

Vastutav osakond: Rahandusministeeriumi strateegia- ja finantsosakond	Kinnitatud: Ministri 06.03.2024 käskkirjaga nr 39
Protsessi koordinaator: Rahandusministeeriumi infoturbejuht	Versioon: 01

## RAHANDUSMINISTEERIUMI VALITSEMISALA INFOTURVAPOLIITIKA

Versiooni nr	Käskkirja kpv ja nr	Jõustumise kuupäev	Muudatuse kirjeldus
Ver 01	06.03.2024 nr 39	06.03.2024	Algse täisversiooni loomine.

### I Üldsätted

- 1.1 Rahandusministeeriumi valitsemisala infoturvapoliitika lähtub küberturvalisuse seadusest ja selle alusel kehtestatud õigusaktidest, Euroopa Liidu vastava valdkonna õigusaktidest, rahvusvahelistest infoturbe halduse standarditest ja parimast praktikast.
- 1.2 Käesoleva infoturvapoliitika eesmärgiks on kehtestada raamistik ja suunised Rahandusministeeriumi (edaspidi *RM*) ja Rahandusministeeriumi valitsemisala asutuste (edaspidi koos *RMV asutused*) infoturbevaldkonna korraldamiseks ning varade ja väärtuste haldamiseks nii, et oleks tagatud ühetaoliselt RMV asutuste infovarade käideldavus, terviklus ja konfidentsiaalsus.
- 1.3 Infoturbe korraldamise eesmärgiks RMV asutustes on asutuse mainet ja õigusaktidega pandud ülesannete täitmise võimekust kahjustavate olukordade ärahoidmine, infoturvasündmuste asjakohane ja kiire käsitlemine ning infoturvaintsidentide mõju vähendamine, vastavalt asutuse enda poolt aktsepteeritud kvaliteedi- ja riskitasemeteni.
- 1.4 Informatsiooni terviklus, käideldavus ja konfidentsiaalsus tuleb eelkõige tagada ulatuses, mis võimaldab RMV asutustes kõige tõenäolisemate ohtude realiseerumisel häireteta oma ülesandeid täita.
- 1.5 Infovarade kaitse RMV asutustes tuleb tagada vastavalt infovaradele määratud kaitsetarbele või nende rahalisele väärtusele ning kehtivatele õigusaktidele.
- 1.6 RMV ülese infoturvapoliitika sihtrühmaks on RMV asutuste juhtkondade liikmed, asutuste struktuuriüksuste, valdkonna- ja funktsioonijuhid.
- 1.7 Rakendatavad turvameetmed peavad olema majanduslikult õigustatud ja proportsiooniliselt võimaliku meetmete puudulikkusest tekkiva kahjuga ning nende häiriv toime RMV asutuste tegevusele ja teenistujate tööle peab olema võimalikult väike.
- 1.8 Infoturvapoliitika vaadatakse üle ja vajadusel uuendatakse vähemalt kord kahe aasta jooksul või vastavalt muutustele RMV eesmärkides ja strateegias, õigusaktides, lepingulistes kohustustes ning ümbritsevas infoturbeolukorras. Ülevaatuse korraldamise eest vastutab RM infoturbejuht.

### II Infoturvapoliitikas kasutatud mõisted

Vastutav osakond: Rahandusministeeriumi strateegia- ja finantsosakond	Kinnitatud: Ministri 06.03.2024 käskkirjaga nr 39
Protsessi koordinaator: Rahandusministeeriumi infoturbejuht	Versioon: 01

RMV infoturvapoliitikas kasutatakse mõisteid järgmises tähenduses:

- 2.1 **Andmed (üldmõiste)** - Andmed kui infovarad on mis tahes viisil ja mis tahes andmekandjale jäädvustatud või infotehnoloogiliste vahendite abil edastatav või töödeldav teave.
- 2.2 **Infotehnoloogilised vahendid (edaspidi IT-vahendid)** - Infosüsteemide teenuste osutamiseks ja andmete töötlemiseks kasutatavad hooned, ruumid ja infrastruktuur, erinevate tehnoloogiliste seadmete riist- ja tarkvara.
- 2.3 **Infoturvasündmus** - Süsteemi, teenuse või võrgu sellise oleku tuvastatud ilmnemine, mis näitab võimalikku infoturbe rikkumist või turvameetmete tõrget või senitundmatut olukorda, mis võib puudutada turvalisust.
- 2.4 **Infoturvaintsident** - Ootamatu või soovimatu infoturvasündmus, mille tagajärjel tekib asutusele oluline varaline või mittevaraline kahju, kahju andmetele, ümbritsevale keskkonnale, klientidele või teenistujatele, samuti sündmus, mille tulemusena asutuse põhi- või tugitegevuse valdkonnas töö seiskub või on häiritud.
- 2.5 **Infoturve** - Informatsiooni tervikluse, käideldavuse ja konfidentsiaalsuse tagamine, kus:
  - käideldavus tähendab informatsiooni kasutuskõlblikkust ja õigeaegset kättesaadavust volitatud isikule;
  - terviklus tähendab, et informatsioon pärineb autentsest allikast ning seda ei ole volitamata muudetud ega kustutatud;
  - konfidentsiaalsus tähendab, et informatsioon on kättesaadav vaid volitatud isikule.
- 2.6 **Infovarad** - asutuse infosüsteemide käitamiseks kasutatavad IT-vahendid ja andmed, samuti neid funktsionaalseks tervikuks siduvad asutuse IT-teenused.
- 2.7 **IT-teenus** - Asutuse poolt hallatud või kasutatav teenus, mis seob asutuse IT-vahendeid ja andmeid funktsionaalseks tervikuks ning mida asutus käsitleb kaitset vajava infovarana.
- 2.8 **Kaitsetarve** - infovara väärtusest tulenev asutuse kui infovara omaniku hinnang infovara kaitsmise vajadusele. Mõiste on täpsemalt kirjeldatud infoturbestandardis E-ITS.

### III Asutuse infoturbe halduse süsteem (ISMS)

- 3.1 Asutuse infovarade kaitseks ning nende kvaliteedi ja sihipärase kasutamise tagamiseks rakendab iga RMV asutus asutusepõhist terviklikku ja infovarade olelusringist lähtuvat infoturbe halduse süsteemi (edaspidi ISMS).
- 3.2 RMV asutuse ISMS-i ülesehitus ja toimemudel peavad lähtuma asutuse põhimäärusest, asutusele õigusaktidega pandud ülesannetest ja asutuse vajadustest ning IT-teenuste iseloomust.
- 3.3 RMV asutuses rakendatud ISMS peab täitma kas Eesti infoturbestandardis E-ITS (<https://eits.ria.ee>) või rahvusvahelise ISO/IEC 27000 infoturbejuhtimise seeria standardites esitatud nõudeid ning täitma valitud standardi eeltingimused infoturbe auditeerimiseks.

### IV Vastutuse ja ülesannete jaotus RMV üleselt infoturbe korraldamisel

- 4.1 RM on RMV-s infoturbe korraldamise koordinaator.

Vastutav osakond: Rahandusministeeriumi strateegia- ja finantsosakond	Kinnitatud: Ministri 06.03.2024 käskkirjaga nr 39
Protsessi koordinaator: Rahandusministeeriumi infoturbejuht	Versioon: 01

- 4.2 **RMV IT nõukogu**, mida juhib RM kantsler, koordineerib RMV IKT-valdkonna juhtimist ning kiidab heaks ka käesoleva RMV infoturvapoliitika.
- 4.3 RMV IT nõukogu tööd infoturbe- ja IT-riskijuhtimise valdkonnas toetab **RMV asutuste infoturbejuhtide komisjon**, mis koordineerib RMV infoturvapoliitika elluviimist, valmistab ette RMV üleseid infoturberiski otsuseid ning täidab muid RMV IT nõukogu antud ülesandeid.
- 4.4 RMV infoturvapoliitika rakendamisel on RMV asutustel järgmised ülesanded:
- 4.4.1 Asutuse kõik juhtimistasandid toetavad RMV infoturvapoliitikas kirjeldatud eesmärkide saavutamist ning tagavad oma vastutusalala tööprotsessides RMV infoturvapoliitika ja asutuse enda infoturvapoliitika põhimõtete järgimise.
  - 4.4.2 Asutuse infoturbe eest vastutav isik tagab, et RMV infoturvapoliitika põhimõtted oleksid rakendatud asutuse enda infoturvapoliitikas, asutuse töökorralduse reeglites või protsessikirjeldustes.

