

JUSTIITS- JA DIGIMINISTER  
MÄÄRUS

**Eesti infoturbestandard**

Määrus kehtestatakse küberturvalisuse seaduse § 7 lõike 5 ning Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded” § 3 lõike 1 alusel.

**1. peatükk**  
**Üldsätted**

**§ 1. Määruse reguleerimisala ja eesmärk**

(1) Eesti infoturbestandardi rakendamine seisneb võrgu- ja infosüsteemi infoturbe halduses ja infoturbe halduse meetmete auditeerimises.

(2) Teenuseosutajate Eesti infoturbestandardi rakendamise kohustus ja ulatus on sätestatud Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded” 2. peatükis.

(3) Eesti infoturbestandardi kehtestamise eesmärk on:

- 1) tagada avalike ning ühiskonna toimimiseks vajalike, sealhulgas oluliste ja kriitiliste ülesannete täitmiseks kasutatavate võrgu- ja infosüsteemide kõikehõlmav kaitse ning saavutada infoturbe ühtlane tase kõigis nende osades kogu elutsükli jooksul;
- 2) luua süsteemne raamistik, mis aitab teenuseosutajal kaitsta oma äriprotsesse, varasid, võrgu- ja infosüsteemi ning ennetada ohte ja hallata riske.

**§ 2. Terminid**

(1) Määruses kasutatakse järgmisi termineid:

- 1) **infoturbe halduse süsteem** – riskide hindamisel, käsitlemisel ja aktsepteerimisel põhinev teenuseosutaja süsteemse kaitsmise ning infoturbe rajamise, teostamise, seire, läbivaatamise ja täiustamise süstemaatilise käsitlemise viis;
- 2) **infoturvameetmete rakendamise plaan** – organisatsioonikeskne struktureeritud ühest või mitmest dokumendist koosnev juhend turvameetmete haldamiseks;
- 3) **organisatsioon** – teenuseosutaja küberturvalisuse seaduse tähenduses;
- 4) **äriprotsess** – organisatsiooni tegevuse osa, mingi eesmärgi saavutamiseks rakendatavate inimeste, aja, finants- ja töövahendite (edaspidi koos *ressursid*), tegevuste, toimingute või protseduuride kogum, mille tulemusel valmib toode või teenus (inglise keeles *business process*).

## **2. peatükk**

### **Infoturbe haldus**

#### **§ 3. Infoturbe halduse süsteem**

(1) Infoturbe halduse süsteemi raames vaadatakse organisatsiooni:

- 1) tegevusvaldkonda, eesmärgi, protsesse, protseduure ja tavasid;
- 2) õigusaktidest ning lepingutest tulenevaid õigusi ja kohustusi;
- 3) keskkonda, ressursse ja vara.

(2) Infoturbe halduse süsteemi toimimiseks tuleb määrata järgmised rollid:

- 1) hankejuht – jälgib, et turvameetmed on vara kogu elutsükli ulatuses plaanitud uue vara ja teenuste hankimise etappi juba selle kavandamise käigus;
- 2) infoturbejuht – koordineerib ja nõustab turvameetmete rakendamist, sealhulgas koolituste formaadi valimist;
- 3) kasutaja – järgib tema kasutusse antud vara kasutamise korda, läbib regulaarselt infoturbekoolitusi, reageerib intsidentidele kokkulepete kohaselt, sealhulgas teavitab küberintsidentidest;
- 4) äriüksuse juht – korraldab vara kaardistuse, kaitsetarbe määramise ja vajalike meetmete rakendamise regulaarse seire.

(3) Taasesitatavas vormis säilitatakse järgmist teavet:

- 1) infoturbe halduse süsteemi alusdokumendid ja otsuste kulg;
- 2) infoturvasündmused ja organisatsiooni reaktsioon neile;
- 3) infoturvameetmete rakendamise plaan ja selles sisalduvad riski käsitlemise viisid.

#### **§ 4. Organisatsiooni juhatuse tegevus**

(1) Infoturbe halduse süsteemi toimimist korraldab organisatsiooni juhatus.

(2) Infoturbe halduse süsteemi toimimiseks juhatus:

- 1) määrab organisatsiooni sees rollid ja vastutajad, määramata rollide eest vastutab juhatus ise;
- 2) eraldab vajalikud ressursid;
- 3) määrab kindlaks infoturbe eesmärgid, kehtestades infoturvapoliitika;
- 4) otsustab infoturvameetmete rakendamise plaanis kavandatud meetmete rakendamata jätmisest tulenevate riskide aktsepteerimise üle, arvestades võimalikku mõju äriprotsessile.

