System of security measures for information systems

Government of the Republic Regulation No. 252 of 20 December 2007

RT[1.] I, 28.12.2007, 71, 440

Entered into force 01.01.2008

The Regulation is established on the basis of clause 43[9] (1) 4) of the Public Information Act.

Chapter 1
General Provisions

§ 1. Scope of application

(1) The Regulation establishes the system of security measures for information systems used for processing the data contained in state and local government databases and for information assets related therewith.

(2) The system of security measures consists of the procedure for the specification of security measures and the description of organisational, physical and IT security measures to protect data.

(3) This Regulation does not apply to security of information systems processing state secrets.

§ 2. Implementation of system of security measures

The implementation of system of security measures consists in determining the security classes which conform to the objectives of information security and in the selection of appropriate security measures in compliance with the guidelines for the implementation of the three-level baseline security system for information systems (hereinafter ISKE) and in the implementation thereof.

§ 3. Definitions

(1) In this Regulation, the following definitions are used:

1) "security analysis of data" means assessment of the importance of data and damage arising from absence of information security carried out for determining the security class;

2) "baseline security measures" mean standard catalogued security measures supplied with a selection method, the selection of which depends on the security class and the composition of the information system processing the data;

3) "baseline security" means security measures the application of which is necessary for achieving and preserving information security;
4) "information system" means a technical system processing, saving or transmitting data together with the means, resources and processes required for its normal operation;
5) "information security" means a set of processes for the generation, selection and application of security measures;
6) "security measures" mean organisational operations and means, technical processes and application of technical means for the achievement and preservation of data and the security of the data of information systems;
7) "security class" means the required information security level arising from the importance of the data expressed on a four-level scale consisting of three components, i.e. three security sub-classes;
8) "security sub-class" means the required level of the achievement of information security arising from the importance of the data expressed on a four-level scale; three security sub-classes arise from three objectives of information security.
(2) The definitions in this Regulation are used within the meaning of the standard EVS/ISO/IEC 2382 (Information technology. Vocabulary) Parts 1-5 of the standard EVS ISO/IEC 13335 (Information technology. Guidelines for the management of IT Security) and the standard EVS ISO/IEC 17799 (Information technology. Security techniques. Code of practice for information security management.).

Chapter 2
Security classes and security measures

§ 4. Specification of security measures
(1) In order to determine the security class in compliance with the objectives of information security the chief processor of the database shall organise security analysis of the data in the database.
(2) The security class determined for the data in a database together with the technical documentation prepared for the registration of the database or updating data in the database shall be approved pursuant to the procedure provided for in the legislation established on the basis of clause 43^9 (1) 6) of the Public Information Act. The security measures corresponding to the security class shall have implemented by the time of taking a database into use.

§ 5. Determination of security classes

(1) As a result of security analysis the chief processor of a database shall organise determination of security sub-classes independent of each other based on the objectives of information security and the importance of the achievement thereof.

(2) Security classes shall be determined for data processed in a database. Different types of data of one database may have different security classes. The security measures corresponding to the security class shall be applied to an information system processing the data or a part therof based on the processed data.

(3) A security class shall be determined on the basis of the information security level of the data requiring the highest level of protection.

(4) The letters and level numbers indicating the names of the relevant objectives of information security shall be used in the denotation of security classes (e.g. K2T3S1).

§ 6. Security levels

(1) A security level may be high (H), medium (M) or low (L).

(2) The required security level shall be determined in compliance with the objectives of information security through the parameters of integrity, confidentiality and availability.

(3) The integrity of data means the guarantee of the correctness, completeness, up-to-datedness and authenticity of data and absence of unauthorised alterations.

(4) The confidentiality of information means access to the data only for authorised persons or technical means.

(5) The availability of data means timely and easy access to usable data during previously agreed necessary and required business hours (i.e. at the necessary and required moment and within the necessary and required period of time) for authorised persons or technical means.

§ 7. Security sub-classes

(1) On the basis of the availability of data security sub-classes shall be determined from the following scale:

1) K0 – reliability – not important; performance – not important;

2) K1 – reliability – 90% (total permissible outage a week ~ 24 hours); permissible increase of required response time at peak loads – hours (1÷10)

3) K2 – reliability – 99% (total permissible outage a week ~ 2 hours); permissible increase of required response time at peak loads – minutes (1÷10);

4) K3 – reliability – 99.9% (total permissible outage a week~ 10 minutes); permissible increase of required response time at peak loads – seconds (1÷10).

(2) On the basis of the integrity of data security sub-classes shall be determined from the following scale:

1) T0 – the source of information, the detectability of alterations or destruction is not important, verification of the correctness, integrity and up-datedness of information is not necessary;

2) T1 – the source of information, the fact of the alteration and destruction therof shall be detectable, verification of the correctness, integrity and up-datedness of information in special cases and as necessary;

3) T2 – the source of information, the fact of the alteration and destruction therof shall be detectable, periodic verification of the correctness, integrity and up-datedness of information is required;

4) T3 – the source of information, the fact of the alteration and destruction therof shall have evidential value; verification of the correctness, integrity and up-datedness of information in real time is required.

(3) On the basis of the confidentiality of data security sub-classes shall be determined from the following scale:

1) S0 – public information: access to information is not restricted (i.e. all the interested persons have the right to read the data; the right to alter the data is determined by the requirements of integrity);

2) S1 – information for internal use: access to information is permitted provided that the person applying for access has a legitimate interest therein;

3) S2 – confidential information: the use of information is permitted only to certain user groups; access to information is permitted provided that the person applying for access has a legitimate interest therein;

4) S3 – top secret information: the use of information is permitted only to certain users; access to information is permitted provided that the person applying for access has a legitimate interest therein.

§ 8. Formation of security classes

The sign of a data security class is formed from the signs of sub-classes in the order KTS (e.g. K2T3S1).

§ 9. Selection of security measures corresponding to security classes

(1) In order to guarantee the objectives of information security of a database processing data, security measures shall be applied which shall comply with the security class established for the data of the database maintained in this information system.

(2) Security measures shall be selected in compliance with the security class pursuant to ISKE implementation guidelines.

(3) ISKE implementation guidelines shall be approved by the Minister of Economic Affairs and Communications and the Ministry shall publish it on its website.

Chapter 3

Implementing Provision

§ 10. Entry into force of Regulation

This Regulation enters into force on 1 January 2008.

[1] RT = *Riigi Teataja = State Gazette*