FINANTSINSPEKTSIOON

Advisory Guidelines of Financial Supervision Authority

Requirements for the organization of the field of information security

These advisory guidelines were established by Resolution No 1.1-7/52 of the Management Board of the Financial Supervision Authority of 04.11.2009.

1. Competence

1.1 According to section 3 of the Financial Supervision Authority Act (hereinafter FIS), the Financial Supervision Authority conducts state financial supervision in order to enhance the stability, reliability, transparency and efficiency of the financial sector, to reduce systemic risks and to promote prevention of the abuse of the financial sector for criminal purposes, with a view to protecting the interests of clients and investors by safeguarding their financial resources, and thereby supporting the stability of the Estonian monetary system.

1.2 According to subsection 57 (1) of the FIS, the Financial Supervision Authority has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and to provide guidance to subjects of financial supervision.

2 Purpose and scope

2.1 Information security is a continuous process, during the course of which an entity assesses the risks connected with using information technology for business processes, chooses the ways in which it manages, measures and reduces risks, and makes sure that these measures are functioning.

2.2 The main goal of information security is to reduce the risks connected with using information technology for business processes to an acceptable level.

2.3 The purpose of these guidelines is to ensure a harmonious approach to the management of information security in supervised entities and describe the requirements for the information technology field, the performance of which results in the assurance that information security objectives are met.

2.4 These guidelines establish advisory and general codes of practice, and guidelines for supervised entities for organizing their information security processes.

2.5 The internationally recognized standards ISO/IEC 27001 and ISO/IEC 27002 were used for developing the recommendations contained herein.

3 Application of guidelines

3.1 These guidelines contain what the Financial Supervision Authority believes to be the minimum requirements for ensuring information security. When preparing the guideline's requirements and in the developing and implementing of corresponding solutions by a specific subject of supervision the scope of application of these guidelines, the nature of the subject's business activity, organization and the complexity of its functioning, the effect of the company on the entire financial sector as a whole, as well as information security risks and the weight of the consequences of their realization should be taken into consideration.

3.2 Application of these guidelines should take into account requirements arising from law, as well as the other recommended advisory guidelines of the Financial Supervision Authority and the characteristics of the particular supervised entity, as well as the internal organization of information security of the entity. Where the legislation provides for special requirements, these shall be followed.

3.3 The "comply or explain" principle should be taken into account in the application of these guidelines: if necessary, a supervised entity shall be able to explain why it is not applying or is only partly applying any of the paragraphs of these guidelines.

3.4 The guidelines should be applied, and any problems involving interpretation should be solved following the principle of reasonability, taking into account the purpose of these guidelines, and acting in good faith with the diligence expected of a supervised entity.

4 Definitions used in guidelines

4.1 **Information security** is the protection of information in order to ensure:

- confidentiality – protection of information against unauthorised publication;
- integrity – protection of information against counterfeiting and unauthorised alteration;
- availability – timely and regular availability of information and services for authorised persons.

4.2 **Information security measures** are the activities, processes and instruments taken by the enterprise to manage, measure and reduce risks and to anticipate, avoid and minimize the damages of information security incidents.

4.3 **Information security** policy is a written document, which defines the main objectives of enterprise information security and describes the main rules for achieving the objectives.

4.4 **Information assets** are information, data and the applications necessary for their processing.

4.5 **Owner of information assets** is an employee of a company who is liable for the security and maintenance of information assets and whose tasks, among others, include classification of data and determination of user's rights.

4.6 **Security incident** is an event the result of which is (or may be) violation of information security.

4.7 **Sensitive information** – information that, according to the decision of a competent authority, must be protected, as its public disclosure, alteration, destruction or loss would cause significant damage to somebody or something.

4.8 **Secure area** is an area inside of an enterprise's premises, where critical infrastructure components are maintained and for where special security measures have been implemented in order to protect these areas.

4.9 **Supervised entity –** a person treated as a subject of financial supervision under subsection 2 (1) of the FIS, including branches of credit institutions, insurance companies, investment firms and fund management companies within reach and content decreed in legal acts, except for insurance brokers as referred to in subsection 130 (2) 1) of the Insurance Activities Act.