(3) Infoturbe halduse süsteemi korraldus peab võimaldama juhatusel saada regulaarseid ja operatiivseid ülevaateid:

- 1) riskidest ning nende võimalikust mõjust ja kulust;
- 2) toimunud küberintsidentide mõjust äriprotsessidele;
- 3) õigusaktides ja lepingutes sätestatud nõuetest ja nende muudatustest;
- 4) infoturbe hetkeseisust ja infoturvameetmete rakendamise plaani täitmisest.

#### **§ 5. Infoturvapoliitika**

(1) Infoturvapoliitikas nähakse ette vähemalt:

- 1) turbe üldised eesmärgid ja põhimõtted, sealhulgas riskihalduse alused;
- 2) rollide ja vastutusalade jaotus;

- 3) küberintsidentide käsitlemise ja infoturbe halduse süsteemi hindamise alused;
- 4) viited seotud dokumentidele, sealhulgas näiteks alampoliitikad, korrad, tegevuse dokumentatsioon.

(2) Infoturvapoliitika vaadatakse üle ja vajaduse korral muudetakse vähemalt kord kalendriaastas.

## **§ 6. Riskihaldusmetoodika**

(1) Riskihaldusmetoodika kasutuselevõtmise eeldus on organisatsiooni varade arvelevõtmine ja nende kaitseala kindlaksmääramine.

(2) Organisatsioon peab kehtestama riskihaldusmetoodika, mis on seotud organisatsiooni üldise riskihaldusega ja koosneb vähemalt järgmisest:

- 1) äriprotsessidele mõju avaldavate ohtude tuvastamine, arvestades konfidentsiaalsust, terviklust ja käideldavust;
- 2) vara ja äriprotsessi vastendamine infoturbekataloogi moodulitega;
- 3) infoturvameetmete rakendamise plaani täitmise otsused, sealhulgas riskide hindamine.

## **§ 7. Infoturbekataloog**

(1) Määruse lisas 1 sätestatud infoturbekataloog on organisatsiooni kahjustada võivate ohtude kaitseks võetavate meetmete loend.

(2) Lõikes 1 nimetatud meetmed jaotatakse protsessi- ja süsteemimoodulitesse.

## **§ 8. Infoturvameetmete rakendamise plaan**

(1) Infoturvameetmete rakendamise plaanis esitatakse asjakohased infoturbekataloogiga seotud meetmed. Riskihalduse põhjal lisatakse kõnealusesse rakendusplaani vajaduse korral lisameetmeid.

(2) Infoturbekataloogi süsteemimoodulite meetmeid rakendatakse kõigile kaitseala varadele kooskõlas infoturvameetmete rakendamise plaaniga.

(3) Infoturbekataloogi protsessimoodulite meetmed lõimitakse igapäevasesse töökorraldusse.

(4) Infoturbekataloogi meetmete rakendamise prioriteetide ja tähtaegade määramisel lähtutakse kaitsetarbest, varade omavahelisest sõltuvusest ja vara elutsükli etapist.

(5) Infoturvameetmete rakendamise plaanis võib ette näha infoturbekataloogi mooduli meetme asendamise muu samaväärse meetmega või meetme rakendamata jätmise, kui:

- 1) tagatakse vajalik infoturve;
- 2) organisatsioon on riski aktsepteerinud.

(6) Meetme rakendamise tähtaeg ja tegevuste regulaarsus peab tagama infoturvameetmete rakendamise plaani täitmise mõistliku aja jooksul. Kui meetme rakendamise tähtaeg ületab ühte aastat, tuleb seda käsitleda regulaarses riskihalduses kui aktsepteeritud riski.

(7) Kui äriprotsess sõltub organisatsioonivälisest tarneahelast, hinnatakse sellega kaasnevaid riske.

(8) Organisatsioonivälise tarneahela kaitse vajaduse hindamiseks on organisatsioonil õigus nõuda väliselt osapoolelt kaitsetarbele vastavate turvameetmete rakendamist, sealhulgas seirearuandeid, asjakohase käsitlusalaga auditi järeldusotsuseid, turvasertifikaate, enesehindamise tulemusi või muud asjakohast teavet.