## V RMV asutuses infoturbestandardi põhimeetmete rakendamine

- 5.1 Asutus lähtub infoturbe planeerimisel ja korraldamisel Eesti Infoturbestandardi E-ITS meetmete kataloogist.
- 5.2 Meetmete konteksti loomiseks tuleb lähtuda standardi dokumentatsioonist.
- 5.3 Kõik asutused kohustuvad rakendama vähemalt E-ITS põhimeetmeid. Standardmeetmete ja kõrgmeetmete rakendamine ja rakendamise tähtaeg otsustatakse asutuse riskianalüüsi põhjal.
- 5.4 Vastavalt E-ITS standardis kirjeldatud ISMS turbehalduse peatükile, on asutuse infoturbe korraldamise üldvastutajaks asutuse juht ja tema volitatud isikud, lähtuvalt asutuse põhimäärusest (asutuse juhtkond).
- 5.5 Asutuse juhtkond:
- 5.5.1 algatab, juhib ja kontrollib turbeprotsessi;
  - 5.5.2 määrab infoturbega seotud rollid;
  - 5.5.3 kehtestab asutuse infoturvapoliitika.
- 5.6 Asutuse juhtkond loob protsessi, mis tagab asutuse juhtkonnale regulaarse ja piisava teavituse asutuse infoturbe olukorrast.
- 5.7 Asutus kehtestab teenistujate kaasamise ja teavitamise põhimõtted nii, et teenistujad oleksid teadlikud infoturbe ohtudest, tunneksid turvameetmeid ning oskaksid neid tööülesannete täitmisel nõuetekohaselt järgida.
- 5.8 Kui asutuses rakendatakse infoturbestandardina ISO/IEC 27000 seeriat, siis lähtutakse meetmete rakendamisel ISO standardist ning RMV infoturvapoliitika punktides 5.1 – 5.7. kirjeldatu ei kohaldu.

## VI Infoturbe eesmärkide täitmiseks vajalikud protsessid

Vastutav osakond: Rahandusministeeriumi strateegia- ja finantsosakond	Kinnitatud: Ministri 06.03.2024 käskkirjaga nr 39
Protsessi koordinaator: Rahandusministeeriumi infoturbejuht	Versioon: 01

- 6.1 RMV asutus kirjeldab ja kehtestab infoturbe eesmärkide saavutamiseks toimimisreeglid või protsessikirjeldused asutuse IT-valdkonna korraldamisel vähemalt järgmistes valdkondades:
- 6.1.1 asutuse teenuste ja/või protsesside kirjeldamine ja haldus;
  - 6.1.2 riskijuhtimine;
  - 6.1.3 asutuse asukohtade, hoonete ja ruumide füüsilise turvalisuse tagamine;
  - 6.1.4 IT-teenuste hankimine ning IT-valdkonna lepete ja lepingute haldus;
  - 6.1.5 IT-teenuste muudatuste haldus;
  - 6.1.6 IT-teenuste ja andmete juurdepääsuõiguste haldus;
  - 6.1.7 infoturvaintsidentide ja kriisihaldus;
  - 6.1.8 asutuse teenistujate andmekaitse- ja turvateadlikkuse arendamine.
- 6.2 Toimimisreeglite või protsesside täpsemal kirjeldamisel lähtub asutus Eesti ja rahvusvahelistest infoturbestandarditest, asutuse tegevusvaldkonna asutuse-välistest nõuetest ja headest praktikatest ning koostööprotsesside puhul lisaks ka koostööpartneritega sõlmitud kokkulepetest.