

Väljaandja:
Akti liik:
Teksti liik:
Redaktsiooni jõustumise kp:
Redaktsiooni kehtivuse lõpp:
Avaldamismärge:

Vabariigi Valitsus
määrus
terviktekst
01.07.2024
30.09.2025
RT I, 19.06.2024, 12

Võrgu- ja infosüsteemide küberturvalisuse nõuded

Vastu võetud 09.12.2022 nr 121
[RT I, 13.12.2022, 30](#)
jõustumine 16.12.2022

Muudetud järgmiste aktidega

Vastuvõtmine
13.06.2024

Avaldamine
[RT I, 19.06.2024, 6](#)

Jõustumine
01.07.2024

Määrus kehtestatakse [küberturvalisuse seaduse](#) § 7 lõike 5 alusel.

1. peatükk Üldsätted

§ 1. Kohaldamisala

Määrusega volitatakse üleriigilise küberturvalisuse tagamise korraldamise eest vastutavat ministrit kehtestama Eesti infoturbestandardi ja kehtestatakse vastavalt küberturvalisuse seaduse §-le 7:

- turvameetmete üldnõuded;
- võrgu- ja infosüsteemide (edaspidi *süsteem*) turvameetmete erinõuded ja nende kohaldamise ulatus.
[[RT I, 19.06.2024, 6](#)- jõust. 01.07.2024]

§ 2. Terminid

Määruses kasutatakse termineid järgmises tähenduses:

- andmekogu on andmekogu avaliku teabe seaduse § 43¹ lõike 1 tähenduses;
- infoturve on süsteemile turvameetmete loomise, valimise ja rakendamise protsesside kogum.

2. peatükk Eesti infoturbestandard

§ 3. Eesti infoturbestandardi kehtestamise volitus

(1) Eesti infoturbestandardi kehtestab [üleriigilise küberturvalisuse tagamise korraldamise eest vastutav minister](#) määrusega.

(2) Teenuse osutajale ei kohaldata lõike 1 alusel kehtestatud nõudeid, kui on täidetud kõik järgmised tingimused:

- teenuse osutaja rakendatud turvameetmed vastavad rahvusvahelise standardiga ISO/IEC 27001 kehtestatud nõuetele;
- teenuse osutaja on esitanud Riigi Infosüsteemi Ametile kehtiva vastavussertifikaadi, mis kinnitab punktis 1 sätestatud tingimuse täitmist.

(3) Julgeolekuasutusele ei kohaldata lõike 1 alusel kehtestatud nõudeid, kui ta täidab lõike 2 punktis 1 sätestatud tingimuse ja esitab lõike 2 punktis 2 nimetatud vastavussertifikaadi küberturvalisuse seaduse § 14 lõikes 5 nimetatud haldusjärelevalve teostajale.

§ 4. Eesti infoturbestandardi järgimise auditeerimine

- (1) Teenuse osutaja tagab Eesti infoturbestandardi tingimuste täitmise auditi läbi viimise iga kolme aasta järel.
- (2) Teenuse osutaja edastab lõike 1 alusel läbi viidud auditi järeldusotsuse Riigi Infosüsteemi Ametile 30 päeva jooksul selle kättesaamisest.
- (3) Julgeolekuasutus edastab lõike 1 alusel läbi viidud auditi järeldusotsuse küberturvalisuse seaduse § 14 lõikes 5 nimetatud haldusjärelevalve teostajale 30 päeva jooksul selle kättesaamisest.
- (4) Lõikes 1 sätestatud ei kohaldata:
 - 1) teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 10 töötaja ja kelle aasta bilansimaht või aastakäive ei ületa 2 miljonit eurot, arvestades mikroettevõtjate määratlusi Euroopa Komisjoni soovitusel 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.05.2003, lk 36–41);
 - 2) riigimuuseumile, avalik-õigusliku isiku muuseumile, valla või linna ametiasutusele, valla või linna ametiasutuse hallatavale asutusele, osavalla või linnaosa ametiasutusele, osavalla või linnaosa ametiasutuse hallatavale asutusele ning kohaliku omavalitsuse üksuste ühisametile ja -asutusele, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga;
 - 3) teenuse osutajale, kes on täitnud § 3 lõikes 2 või 3 sätestatud tingimused.