(9) Kui organisatsioonivälisest tarneahelast tulenev risk ei ole organisatsiooni jaoks aktsepteeritav, tuleb kaaluda alternatiivseid meetmeid või välise osapooli vahetust.

## **§ 9. Personali koolitamine**

Organisatsioon korraldab personalile järjepidevalt koolitusi eesmärgiga:

- 1) parandada turvateadlikkust;
- 2) tagada teabe turvalise töötlemise ja töövahendite turvalise käitlemise oskused;
- 3) ennetada riskikäitumist;
- 4) tõsta teadlikkust küberintsidentide ennetamisest, tuvastamisest ja neile reageerimisest ning täiendada sellealaseid oskusi.

## **3. peatükk Seire**

## **§ 10. Organisatsioonisisene hindamine**

(1) Organisatsioon hindab regulaarselt, kas tal on:

- 1) kindlaks määratud äriprotsessid;
- 2) kaardistatud äriprotsessidega seotud varad;
- 3) kindlaks tehtud välised infoturvanõuded, sealhulgas õigusaktid ja lepingud;
- 4) määratud kaitsetarve;
- 5) vastendatud infoturbekataloogi moodulid kaitseala varaga;
- 6) kehtestatud riskihaldusmetoodika;
- 7) koostatud infoturvameetmete rakendamise plaan;
- 8) rakendatud ja seiratud infoturvameetmeid vastavalt infoturvameetmete rakendamise plaanis seatud tähtaegadele;
- 9) kõrvaldatud auditite ja hindamiste käigus tuvastatud puudused.

(2) Lõikes 1 nimetatud hindamist võib teha organisatsiooniväline isik.

(3) Lõikes 1 nimetatud hindamise käigus tuvastatud puudused tuleb kõrvaldada auditeerimise alguseks.

## **§ 11. Auditeerimine**

(1) Eesti infoturbestandardi järgimise auditeerimise eesmärk on hinnata, kas auditeeritava organisatsiooni infoturbe halduse süsteem ja selle raames rakendatud meetmed vastavad 2. peatüki nõuetele ning kaitsevad organisatsiooni äriprotsesse ja eesmärkide täitmist.

(2) Organisatsioonivälise audiitori sõltumatu hinnang annab organisatsioonile, selle klientidele ja partneritele teavet auditeeritava infoturbe halduse süsteemi jätkusuutlikkuse ja infoturvalisuse ohtudele vastupanuvõime kohta.

(3) Organisatsioonipoolset auditi tellimist, auditiga kaasnevaid kohustusi, auditi kvaliteedi hindamist ning audiitoripoolset auditi kavandamist, tegemist ja selle kohta aruande koostamist on kirjeldatud määruse lisas 2 sätestatud auditeerimiseeskirjas.

#### **4. peatükk**

### **Eesti infoturbestandardi tugi ja rakendamine**

#### **§ 12. Eesti infoturbestandardi rakendamise tugitegevused**

(1) Eesti infoturbestandardi rakendamise toetamiseks ja ühtlustamiseks loob Riigi Infosüsteemi Amet asjaomase veebilehe või rakenduse.

(2) Riigi Infosüsteemi Amet võib lõikes 1 sätestatud veebilehel või rakenduses anda Eesti infoturbestandardi rakendamist toetavaid soovituslikke juhiseid ning esitada muud rakendamist toetavat ajakohast teavet.

#### **§ 13. Enne määruse jõustumist rakendatud turvameetmete ja koostatud dokumentatsiooni kehtivus**

Enne käesoleva määruse jõustumist Eesti infoturbestandardi järgimiseks rakendatud turvameetmed ja koostatud dokumentatsioon kehtivad kuni nende uuendamiseni käesolevas määruses sätestatud korras, kuid mitte kauem kui kolm aastat määruse jõustumisest.

#### **§ 14. Määruse kehtetuks tunnistamine**

Ettevõtlus- ja infotehnoloogiainistri 16. detsembri 2022. a määrus nr 101 „Eesti infoturbestandard“ tunnistatakse kehtetuks.

#### **§ 15. Määruse jõustumine**

Määrus jõustub 1. augustil 2026. a.

Liisa-Ly Pakosta  
Minister

Tiina Uudeberg  
Kantsler

Lisa 1 Infoturbekataloog  
Lisa 2 Auditeerimiseeskiri