5 Field of application

5.1 Information security issues shall be an integral part of a supervised entity's risk management.

5.2 The activities in connection with information security shall ensure that a supervised entity's information security risks are outlined and in order to prevent information security incidents adequate measures are taken, and in case incidents occur, predefined procedures and action plans will be practiced to ensure fast incident resolution and minimisation of damage.

6 Information security policy

6.1 Common information security principles of a supervised entity shall be represented inside of information security policy. Management should set a clear direction with information security policy, and demonstrate support and assistance in ensuring information security inside of the organization.

6.2 Information security assurance is a part of entity's risk management, and information security policy should conform to risk assessment results and correspond to the entity's information security level.

6.3 Inside of information security policy, conception of information security should be defined; the measures for ensuring information security, responsible persons for information security and programmes, standards, procedures and guidelines for implementing information security, should be described.

6.4 The employees of a supervised entity should be aware of current information security policy, regulations arising from information security policy, and their roles and responsibilities in ensuring information security. In case of bigger changes in information security policy, employees should be notified; newly recruited employees should also be instructed in current information security policy.

6.5 Based on the supervised entity's business area, business and IT strategy and risk tolerance, the frequency for bringing information security policy up-to-date should be established. Also, it should be ensured that an information security policy review takes place in the case of each larger change to business operations or in the organization of information technology.

7 Information security organization

7.1 Common responsibility for ensuring information security inside of an enterprise resides with the management board. Information security responsibility should be assigned to a specific employee and considering the size of the enterprise and complexity of its business, a separate post should be created. It is suggested that responsibility for organizing information security is assigned to one member of the management board.

7.2 The primary obligations of the responsible person shall be to ensure that information security activities correspond to information security policy and internal and external regulations. One of the most important functions for the responsible person should be coordination of the staff's activities in ensuring information security inside of the organization.

7.3 When including the business side in information security initiatives, it is suggested to create an information security steering committee consisting of the managers of all important business units and functions, and the information security officer (ISO).

7.4 The requirements for confidentiality, information security roles and responsibilities described in information security policy shall be fixed for each employee. Ensuring information security in performing their duties should be the responsibility of each employee and it should be expressed in organizational culture and contracts with employees. The employees shall be aware of their duties and responsibilities in ensuring information security.

7.5 A supervised entity should assess the risks connected with using external service providers, including risks to information security. This type of risk assessment should be done when choosing an external provider, in when concluding an outsourcing contract as well as stipulating service level agreements. Considering the content of outsourced services it should be determined which security criteria the service provider shall be required to meet. A control mechanism shall be established in the entity to allow for the assessment of the capacity of the external service provider's information security. Detailed requirements for outsourcing are covered by the advisory guidelines of the Financial Supervision Authority "Outsourcing Requirements for Supervised Entities", established on 25.10.2006 with management decision 1.1-7/84.

8 Organizational security

8.1 Mechanisms shall be established within the entity to control the background of employees to be placed in charge of important functions (for example, those employees who have special

rights in the information systems). In addition to competences of speciality, the features of the entity's area of activity and the need to work with sensitive information shall also be taken into consideration.

8.2 Before granting users access to the information assets, it should be ensured that they are aware of the entity's current policies and procedures (including security requirements and mechanisms for performance) and they know how to use information technology and systems as they were intended to be used. It is suggested that regular trainings be organized within the entity for all employees (including management) to increase the awareness of information security. The trainings would present, in first order, information security policy, the reasons behind the importance of information security, the duties and procedures connected with information security, security requirements, reporting about information security incidents and their effect.

8.3 As an additional information security measure, it is suggested that, among other things, an obligation to keep confidential information be added to contracts with employees as well as a liability for the violation of these obligations after the departure of the employee from the entity.

8.4 Employees' rights, obligations and responsibilities should be clearly defined within the information security regulations and other relevant internal regulations.

9 Physical and environmental security

9.1 A subject of supervision shall map the areas of the entity that require protection in terms of information security and where only authorized persons may enter. The information technology assets supporting critical or sensitive functions shall be located in secure areas with limited access, and these assets shall be physically protected against unauthorized application, damage, security threats (for example, fire) and environmental risks.

