Unofficial translation

The date for the entry into force of the wording: 25/01/2009

GOVERNMENT OF THE REPUBLIC

REGULATION

The system of security measures for information systems

Adopted on 20/12/2007 No. 252
Entry into force 01/01/2008

This regulation is laid down on the basis of clause 43^9 (1) 4) of the Public Information Act.

Chapter 1
GENERAL PROVISIONS

§ 1. Area of application

(1) This regulation shall lay down the security management system of information systems used for processing data content included in the data stores of the state and local government.

(2) The security management system shall be comprised of the procedure for specifying security requirements and description of the organisational, physical and information technology-related security measures of the data.

(3) This regulation shall not be applied to the securing of information systems which process state secrets.

§ 2. Implementing the security management system

Implementing the security management system means assigning security classes that correspond to the purposes of information security and choosing security measures which correspond to these pursuant to the implementation manual of the three-level IT baseline security system (hereinafter *ISKE*) and implementing these, and auditing the implementation. [RT I 2009, 6, 39 – entry into force 25/01/2009]

§ 3. Definitions

(1) The terms used herein have the following meaning:

1) **security analysis of data** – the assessment of the criticality of data, carried out for the assignment of security class and determination of damages that arise from the lack of data security;
2) **baseline measures** – typical catalogued security measures which are equipped with selection methods; the selection among them depends on the security class and the composition of the information system which is processing the data;

3) **baseline security** – set of measures, the implementation of which is necessary for obtaining and retaining data security;
4) **information system** – technical system processing, storing or transmitting data, along with the means, resources and processes needed for its normal operation;
5) **information security** – the collection of processes for the creation, selection and implementation of security measures;
5^{1}) **information asset** – information and data, and the information technology-related implementations and technical means necessary for processing these; [RT I 2009, 6, 39 – entry into force 25/01/2009]
6) **security measures** – organisational acts and means, technical processes and implementation of technical means for obtaining and retaining the safety of data and data in information systems;
7) **security class** – security level based on the criticality of data, expressed on a four-level scale and with three components, i.e. as a combination of three security subclasses;
8) **security subclass** – level required to obtain the purpose of information security based on the criticality of data, expressed on a four-level scale; three purposes of information security give rise to three security subclasses.

(2) The terms used in the regulation are used within the meaning provided by standard EVS/ISO/IEC 2382 (Information technology – Vocabulary), parts 1–5 of standard EVS ISO/IEC 13335 (Information technology – Guidelines for Information Security Management) and standard EVS ISO/IEC 17799 (Information technology – Security Methods. Code of Practice for Information Security Management).

Chapter 2
SECURITY CLASSES AND SECURITY MEASURES

§ 4. Specification of security measures

(1) In order to assign a security class which considers the purposes of information security, the chief processor of the data store shall organise a security analysis of the data in the data store.

(2) The security class assigned for the data in the data store shall be coordinated with the technical documentation required for the registration of the data store or update of the data in the data store under the procedure provided by the legal act laid down based on § 43^{9} (1) 6) of the Public Information Act. The security measures corresponding to the security class shall be implemented by the time the data store is put into service.

§ 5. Assigning the security class

(1) As a result of the security analysis, the chief processor of a data store shall organise the assignment of security subclasses independent of each other, based on the purposes of information security and the criticality of obtaining these.

(2) The security class shall be assigned for the data processed in the data store. Different types of data of the same data store may have a different security class. The security measures corresponding to the security class are implemented on the information system which processes the data or its part, based on the data that is being processed.

(3) The assignment of the security class shall be based on the information security level of the data which need protection the most.

(4) Letters which refer to the corresponding purposes of information security and level numbers (e.g. K2T3S1) shall be used in the marking of the security class.

§ 6. Security levels

(1) The security level may by high (H), medium (M) or low (L).

(2) The required security level shall be assigned based on the parameters of the integrity, confidentiality and availability of the purposes of information security.

(3) Data integrity means the assurance of data correctness, completeness and being up to date and authenticity of origin, and absence of unauthorised changes.

(4) Data confidentiality means the accessibility of data only by the persons or technical means authorised for this.

(5) Data availability is the timely and easy accessibility of usable data at the previously agreed upon necessary and required working time (i.e. at the necessary and required moment and within the necessary and required time period) by the persons or technical means authorised for this.

§ 7. Security subclasses

(1) Based on the availability of data, the security subclass shall be assigned from the following scale:
1) K0 – reliability – not important; performance – not important;
2) K1 – reliability – 90% (acceptable total interruption per week ~ 24 hours); acceptable increase in the required response time during peak – hours (1÷10);
3) K2 – reliability – 99% (acceptable total interruption per week ~ 2 hours); acceptable increase in the required response time during peak – minutes (1÷10);
4) K3 – reliability – 99.9% (acceptable total interruption per week ~ 10 minutes); acceptable increase in the required response time during peak – seconds (1÷10).

