Publisher: Government of the Republic
Type of Act: Regulation
Type of text: Whole text
Entry into force of the publication: 25.01.2009
End of editing: Currently active
Release note:

Information systems security system

Adopted on 20.12.2007 No 252
RT I 2007, 71, 440
Entry into force 01.01.2008

The Regulation is established on the basis of subsection 43 ^{9} (1) 4) of the Public Information Act .

Chapter 1 GENERAL PROVISIONS

§ 1. Scope

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

(2) The system of security measures consists of a procedure for the specification of security requirements and descriptions of the organizational, physical and informational technical security measures.

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

§ 2. Implementation of security measures system

The implementation of the security measures consists in determining the security classes corresponding to the information security objectives and selecting the security measures corresponding to them, in accordance with the Implementation *Guide for the* Information Systems Three-Step Reference Security System (hereinafter referred to as the *ISKE*) and their implementation and audit implementation.
[RT I 2009, 6, 39 - entered into force. 25.01.2009]

§ 3. Definitions

(1) For the purposes of this Regulation, the following definitions shall apply:
1) " data security analysis" means the assessment of the significance of the security class to determine the security class and the damage assessment resulting from the lack of data security;
2) " reference measures" means standardized security measures with a cataloged and selective method, the choice of which depends on the security class and the composition of the information processing system;
3) " reference security" means a security measure the implementation of which is necessary to achieve and maintain data security;
4) " information system" means a technical system processing, storing or transmitting data, together with the resources, resources and processes necessary for its normal operation;
5) "Information security" means a set of processes for the creation, selection and implementation of security measures;
5 ^{1}) information assets - information, data and information technology applications and technical means necessary for their processing;
[RT I 2009, 6, 39 - entered into force. 25.01.2009]
6) " security measures" means organizational processes and facilities, technical processes and the implementation of technical means for achieving and maintaining the security of data and information systems;
7) " security class" means the required level of data security resulting from the importance of the data, expressed on a four-level scale and as a three-component, that is, a combination of three security classes;
8) Security class - the required level of achievement of the information security objective as a result of the importance of the data, expressed on a four-level scale; Three of the three security objectives are derived from the three security classes.

(2) The term uses the terms of EVS / ISO / IEC 2382 (Information Technology Glossary), EVS ISO / IEC 13335, parts 1-5 (Information Technology, Information Security Management Guidelines) and EVS ISO / IEC 17799 (Information Technology, Security Methods, Information Security Management Code of Practice).

Chapter 2 SECURITY LAMPS AND SECURITY MEASURES

§ 4. Specification of security requirements

(1) In order to determine the security class which takes into account information security objectives, the data controller shall organize a data security analysis of the data file of the database.

(2) Andmekogu andmetele määratud turvaklass kooskõlastatakse koos andmekogu registreerimiseks või andmekogu andmete ajakohastamiseks ettevalmistatava tehnilise dokumentatsiooniga «Avaliku teabe seaduse» § 43^{9} lõike 1 punkti 6 alusel kehtestatud õigusaktis sätestatud korras. Andmekogu kasutusele võtmise ajaks peavad turvaklassile vastavad turvameetmed olema rakendatud.

§ 5. Turvaklassi määramine

(1) Andmekogu vastutav töötleja korraldab andmete turvaanalüüsi tulemusena üksteisest sõltumatute turvaosaklasside määramise infoturbe eesmärkide ja nende saavutamise olulisuse alusel.

(2) Turvaklass määratakse andmekogus töödeldavatele andmetele. Ühe andmekogu erinevatel andmeliikidel võib olla erinev turvaklass. Turvaklassile vastavad turvameetmed rakendatakse andmeid töötlevale infosüsteemile või selle osale töödeldava andmestiku alusel.

(3) Turvaklassi määramisel lähtutakse andmestiku enim kaitset vajavate andmete infoturbe tasemest.