9.2 To protect secure areas with limited access, physical and logical controls shall be used in such a manner that only authorized persons are able to gain access to areas. A mechanism should also be put in place to ensure that all entries into such areas are recorded.

9.3 When selecting the measures used to protect secure areas, it is suggested to obtain as a basis the standards of an independent and recognized organization. The selection of measures should begin with the selection of the secure area and the implementation of methods, the construction and furnishing of the area. In the case of the outsourcing of server room

services, the same standards should be in place for the service provider and the offered solution.

9.4 In the case of secure areas, they should not be marked in an intelligible manner or listed references. When planning secure areas, construction in rooms with windows shall be avoided.

9.5 The possible physical or accidental damaging of communications and electricity cables shall be avoided. It is suggested that separate load bearing constructions be used for cables and in public areas they should be concealed with suitable structural materials. At connection points for communication and electricity cables the corresponding markings should be used, to enable the determining of the cause of the occurred problems as quickly as possible.

10 Communications and operations security

10.1 Secure areas with limited access should be continuously monitored to prevent possible damage and, in the case of damages, to enable rapid detection.

10.2 In order to organise monitoring, an audit trail of actions conducted in the information system is necessary. An appropriate monitoring level for different parts of the information system should be determined based on risk assessment results. An audit trail or logs shall be created regarding information that is important to the entity, taking into consideration at least the following possible events:

- Entry of users into the system;
- Viewing of information;
- Making inquiries;
- Turning towards the systems and applications;
- Database changes and operations;
- Attempts to gain access to sensitive information;
- Use of systems through special (expanded) user rights;
- Unauthorized operations inside of the information system.

10.3 For the timely detection of unauthorized activities and the assessment of the effectiveness of implemented access control mechanisms, an appropriate monitoring of system access and use should be established. An unauthorized activity is certainly an activity which results in the violation of requirements arising from legislation, or the purpose or content of which is the inappropriate implementation or failure to perform the administrative acts of the financial supervisory authority or investigative body, including the manipulation of the integrity or

availability of information compared with the period before the entity obtained an act or performed an operation. After obtaining the respective request from the financial supervisory authority, the subject of supervision shall give detailed reasons for the unauthorized activity described above.

10.4 Examination of logs shall be performed in cases where there is a motivated suspicion regarding the legality of the operations of the entity's employees or clients and also in instances where there is an actual threat regarding the violation of the entity's information availability, integrity or confidentiality.

10.5 Procedures shall be implemented and measures developed to administer recorded logs, to protect the availability of logs, their integrity and confidentiality. It is suggested to store the data carriers of log files inside of secure areas and apart from the logged information processing environment.

10.6 In the entity, there should be documented and implemented procedures for making backup copies. Backup copies should be made regularly and backups should be stored inside of secure areas, which prevents unauthorized access and ensures the physical security of copies. One copy of the backup should be regularly and securely stored in an area geographically separated from the building where backup copies are made. The usability and completeness of backup copies should be controlled regularly. Backup procedures shall include at least the following topics:

- Information to be backed up on a copy;
- Scope and frequency of making backup copies;
- The responsibilities of making backup copies;
- Time for maintaining backup copies;
- Restoration of data from a backup copy.

10.7 The subject of supervision shall have established rules for prescribing what kind of information is exchanged with external parties, what kind of channels are used and how the information is secured. In case risks are realized, it should be possible to implement alternative ways for the transmission of information.

10.8 Confidential information interchange should be secured in the entity if communicated through public channels. When transmitting confidential information over a public network, it should be ensured that the disclosure of data to third parties is precluded. In the case of heightened risk, the encrypting of the transmission of information should be considered. Network security measures should be implemented for access to the network, for services used via the network and for operations performed via the network.

10.9 To detect and prevent malicious software and computer viruses in a timely manner, adequate measures should be implemented and responsibilities designated. Also, it should be ensured that users are immediately notified of the dangers accompanying malicious software and computer viruses when the actual threat to the entity of the spreading of malicious software and viruses has been confirmed by an adequate source of information.

