Väljaandja:	Vabariigi Valitsus
Akti liik:	määrus
Teksti liik:	terviktekst
Redaktsiooni jõustumise kp:	18.09.2020
Redaktsiooni kehtivuse lõpp:	Hetkel kehtiv
Avaldamismärge:	RT I, 15.09.2020, 15

Infosüsteemide turvameetmete süsteem

Vastu võetud 20.12.2007 nr 252
RT I 2007, 71, 440
jõustumine 01.01.2008

Muudetud järgmiste aktidega

Vastuvõtmine	Avaldamine	Jõustumine
08.01.2009	RT I 2009, 6, 39	25.01.2009
10.09.2020	RT I, 15.09.2020, 12	18.09.2020

Määrus kehtestatakse «Avaliku teabe seaduse» § 43^9 lõike 1 punkti 4 alusel.

1. peatükk
ÜLDSÄTTED

§ 1. Reguleerimisala

(1) Määrusega kehtestatakse riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteem.

(2) Turvameetmete süsteem koosneb turvanõuete spetsifitseerimise korrast ning andmete organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete kirjeldustest.

(3) Määrust ei kohaldata riigisaladust töötlevate infosüsteemide turbeks.

§ 2. Turvameetmete süsteemi rakendamine

(1) Turvameetmete süsteemi rakendamine seisneb infoturbe eesmärkidele vastavate turvaklasside määramises ja nendele vastavate turvameetmete valimises vastavalt infosüsteemide kolmeastmelise etalonturbe süsteemi (edaspidi *ISKE*) rakendamisjuhendile ja nende rakendamises ning rakendamise auditeerimises.
[RT I 2009, 6, 39- jõust. 25.01.2009]

(2) Andmekogu turvalisuse tagamiseks rakendatud meetmete vastavust määruses sätestatud nõuetele eeldatakse juhul, kui on täidetud kõik järgmised tingimused:
1) vastutav töötleja on täitnud §-dest 4–8 tulenevad kohustused;
2) andmekogu turvalisuse tagamiseks rakendatud meetmed vastavad rahvusvahelise standardiga ISO/IEC 27001 kehtestatud nõuetele;
3) andmekogu vastutav töötleja on punktis 2 nimetatud nõuetekohasuse kinnitamiseks esitanud Riigi Infosüsteemi Ametile kehtiva vastavussertifikaadi.
[RT I, 15.09.2020, 12- jõust. 18.09.2020]

§ 3. Mõisted

(1) Määruses kasutatakse mõisteid järgmises tähenduses:
1) andmete turvaanalüüs – turvaklassi määramiseks sooritatav andmete tähtsuse hindamine ning andmete turvalisuse puudumisest tulenev kahjude hindamine;
2) etalonmeetmed – tüüpsed katalogiseeritud ja valimismetoodikaga varustatud turvameetmed, mille hulgast tehtav valik sõltub turvaklassist ja andmeid töötleva infosüsteemi koostisest;
3) etalonturve – turvameetmestik, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks;

4) infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega;
5) infoturve – turvameetmete loomise, valimise ja rakendamise protsesside kogum;
5[1]) infovara – informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid;
[RT I 2009, 6, 39- jõust. 25.01.2009]
6) turvameetmed – organisatsioonilised toimingud ja vahendid, tehnilised protsessid ja tehniliste vahendite rakendamine andmete ja infosüsteemide andmete turvalisuse saavutamiseks ja säilitamiseks;
7) turvaklass – andmete tähtsusest tulenev nõutav andmete turvalisuse tase väljendatuna neljaastmelisel skaalal ning kolmekomponendilisena, st kolme turvaosaklassi ühendina;
8) turvaosaklass – andmete tähtsusest tulenev infoturbe eesmärgi saavutamise nõutav tase väljendatuna neljaastmelisel skaalal; kolmest infoturbe eesmärgist tuleneb kolm turvaosaklassi.

(2) Määruses kasutatakse termineid standardiga EVS/ISO/IEC 2382 (Infotehnoloogia. Sõnastik), standardi EVS ISO/IEC 13335 osadega 1–5 (Infotehnoloogia. Infoturbe halduse suunised) ning standardiga EVS ISO/IEC 17799 (Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis) määratud tähenduses.

2. peatükk
TURVAKLASSID JA TURVAMEETMED

§ 4. Turvanõuete spetsifitseerimine

(1) Infoturbe eesmärke arvestava turvaklassi määramiseks korraldab andmekogu vastutav töötleja andmekogu andmete turvaanalüüsi.

(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.
[RT I, 15.09.2020, 12- jõust. 18.09.2020]

§ 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]