(4) Turvaklassi tähistuses kasutatakse vastavate infoturbe eesmärkide nimetustele viitavaid tähti ja tasemete numbreid (näiteks K2T3S1).

§ 6. Turvatasemed

(1) Turbeaste võib olla kõrge (H), keskmine (M) või madal (L).

(2) Nõutav turvatase määratakse vastavalt infoturbe eesmärkidele tervikluse, konfidentsiaalsuse ja käideldavuse parameetrite kaudu.

(3) Andmete terviklus on andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

(4) Andmete konfidentsiaalsus on andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile.

(5) Andmete käideldavus on eelnevalt kokku lepitud vajalikul ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus (st vajalikul ja nõutaval ajahetkel ja vajaliku ning nõutava aja jooksul) selleks volitatud isikule või tehnilisele vahendile.

§ 7. Turvaosaklassid

(1) Andmete käideldavuse alusel määratakse turvaosaklass järgmisest skaalast:
1) K0 – töökindlus – pole oluline; jõudlus – pole oluline;
2) K1 – töökindlus – 90% (lubatud summaarne seisak nädalas ~ ööpäev); lubatav nõutava reaktsiooniaja kasv tippkoormusel – tunnid (1÷10);
3) K2 – töökindlus – 99% (lubatud summaarne seisak nädalas ~ 2 tundi); lubatav nõutava reaktsiooniaja kasv tippkoormusel – minutid (1÷10);
4) K3 – töökindlus – 99,9% (lubatud summaarne seisak nädalas ~ 10 minutit); lubatav nõutava reaktsiooniaja kasv tippkoormusel – sekundid (1÷10).

(2) Andmete tervikluse alusel määratakse turvaosaklass järgmisest skaalast:
1) T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontroll pole vajalik;
2) T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse ja ajakohasuse kontroll erijuhtudel ja vastavalt vajadusele;
3) T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll;
4) T3 – info allikas, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

(3) Andmete konfidentsiaalsuse alusel määratakse turvaosaklass järgmisest skaalast:
1) S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus on kõigil huvitatutel, muutmise õigus on määratud tervikluse nõuetega);
2) S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
3) S2 – salajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
4) S3 – ülisalajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

§ 8. Turvaklasside moodustamine

Andmete turvaklassi tähis moodustatakse osaklasside tähistest nende järjestuses KTS (näiteks K2T3S1).

§ 9. Turvaklassidele vastavate turvameetmete valimine

(1) Andmekogu andmeid töötleva infosüsteemi infoturbe eesmärkide tagamiseks peab rakendama turvameetmeid, mis vastavad selles infosüsteemis peetava andmekogu andmetele määratud turvaklassile.

(2) Turvameetmed valitakse vastavalt turvaklassile ISKE rakendamisjuhendi kohaselt.

(3) ISKE rakendamisjuhendi kinnitab majandus- ja kommunikatsiooniminister ning ministeerium avaldab selle oma veebilehel.

§ 9[1]. Turvameetmete süsteemi rakendamise auditeerimine riigi infosüsteemi kuuluvate riigi andmekogude pidamisel

(1) Andmekogu vastutav töötleja, kelle andmekogu turbeaste on «H», peab turvameetmete süsteemi rakendamise kohta läbi viima sõltumatu auditi iga kahe aasta järel.

(2) Andmekogu vastutav töötleja, kelle andmekogu turbeaste on «M», peab turvameetmete süsteemi rakendamise kohta läbi viima sõltumatu auditi iga kolme aasta järel.

(3) Andmekogu vastutav töötleja, kelle andmekogu turbeaste on «L», peab turvameetmete süsteemi rakendamise kohta läbi viima sõltumatu auditi iga nelja aasta järel.