10.10 The subject of supervision shall have established protective measures for portable information technology devices (for example portable computers) and for portable media (for example memory sticks). In the case of increased risk to the data carriers themselves, information technology measures (for example, data encryption) should be implemented in order to protect the data.

11 Access management

11.1 Policies or procedures shall be implemented in the entity to regulate the distribution of access rights to the information systems and these policies or procedures shall encompass all phases of the access lifecycle, including the initial registering of users, changing the access rights of users and permanently removing users, i.e., suspending or stopping the access rights of those users who no longer need information services. Access policies or procedures shall designate all possible access points, including access to the work computers, access to the communications network, access to operating systems, access to applications and databases, mobile and remote access to information assets and access of temporary and external users to the information system. Access rights and other work organisation should be regulated in such a manner that the user of information assets is identified to a sufficient degree by the entity. An employee of the entity and its associated concerns as well as a member of a directing body being the user of information assets shall be identified individually (and not collectively) in connection with every change or deletion of information.

11.2 The subject of supervision shall have established rules for the selection and administration of passwords. The passwords connected with user accounts in the information system should be of a sufficient degree of difficultly that an attempt to acquire them via guessing is excluded to a significant degree.

11.3 The procedure for the administration of passwords shall be co-ordinated with the owners of the information assets in the entity. These rules shall be communicated to all employees who have access to the information assets and the shall include at least information regarding the following – password creation and notification procedure, frequency and conditions for

changing passwords, keeping of passwords, user responsibility and password administration rules for users with special rights.

11.4 Users should be notified regarding their obligation to use passwords in a secure manner. A user whose password has been used to gain access to the information system is responsible for the performance of operations inside of the information system.

11.5 Access to data and information shall be limited to those persons who need it to perform their job. The granting of access rights should be co-ordinated with the owner of the information asset. Issued access rights shall be documented and be based on the wish of the information asset owner.

11.6 The subject of supervision shall establish and implement an access rights control procedure. The conformity of documented and actually issued access rights should be controlled regularly; also, the conformity of user access rights with the actual needs of the user should be assessed regularly. The access rights discovered during control, for which there is no actual user, shall be removed.

11.7 Special attention should be paid to the closing of access rights in case an employee leaves the entity. In case of the loss of confidence in an employee, the access rights to the information systems shall be closed before a formal announcement about termination of the working relationship. In case an employee stays away for an extended period of time, it should be weighed whether to stop the issued access rights for this period of time.

11.8 All users of information assets should be identified and authorized. In accordance with the sensitivity of information assets, a level of user identification and authorization and corresponding rules should be established.

11.9 The use of information systems and services outside of the entity's intranet should be monitored closely. Before opening the service and the granting of corresponding access rights, the identity and authentication of external users should be verified for using specific services and performing corresponding activities. Considering the nature of the service, a dual factor authentication solution should be considered for identifying and authorizing the users.

12 Information systems security

12.1 Security requirements and adequate controls for information systems should be established by the information asset's owners or in co-operation with them. The information asset's owner ensures the integrity and availability of data desired by the financial supervisory authority or an investigative body.

12.2 When developing, supplementing and amending the entity's information systems, it should be ensured that the information systems process information as in the manner prescribed. Input and output controls should contribute to data quality.

12.3 To reduce the likelihood of conflicts with legal acts arising in connection with changes to the information system, taking into consideration the goal of the planned change,, the legality of the performance of amendments should be assured.

12.4 Based on need and the sensitivity of information, above all to ensure confidentiality and integrity, encryption should be used. The entity should establish rules governing the use of encryption, and these rules should prescribe under what cases encryption is mandatory. Also, the cryptographic algorithm used shall be agreed upon, the minimum length of cryptographic keys and administration of cryptographic keys.

12.5 The rules for identifying, testing and applying software updates should be established to avoid problems arising from software defects. The responsibility for the administration of software updates shall be assigned to each separate software system.

12.6 The entity designates and establishes a time period for maintaining information assets, taking into consideration the requirements of legal acts, periods of limitation and the financial supervisory authority's possible interest in information.

