The decision to initiate development projects must be made by the management and based on an approved IT strategy.

9.1.3. To create or acquire a solution suitable for fulfilling a company's business needs, respective user requirements must be determined and alternative solutions must be considered. The management must decide the launch of a development project, and in the case of alternative solutions, base its decision on analysis of implementability, which shows technical, operational and economic justifications for the project.

9.1.4. To minimise security risks for new solutions and any existing solutions connected to them, a company must ensure the proper functioning of processes pertaining to system development and administration.

9.1.5. When developing, changing or updating a company's information systems, the information systems must process data in the determined way. Data quality must be ensured by checks in both the input of data and the use of any output.

9.1.6. The implementation of an information system must not have any negative impact on the company's existing infrastructure or the security of other systems functioning within the same infrastructure.

9.1.7. In developing software applications, the best known practices must be used and the principles of information security should be followed throughout the software development cycle.

9.1.8. The separation of the development, testing and production environments must be ensured when developing software applications.

9.1.9. System requirements, standards, acceptance criteria, and intellectual property rights must be specified when ordering development work from external service providers.

9.1.10. Standards for testing and acceptance criteria must be clearly defined. Prior to deploying the information system, the system must be tested according to a testing plan. The testing plan must contain, among other things, tests pertaining to security and interfaced systems.

9.1.11. The use of real data in testing environments should be avoided. If real data is used in a development or testing environment, security measures equal to the production environment must be used (incl. granting rights, authentication and auditing procedures, logging).

## 10. Incident management

### 10.1. Incident management

10.1.1. A company must enact procedures and duties to minimise losses arising from security attacks, incidents or malfunctions, as well as to register incidents, react to them, and make appropriate conclusions.

10.1.2. The notification procedure for various types of incidents (e.g. violation of information security, threat, defect or malfunction), which could affect the security of a company's assets, must be made known to all involved parties. It is necessary to inform of every discovered or suspected incident as soon as possible.

10.1.3. When solving an incident, information gained during this process must be retained, so that it would be possible to determine exactly what happened in subsequent investigation and confirm that the information used to make conclusions has not been changed between the occurrence of the incident and its solution.

10.1.4. A company's procedure rules must ensure that each determined and reported incident be designated a responsible party, whose main purpose is the coordination of the incident's solution. Procedural rules must, among other things, contain the description of a possible escalation of the incident.

10.1.5. Incidents must be analysed to determine the reasons for their occurrence, establish possible deficiencies, and develop measures (asses the efficiency of previously applied measures) for their elimination and, through that, avoid the future recurrence of such incidents. Analysis of incidents also aids in assessing the efficiency of applied measures and helps determine what kind of expertise needs to be developed in the company's clients and employees to avoid the recurrence of similar incidents, as well as in helping to acknowledge, within the company, how the resolution of incidents could be better organised in the future.

### 10.2. Notifying of incidents

10.2.1. The legislation that regulates the operations of subjects of financial supervision stipulates the right of the Financial Supervision Authority to receive information from subjects of financial supervision for exercising supervision.

10.2.2. Based on acts established in clause 10.2.1 of this guide, the Financial Supervision Authority asks that a company:

10.2.2.1. notify the Financial Supervision Authority as soon as possible of major incidents by forwarding as much information about the incident as possible at the time of informing.

10.2.2.2. at least three days after the occurrence of a major incident, present the Financial Supervision Authority with a description of the occurrence by using general contact information and noting the following information:

- type of incident (availability, integrity, confidentiality);
- time of occurrence of the incident;
- the scope and effect of the incident;
- description of the incident;
- cause of the incident;
- solution of the incident;
- measures that are planned to be enacted for the prevention of similar incidents in the future.

10.2.3. If a subject of supervision sends the information described in point 10.2.2 to the Financial Supervision Authority within the scope of reporting carried out on the basis of legislation, the notification obligation described in point 10.2.2 will be deemed to have been performed.

## 11. Inspection and assessment of the organisation of information technology and information security

11.1.1. Regular and, in the case of major changes, irregular inspection of the organisation of information technology and information security must be enacted within a company. It must be assessed whether the rules enacted within the company have been followed, whether IT services are efficient and whether IT activities comply with business objectives.

11.1.2. If necessary, independent parties in the relevant field, for example an internal audit team, or if needed, an external auditor, must be used to assess management mechanisms, compliance with relevant legislation and regulations, and the fulfilment of contractual obligations and enacted technical measures. The results of this assessments must be presented to the company's management, which will enact correctional measures in the case of deficiencies.

11.1.3. In determining the need for and the planning of external audits related to the organisation of information security and information technology, the outsourcing of the auditing service needs to be considered if a company lacks relevant expertise. In determining the external service provider for conducting the audit, the service provider's competence and experience in conducting similar audits must be assessed.

11.1.4. Observations and notes made during the audit need to be considered in the planning and management of the organisation of the information technology and information security of the company. If serious deficiencies in the organisation of the information technology and information security of the company are discovered during the audit, a post audit must be performed after the deficiencies have been eliminated.

11.1.5. To determine possible weaknesses in critical information systems, the performing of penetration testing in tandem with the audit needs to be considered. In performing penetration testing, it must be ensured that the company's normal work will not be disturbed or the company's work-related information damaged.

11.1.6. A company's management must ensure regular assessments of the compliance of its information technology and information security organisation with external requirements (laws, regulations, contracts, etc.) and the consideration of their effects. If necessary, means of bringing the information technology and information security organisation into compliance with external requirements need to be enacted. All applicable requirements of laws, regulations and contracts and the company's method for fulfilling those obligations should be clearly determined, documented and kept up to date for each information system and the company as a whole. Relevant procedures must be enacted within the company to ensure compliance with laws, regulations and contracts and requirements relevant to the company's main activity having to do with intellectual property rights (incl. for example, the use of proprietary software), protection of data sets (against, for example, loss, destruction, counterfeiting, unauthorised access and unauthorised publication), privacy and protection of authorisation data, as well as the use of cryptographic security measures.

## 12. Application

12.1.1. This guide will enter into force on 1 May 2017.