Security measures for information systems of vital services and related information assets

Adopted on 14.03.2013 no. 43

This Regulation shall be established on the basis of subsection 40 (2) of the Emergency Act.

§ 1. Scope of application and purpose of regulation

(1) The Regulation regulates the organisation of implementation of security measures for information systems used for providing vital services and the related information assets.

(2) The purpose of the Regulation is to ensure the capacity for consistent operation of information systems used for providing vital services and the possibility to restore them after an interruption.

§ 2. Terms

The following terms are used in this Regulation:

1) critical activity for providing vital services (hereinafter *critical activity*) – an activity whose interruption severely jeopardises the capacity of an institution or enterprise to provide vital services and hinders the achievement of the goals set out by the institution or enterprise upon providing the service;
2) information system used for providing vital services – an information system that affects the operation of critical activities;
3) risk analysis of information system – an analysis in the course of which the possible threats and vulnerabilities must be determined for a critical information system, the likelihood of the threats coming about and the damage related thereto must be assessed and the suitable security measures for mitigating the consequences of the potential threats shall be chosen;
4) security incident with significant impact – an event related to an information system used for providing vital services that results in failure to comply with the operation requirements of vital services or a direct threat for the capacity of compliance with the operation requirements arises. Security incidents with significant impact may, in addition to its own information system, affect the operation of the information systems necessary for providing other vital services;
5) storage media – data media on which data subject to storage is saved;
6) significant dependence on information system – interruption of a critical activity due to a failure in the information system. Industrial automatic control systems with which critical activities are controlled are also information systems with significant dependence.

§ 3. Dependence of critical activity on information system

(1) A provider of vital services shall prepare a risk assessment of continuous operation on the basis of clause 37 (3) 1) of the Emergency Act. The risk assessment of continuous operation shall clarify whether and to what extent the information systems affect the operation of the critical activity.

(2) If the dependence of a critical activity on the information system is significant, the provider of vital service shall implement security measures pursuant to § 4.

(3) If the critical activity is dependent on the information system, but there is an alternative solution to ensure the operation of the critical activity, the provider of vital services shall

specify the substituting measures in the continuous operation plan provided in subsection 39 (1) of the Emergency Act.

(4) If the dependence of a critical activity on the information system is not significant, the provider of vital services shall implement security measures for the information system at the level that ensures the operation of the service.

§ 4. Implementation of security measures on the basis of the information security management system

(1) A provider of vital service shall, considering its principal activities and risks, create an information security management system that it shall implement, monitor, and improve, if required.

(2) Upon implementing the information security management system, a provider of vital service shall adhere to, on a recommended basis:

1) the EVS-ISO/IEC 27001:2006 Standard;
2) the three-level baseline security system ISKE established with Regulation no. 252 "System of security measures for information systems" of the Government of the Republic of 20 December 2007; or
3) the special requirements for information security management established in their field of activity and good practice arising from legislation, international agreements or other agreements that are equal to the standards specified in clauses 1) and 2).

(3) A provider of vital services shall conduct a risk analysis of the information system and, on the basis thereof, choose the security measures required to protect the information system with the objective of ensuring adherence to the operation requirements established by an authority organising continuous operation of vital service.

(4) A provider of vital service shall document the implementation of security measures.

(5) Upon the implementation of security measures, a provider of vital service shall ensure the following:

1) access to a critical information system only for duly authorised persons;
2) secure identification of authorised persons;
3) the existence of an audit trail in order to afterwards determine the time of interruption and other circumstances that are important for carrying out inspection or other investigation;
4) the existence of a report of a security incident with significant impact that *inter alia* includes the course of restoration of the service after the interruption and measures for avoiding interruptions in the future;
5) preservation of a copy of the data required to provide vital services in rooms protected from electromagnetic radiation;
6) preservation of storage media of data required to provide vital services in locations that are sufficiently distanced from each other, taking into consideration the possible threats and the risks arising therefrom.

(6) A provider of vital service shall appoint a person who is responsible for the implementation of security measures and who regularly notifies the management of occurred security incidents and interruptions in operation.

§ 5. Notification of security incidents

A provider of vital services shall appoint a contact person who shall immediately notify the Estonian Information System's Authority of any security incidents with significant impact and, following the resolution of the security incident, submit a respective report.

§ 6. Exchange of information between the Estonian Information System's Authority and institution organising vital services

(1) If the contact person has notified the Estonian Information System's Authority on the basis of § 5, the Estonian Information System's Authority shall communicate the received information to an institution that organises vital services.

(2) If the provider of vital service has notified an institution that organises vital services of a security incident with significant impact, the institution that organises vital services shall communicate the received information to the Estonian Information System's Authority.

§ 7. Right of the Estonian Information System's Authority to provide instructions

The Estonian Information System's Authority may provide recommended instructions to a provider of vital service for better implementation of security measures.

§ 8. Implementing provisions

(1) A provider of vital service shall inform the Estonian Information System's Authority of the contact person appointed on the basis of § 5 by 1 April 2013.

(2) A provider of vital service shall implement the security measures by 1 January 2014.