3. peatükk Turvameetmete nõuded

1. jagu Turvameetmete üldnõuded

§ 5. Turvameetmete dokumentatsioon

- (1) Teenuse osutaja kaardistab süsteemid ja nendega seotud teenused või protsessid ning dokumenteerib süsteemile rakendatavad turvameetmed ja riskianalüüsi.
- (2) Teenuse osutaja säilitab lõikes 1 nimetatud dokumentatsiooni vähemalt seitse aastat alates selle koostamisest ning teeb selle Riigi Infosüsteemi Ametile taotluse korral kättesaadavaks.
- (3) Julgeolekuasutus säilitab lõikes 1 nimetatud dokumentatsiooni vähemalt seitse aastat alates selle koostamisest ning teeb selle küberturvalisuse seaduse § 14 lõikes 5 nimetatud haldusjärelevalve teostajale taotluse korral kättesaadavaks.
- (4) Teenuse osutaja võib lõikes 1 nimetatud dokumentatsiooni koostada muu õigusakti alusel koostatava dokumendi osana.

§ 6. Riskianalüüsi ajakohastamine

- Teenuse osutaja ajakohastab riskianalüüsi:
- 1) viivitamata pärast olulise mõjuga küberintsidendi toimumist;
 - 2) viivitamata pärast teenuse osutamiseks kasutatava süsteemi sellist muutust, mis mõjutab süsteemi turvalisust, või
 - 3) hiljemalt kolme aasta möödumisel viimasest ajakohastamisest.

2. jagu Turvameetmete erinõuded

1. jaotis Andmekogu

§ 7. Turvameetmete nõuete erisused andmekogu pidamisel

- (1) Andmekogu vastutav töötaja korraldab andmekogu turbeastme ja andmete turvaklassi määramise, andmekogu andmete turvaklassi määramiseks andmete tähtsuse hindamise ning andmete turvalisuse puudumisest tuleneva kahjude hindamise.
- (2) Andmekogu andmetele määratud turvaklass ja andmekogu turbeaste kooskõlastatakse koos andmekogu registreerimiseks või andmekogu andmete ajakohastamiseks ettevalmistatava tehnilise dokumentatsiooniga avaliku teabe seaduse § 43⁹ lõike 1 punkti 6 alusel kehtestatud õigusaktis sätestatud korras.

(3) Andmekogu vastutav töötleja ja andmekogu majutav volitatud töötleja rakendab turvameetmed andmekogu kasutusele võtmise ajaks.

(4) Andmekogu vastutav töötleja ja andmekogu majutav volitatud töötleja rakendab andmekogu pidamisega seotud süsteemide turvameetmeid andmekogu turbeastmest lähtuvalt.
[RT I, 13.12.2022, 30- jõust. 01.01.2023]

§ 8. Andmekogu turbeastme määramine

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

(2) Andmekogu turbeaste määratakse lähtuvalt andmete turvaklassist. Kui andmete turvaklassi vähemalt üks osaklass vastab tasemele 3, on andmekogu turbeaste kõrge (H). Kui andmete turvaklassi vähemalt üks osaklass vastab tasemele 2, on andmekogu turbeaste vähemalt keskmine (M). Muul juhul on andmekogu turbeaste vähemalt madal (L).
[RT I, 13.12.2022, 30- jõust. 01.01.2023]

§ 9. Andmete turvaklassi määramine

(1) Andmete turvaklassi määrab vastutav töötleja vastavalt infoturbe eesmärkidele tervikluse, konfidentsiaalsuse ja käideldavuse parameetrite kaudu.

(2) Andmete käideldavus on vajalikul ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ning hõlbus kättesaadavus selleks volitatud isikule või tehnilisele vahendile.

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

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

(5) Andmete turvaklass on kombinatsioon andmete käideldavuse (K), tervikluse (T) ja konfidentsiaalsuse (S) turvaosaklasside tasemetest. Andmete turvaklassi tähis moodustatakse osaklasside tähistest nende järjestuses KTS (näiteks K2T3S1).
[RT I, 13.12.2022, 30- jõust. 01.01.2023]

§ 10. Andmete turvaosaklasside määramine

(1) Andmete turvaosaklass on andmete tähtsusest tulenev infoturbe eesmärgi saavutamise nõutav tase.