(4) Turvameetmete süsteemi rakendamise auditeerimine viiakse läbi infosüsteemi osas, kus andmekogu andmeid töödeldakse. Auditeerimise käigus tuleb teha järgmised tööd:
1) kontrollida teostatud infovarade inventuuri vastavust nõuetele;

2) kontrollida turvaklasside ja turbeastmete määramist;
3) kontrollida rakendamisele kuuluvate turvameetmete valimist;
4) kontrollida kõigi rakendamisele kuuluvate turvameetmete rakendamist.

(5) Andmekogu vastutav töötleja peab auditeerimise läbiviimisel veenduma, et audiitor omaks auditi läbiviimise ajal kehtivat Rahvusvahelist Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (*Information Systems Audit and Control Association*) väljaantud infosüsteemide sertifitseeritud audiitori (*Certified Information Systems Auditor, CISA*) sertifikaati, Briti Standardi Instituudi (*British Standards Institute*) väljaantud ISO 27001 juhtiva audiitori sertifikaati või Saksa Infoturbeagentuuri (*Bundesamt für Sicherheit in der Informationstechnik*) väljaantud ISO 27001 IT *Grundschutzi* baasil sertifitseeritud audiitori sertifikaati.

(6) Audiitor järgib tööde tegemisel Rahvusvahelise Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni kutse-eetika koodeksit, standardeid, suuniseid, protseduurireegleid ja häid tavasid.

(7) Audiitor peab olema auditeeritavast sõltumatu. Audiitoriks ei tohi olla isik, kes on auditeerimisele eelnenud kahe aasta jooksul asutust konsulteerinud auditeeritavas valdkonnas. Audiitori sõltumatus peab olema kinnitatud audiitori poolt allkirjastatud dokumendiga.

(8) Audiitor peab säilitama oma kohustuste täitmise käigus omandatud informatsiooni konfidentsiaalsuse.

(9) Ühe kuu jooksul pärast auditi teostamist edastab andmekogu vastutav töötleja riigi infosüsteemi halduse infosüsteemi kaudu Majandus- ja Kommunikatsiooniministeeriumile audiitori hinnangu.
[RT I 2009, 6, 39 - jõust. 25.01.2009]

§ 9^2. Turvameetmete süsteemi rakendamise auditeerimine kohaliku omavalitsuse riigi infosüsteemi kuuluvate andmekogude pidamisel

(1) Kohalike omavalitsuste andmekogude auditi tellib Majandus- ja Kommunikatsiooniministeerium arvestades § 9^1 lõigetes 4–8 sätestatud tingimusi ja nõudeid ning lähtuvalt vajadusest.

(2) Ühe kuu jooksul pärast auditi teostamist edastab andmekogu vastutav töötleja riigi infosüsteemi halduse infosüsteemi kaudu Majandus- ja Kommunikatsiooniministeeriumile audiitori hinnangu.
[RT I 2009, 6, 39 - jõust. 25.01.2009]

3. peatükk
RAKENDUSSÄTE

§ 10. Määruse jõustumine

Määrus jõustub 1. jaanuaril 2008. a.

§ 11. Turvameetmete süsteemi rakendamise auditeerimise tähtajad riigi infosüsteemi kuuluvate riigi andmekogude pidamisel

(1) Andmekogu vastutav töötleja, kelle andmekogu kuulub turbeastmesse «H», on kohustatud esmakordse turvameetmete süsteemi rakendamise auditeerimise läbi viima hiljemalt 1. märtsiks 2010. a.

(2) Andmekogu vastutav töötleja, kelle andmekogu kuulub turbeastmesse «M», on kohustatud esmakordse turvameetmete süsteemi rakendamise auditeerimise läbi viima hiljemalt 1. detsembriks 2010. a.

(3) Andmekogu vastutav töötleja, kelle andmekogu kuulub turbeastmesse «L», on kohustatud esmakordse turvameetmete süsteemi rakendamise auditeerimise läbi viima hiljemalt 1. märtsiks 2011. a.
[RT I 2009, 6, 39 - jõust. 25.01.2009]