(2) Based on the integrity of data, the security subclass shall be assigned from the following scale:
1) T0 – information source, detectability of amendments or termination is not important; controlling the correctness, integrity and being up to date is not necessary;
2) T1 – information source, the fact of its amendments or termination shall be detectable; controlling the correctness, integrity and being up to date in special cases and according to need;
3) T2 – information source, the fact of its amendments or termination shall be detectable; periodic control of the correctness, integrity and being up to date is required;
4) T3 – information source, the fact of its amendments or termination shall have evidential value; real-time control of the correctness, integrity and being up to date is required.

(3) Based on the confidentiality of data, the security subclass shall be assigned from the following scale:

1) S0 – public information: access to the information is not limited (i.e. all interested persons have read access, permission to change is determined based on the integrity requirement);
2) S1 – information intended for internal use purposes: access to the information shall be granted if the person requesting access has legitimate interest;
3) S2 – classified information: information can only be used by certain user groups; access to the information shall be granted if the person requesting access has legitimate interest;
4) S3 – highly classified information: information can only be used by certain users; access to the information shall be granted if the person requesting access has legitimate interest.

§ 8. Formation of security classes

The data security class marking shall be formed based on the markings of subclasses in their order KTS (e.g. K2T3S1).

§ 9. Choosing security measures corresponding to security classes

(1) In order to ensure the information security purposes of the information system which processes the data in a data store, such security measures shall be applied which correspond to the security class assigned to the data store kept in this information system.

(2) The security measures shall be chosen based on the security class pursuant to the ISKE implementation manual.

(3) The ISKE implementation manual shall be approved by the Minister of Economic Affairs and Communications and the ministry shall publish this on their website.

§ 9[1]. Auditing the implementation of the security management system in the case of state data stores of the state information system

(1) The chief processor of a data store with a data store security level of "H" shall carry out an independent audit of the implementation of the security management system once every two years.

(2) The chief processor of a data store with a data store security level of "M" shall carry out an independent audit of the implementation of the security management system once every three years.

(3) The chief processor of a data store with a data store security level of "L" shall carry out an independent audit of the implementation of the security management system once every four years.

(4) An audit of the implementation of the security management system shall be carried out in that part of the information system where the data of the data store is being processed. The following works shall be performed in the course of the audit:
1) checking whether the performed inventory of information assets corresponds to the requirements;
2) checking the assignment of security classes and security levels;
3) checking the selection of security measures subject to implementation;
4) checking the implementation of all security measures subject to implementation.

(5) When carrying out the audit, the chief processor of a data store shall ensure that, during the time the audit is carried out, the auditor has a valid certificate of a Certified Information Systems Auditor, CISA, issued by the Information Systems Audit and Control Association, an ISO 27001 auditor in charge certificate issued by the British Standards Institute or an ISO 27001 IT certified auditor certificate based on Grundschutz, issued by the information security office in Germany, Bundesamt für Sicherheit in der Informationstechnik.

(6) Upon performing the work, the auditor shall adhere to the Code of Professional Ethics, standards, guidelines, rules of procedure and good practices of the Information Systems Audit and Control Association.

(7) The auditor shall be independent of the auditable. An auditor may not be a person who has consulted the institution in the field that is being audited within two years prior to the audit. The auditor's independence shall be verified by a document signed by the auditor.

(8) The auditor shall keep the information obtained while performing their duties confidential.

(9) Within one month after the audit was carried out, the chief processor of the data store shall send the auditor's assessment to the Ministry of Economic Affairs and Communications via the state information system of information system management. [RT I 2009, 6, 39 – entry into force 25/01/2009]

§ 9^2. Auditing the implementation of the security management system in the case of state data stores of the state information system of a local government

(1) If necessary, the Ministry of Economic Affairs and Communications shall order an audit of the data stores of local governments pursuant to the conditions provided in subsections 9^1 4)–8).

(2) Within one month after the audit was carried out, the chief processor of the data store shall send the auditor's assessment to the Ministry of Economic Affairs and Communications via the state information system of information system management. [RT I 2009, 6, 39 – entry into force 25/01/2009]

Chapter 3
IMPLEMENTING PROVISION

§ 10. Entry into force of the regulation
The regulation shall enter into force on 1 January 2008.

§ 11. Auditing terms for the implementation of the security management system in the case of state data stores of the state information system

(1) The chief processor of a data store with a data store security level of "H" shall carry out an audit of the implementation of the security management system no later than 1 March 2010.

(2) The chief processor of a data store with a data store security level of "M" shall carry out an audit of the implementation of the security management system no later than 1 December 2010.

(3) The chief processor of a data store with a data store security level of “L” shall carry out an audit of the implementation of the security management system no later than 1 March 2011. [RT I 2009, 6, 39 – entry into force 25/01/2009]