(2) Andmekogu vastutav töötleja määrab andmete käideldavuse, tervikluse ja konfidentsiaalsuse turvaosaklasside tasemed vastavalt käesolevas paragrahvis sätestatud skaalale.

(3) Turvaosaklasside taseme määramisel lähtub andmekogu vastutav töötleja järgnevast:

- 1) andmetega seotud nõuded tulenevalt õigusaktidest ja lepingulistest kohustustest;
- 2) andmetega seotud nõuded tulenevalt pakutavate teenuste iseloomust;
- 3) küberintsidentidest tekkivate kahjude olulisus.

(4) 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 reaktsioonijaaja kasv tippkoormusel – tunnid (1÷10);
- 3) K2 – töökindlus – 99% (lubatud summaarne seisak nädalas ~ 2 tundi), lubatav nõutava reaktsioonijaaja kasv tippkoormusel – minutid (1÷10);
- 4) K3 – töökindlus – 99,9% (lubatud summaarne seisak nädalas ~ 10 minutit), lubatav nõutava reaktsioonijaaja kasv tippkoormusel – sekundid (1÷10).

(5) Andmete tervikluse alusel määratakse turvaosaklass järgmisest skaalast:

- 1) T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised ja info õigsuse, täielikkuse ning ajakohasuse kontroll pole vajalik;
- 2) T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad ning info õigsuse, täielikkuse ja ajakohasuse kontroll erijuhtudel ning vastavalt vajadusele;
- 3) T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad ning vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll;
- 4) T3 – info allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärne ning vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

(6) Andmete konfidentsiaalsuse alusel määratakse turvaosaklass järgmisest skaalast:

- 1) S0 – avalik info, juurdepääsu teabele ei piirata, lugemisõigus on kõigil huvitatutel ja muutmise õigus on määratud tervikluse nõuetega;
- 2) S1 – info asutusesiseseks kasutamiseks ja juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmismajaduse korral;
- 3) S2 – info asutusesiseseks kasutamiseks, info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele ja juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmismajaduse korral;
- 4) S3 – info asutusesiseseks kasutamiseks, info kasutamine on lubatud ainult teatud kindlatele kasutajatele ja juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmismajaduse korral.

(7) Turvaosaklassi määramisel lähtutakse andmestiku enim kaitset vajavate andmete infoturbe tasemest.
[RT I, 13.12.2022, 30- jõust. 01.01.2023]

§ 11. Turvameetmete rakendamine andmekogu turbeastmest lähtuvalt

(1) Paragrahvi 7 lõikes 4 sätestatud kohustuse täitmiseks peab andmekogu vastutav töötaja ja andmekogu majutav volitatud töötaja lähtuma kaitsealast, mis hõlmab vähemalt kõiki andmekogu pidamisega seotud süsteeme, määrama kõikidele andmekogu pidamisega seotud süsteemidele ja teenustele vähemalt andmekogu turbeastmele vastava kaitsetarve ning rakendama asjakohast turbeviisi.

(2) Turbeastmele kõrge (H) vastav Eesti infoturbestandardi kaitsetarve on väga suur (VS), turbeastmele keskmine (M) vastav Eesti infoturbestandardi kaitsetarve on suur (S) ja turbeastmele madal (L) vastav Eesti infoturbestandardi kaitsetarve on normaalne (N).