12.7 The entity shall ensure that business information (both created and/or processed) will be saved at the first available opportunity to hardware owned or used by the enterprise, if the professional information referring to an employee or member of the managing body of the entity is created or processed in hardware outside of the possession or use of the entity (for example, personal computer, personal outsourced e-mail account, etc), in case the legal act do not require the immediate saving of information.

13 Information security incident management

13.1 In case of security breaches, it should be assured that immediate notification, registration, and incident verification by a competent employee and the implementation of countermeasures takes place.

13.2 In addition to the requirements for incident management, which are covered by the advisory guidelines of the Financial Supervision Authority "Requirements for the organisation of the field of information technology", established on 22.09.2004 with management decision 44-4, section 18 "Problem and incident management", in resolving information security incidents, it should be considered that information collected during the incident is maintained in such a manner that during further investigation it is possible establish what happened and it is possible to ensure that information used for making conclusions is not changed between incident occurrence and incident solution.

13.3 Internal procedures shall ensure that for each detected and reported security incident, a responsible person will be assigned, whose main purpose shall be to co-ordinate incident resolution throughout the course of the incident. Also, the procedures shall include a description of the potential escalation of incidents. Requirements for resolving business continuity incidents according to the business continuity plan are covered by the advisory guidelines of the Financial Supervision Authority "Requirements for Organising the Business Continuity Process of Supervised Entities", established on 06.12.2006 with management decision No 96.

13.4 Information security incidents that have already occurred should be analyzed to determine the reasons, ascertain deficiencies and develop measures to eliminate these deficiencies with the intention of avoiding the occurrence of similar incidents in the future. Also, the analysing of incidents helps to determine what kind of knowledge and skills need to be developed in employees and clients of the client to avoid similar incidents and improve the organisation of incident resolution in the future.

14 Assessment of the need for the auditing of information security and the planning of audits

14.1 In addition to the requirements covered by the advisory guidelines of the Financial Supervision Authority "Requirements for the organisation of the field of information technology", established on 22.09.2004 with management decision 44-4, section 21 "Monitoring and assessment", attention should be paid in the entity to information security

auditing. In planning the entity's information technology and information security activities, efficient assistance for performing supervision activities should be ensured for the financial supervisory authority. In planning internal audits for an entity, the activities in connection with information security should be also considered, among other things.

14.2 Conformity with information security requirements in an entity should be constantly monitored and measured; if necessary, consultation by experts should be used and for assessment compliance with security requirements, an independent control function should be established.

14.3 The need for information security audits should be determined during the risk analysis. As a result of the risk analysis, the most critical areas appear regarding which the conduction of an audit should be considered. The main purpose of an information security audit should be to independently assess whether the entity conforms to internal and external information security requirements.

14.4 When planning an information security audit, the audit function, auditing procedures, audit plan, the particular duties of the auditor and the duties of employees in connection with the audit should be confirmed.

14.5 Upon discovery of the need for an information security audit and the planning of the audit the outsourcing of the IT audit should be weighed in the event of a corresponding lack of skill. In outsourcing auditing services, the outsourcing partner's competences and experiences in organizing similar audits should be assessed and extra attention should be paid to the outsourcing partner's obligations in maintaining and protecting the confidential information recorded during the audit. Specific requirements for outsourcing are covered by the advisory guidelines of the Financial Supervision Authority "Outsourcing Requirements for Supervised Entities", established on 25.10.2006 with management decision No 1.1-7/84.

14.6 Audit findings and observations should be taken into consideration when managing and planning the entity's information security activities. In the event that critical deficiencies are discovered, a follow-up audit should be performed.

14.7 To determine possible weaknesses of critical information systems, penetration testing, as alternative to thorough audits, should be considered. In performing penetration tests, it should be ensured that normal work is not disturbed and information is not corrupted.

15 Implementation

15.1 These guidelines shall enter into force as of 04.05.2010.

15.2 Clauses 16 and 19 of the Financial Supervision Authority's advisory guidelines "Requirements for the organisation of the field of information technology" are changed by the adoption and entry into force of these guidelines.