(3) Paragrahvi 7 lõikes 4 sätestatud kohustus loetakse täidetuks, kui andmekogu vastutav töötaja ja andmekogu majutav volitatud töötaja on täitnud § 3 lõikes 2 või 3 sätestatud tingimused.
[RT I, 13.12.2022, 30- jõust. 01.01.2023]

2. jaotis Avalike ülesannete täitmist oluliselt mõjutavad süsteemid

§ 12. Avalike ülesannete täitmist oluliselt mõjutavate süsteemide loetelu

Loetelu süsteemidest, millel on oluline mõju riigi ja kohaliku omavalitsuse üksuse võimele täita avalikke ülesandeid, kehtestab [valdkonna eest vastutav minister](#).
[RT I, 19.06.2024, 6- jõust. 01.07.2024]

§ 13. Avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamise nõuded

Paragrahvi 12 alusel kehtestatud loetelus nimetatud süsteemide tarkvara lähtekood, andmed ja taastejuhendid varundatakse keskselt välisriigiga sõlmitud rahvusvahelise lepingu alusel regulaarselt välisriigis asuvasse turvalisse andmekeskusesse.
[RT I, 19.06.2024, 6- jõust. 01.07.2024]

4. peatükk Rakendussätted

§ 14. Üleminek Eesti infoturbestandardile

(1) Kui teenuse osutaja haldab riigi või kohaliku omavalitsuse üksuse süsteemi, eeldatakse süsteemi turvalisuse tagamiseks rakendatud meetmete vastavust Eesti infoturbestandardile kuni 31. detsembrini 2022. a, kui teenuse osutaja kohaldab nimetatud süsteemi turvalisuse tagamisele avaliku teabe seaduse § 43⁹lõike 1 punkti 4 alusel kehtestatud määruises sätestatud nõudeid.

(2) Kui teenuse osutaja ei halda riigi või kohaliku omavalitsuse üksuse süsteemi, eeldatakse süsteemi turvalisuse tagamiseks rakendatud meetmete vastavust Eesti infoturbestandardile kuni 30. juunini 2023. a, kui teenuse osutaja rakendab, seirab ja ajakohastab turvameetmeid, millega nähakse ette vähemalt:

- 1) süsteemide juurdepääsuõiguste haldamine, süsteemi kasutajate identifitseerimine ja autoriseerimine;
- 2) teenuse osutamiseks vajalikest andmetest regulaarsete varukoopiate tegemine ja protseduurid andmete varukoopiatest taastamiseks;
- 3) süsteeme käitava ja süsteemides käideldava tarkvara ajakohasus;
- 4) süsteemides tehtavate toimingute logid toimingu tegija, liigi ja tegemise ajaga;
- 5) tarkvaralised ja riistvaralised lahendused süsteemide turvalisust ohustava tegevuse ning tarkvara tuvastamiseks ja tõrjumiseks;
- 6) protseduurid süsteemide turvalisuse või teenuse toimepidevuse taastamiseks.

§ 15. Eesti infoturbestandardi järgimise auditeerimise tähtajad

(1) Teenuse osutaja, kes on või oli 31. detsembri 2022. a seisuga Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem” § 9¹lõike 1 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditi, on kohustatud esmakordse Eesti infoturbestandardi järgimise auditi läbi viima kahe aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem” § 9¹lõike 1 alusel läbi viidud turvameetmete süsteemi auditit.

(2) Teenuse osutaja, kes on või oli 31. detsembri 2022. a seisuga Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem” § 9¹lõike 2 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditi, on kohustatud esmakordse Eesti infoturbestandardi järgimise auditi läbi viima kolme aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem” § 9¹lõike 2 alusel läbi viidud turvameetmete süsteemi auditit, kuid hiljemalt kolm aastat pärast käesoleva määruse jõustumist.

(3) Teenuse osutaja, kes on või oli 31. detsembri 2022. a seisuga Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem” § 9¹lõike 3 alusel kohustatud läbi viima turvameetmete süsteemi rakendamise auditi, on kohustatud esmakordse Eesti infoturbestandardi järgimise auditi läbi viima nelja aasta jooksul pärast viimast Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem” § 9¹lõike 3 alusel läbi viidud turvameetmete süsteemi auditit, kuid hiljemalt kolm aastat pärast käesoleva määruse jõustumist.

(4) Lõigetes 1–3 nimetamata teenuse osutaja on kohustatud esmakordse Eesti infoturbestandardi järgimise auditi läbi viima kolme aasta jooksul alates Eesti infoturbestandardi järgimise auditeerimise kohustuse tekkimisest.

§ 16. Määruse jõustumine

Käesoleva määruse §-d 7–11 jõustuvad 1. jaanuaril 2023. a.