

Ühismaja arvutivõrgu infoturbe poliitika põhimõtted

1. Mõisted

- 1.1. **RIKi infoturbejuht** – RIKi hallata olevate teenuste infoturbe korraldamise eest vastutav töötaja.
- 1.2. **Tellija infoturbejuht** – Tellija infoturbe korraldamise eest vastutav töötaja.
- 1.3. **Infoturbe** – andmete tervikluse, käideldavuse ja konfidentsiaalsuse tagamine, kus:
 - Käideldavus tähendab informatsiooni kasutuskõlblikkust ja õigeaegset kättesaadavust volitatud isikule;
 - Terviklus tähendab, et info pärineb autentsest allikast ning seda ei ole volitamata muudetud ega kustutatud;
 - Konfidentsiaalsus tähendab, et informatsioon on kättesaadav vaid volitatud isikule.
- 1.4. **Infoturbeintsidendid** – kõik reaalse või potentsiaalse kahju juhtumid, mis võivad ohustada või halvata IT-teenuste turvalisust, põhjustades nende käideldavuse (töökindlus), tervikluse (andmete õigsuse ja muutumatuse) või konfidentsiaalsuse (andmete salastatuse) kao. Infoturbe intsidendiks loetakse ka toiminguid, mis ei ole infoturbe valdkonda reguleerivate õigusaktidega kooskõlas.
- 1.5. **Infovara** – tellija kasutuses olevad infotehnoloogilised vahendid (riist-, tarkvara ja andmesideseadmed) ja viimaste abil töödeldavad andmed.
- 1.6. **Intsident** – on iga sündmus või pöördumine, mis ei ole standardse IT-teenuse osa ning mis võib põhjustada või põhjustab teenuse katkestuse või kvaliteedi halvenemise.
- 1.7. **ISKE** – infosüsteemide kolmeastmeline etalon turbe süsteem.
- 1.8. **Kontrolljälg** – on kronoloogiline sündmuste andmestik, mis talletatakse andmefailina järgnevatks läbivaatuseks ja analüüsimiseks.

2. Sissejuhatus

- 2.1. Käesoleva dokumendi eesmärk on luua raamistik arvutivõrgu infoturbe korraldamiseks, et tagada tellija kasutuses olevate infovarade käideldavus, terviklus ja konfidentsiaalsus kokkulepitud tasemel.
- 2.2. Infovarade kaitse tuleb tagada vastavalt varade väärtusele ning Eesti Vabariigis kehtivatele õigusaktidele.

3. Infoturbe organisatsioon

- 3.1. Tellija infoturbealase tegevuse koordineerimise ja korraldamise eest tervikuna vastutab tellija infoturbejuht.
- 3.2. Infoturbealase tegevuse koordineerimise ja korraldamise eest RIKi pakutavate teenuste osas vastutab RIKi infoturbejuht.
- 3.3. Kõik infoturvet puudutavad muudatused tuleb kooskõlastada infoturbe juhiga vastavalt punktides 3.1 või 3.2 toodud vastutusalale.
- 3.4. Justiitsministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Rahandusministeeriumi, Haridus- ja Teadusministeeriumi ning Sotsiaalministeeriumi ühishoone infoturvet puudutavad olulised otsused võetakse vastu RIKi infoturbejuhi eestvedamisel ministeeriumite kantslerite või kantslerite poolt volitatud isikute vahel (edaspidiselt ka kui *kantslerite kogu*).
- 3.5. Olulisteks otsusteks on muuhulgas:
 - 3.5.1. olulisemate ministeeriumite ühismajaga seotud infoturbealastele probleemide käsitlemine;
 - 3.5.2. füüsilise turbe eest vastutava isiku/struktuuriüksuse määramine;
 - 3.5.3. ministeeriumite ühismaja puudutavate infoturbe põhimõtete kinnitamine.
- 3.6. Tellija infoturbejuhi ülesanneteks on:

- 3.6.1. tagada infoturvet reguleerivate poliitikate, kordade ja juhiste olemasolu, elluviimine ja ajakohastamine;
- 3.6.2. nõustada füüsilise turbe eest vastutavaid isikuid organisatsioonide ja füüsiliste infoturbemeetmete rakendamise osas;
- 3.6.3. teha oma ülesannete täitmisel koostööd RIK infoturbe eest vastutavate isiku(te)ga, isikuandmete töötlemise eest vastutavate isiku(te)ga ning teiste asjakohaste partneritega;
- 3.6.4. koordineerida infoturvet reguleerivate poliitikate, standardite, kordade ja juhiste täitmise kontrollimist ning infoturbemeetmete rakendamise tõhususe testimist;
- 3.6.5. kantslerite või nende poolt määratud infoturbe eest vastutavate isikute teavitamine intsidentidest;
- 3.6.6. teavitada Riigi Infosüsteemi Ameti (RIA) infoturbeintsidentide käsitlemise osakonda (CERT-EE) olulistest turvaintsidentidest vastavalt Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 "Infosüsteemi turvameetmete süsteem" kehtestatud rakendusjuhendile;
- 3.6.7. korraldada tellija töötajate ja teenistujate teavitamine turvareeglitest, nende infoturbealane nõustamine ning vajadusel korraldada töötajatele ja teenistujatele koolitusi üldise turvateadlikkuse tõstmiseks;
- 3.7. RIKi infoturbejuhi ülesanneteks on muuhulgas:
 - 3.7.1. korraldada RIKi poolt pakutavate teenuste ISKE IT-valdkonda kuuluvate turvameetmete rakendamist, koostöös tellija infoturbejuhiga, sh koostada RIKi pakutavate teenuste infovarade ning rakendatud ISKE meetmete nõuetekohased alusdokumendid;
 - 3.7.2. menetleda RIKi poolt pakutavate teenustega seotud infoturbeintsidente ning teavitada tulemustest tellija infoturbejuhti.
 - 3.7.3. esitada iga kvartali kümnendaks tööpäevaks koondraport eelmise kvartali infoturbeintsidentidest.
 - 3.7.4. viia läbi infoturbealaseid koolitusi tellija töötajatele RIKi poolt pakutavate teenuste osas.
 - 3.7.5. korraldada tellija infoturbejuhi viivitusteta teavitamine tellija infoturvet puudutavatest sündmustest (intsidentid, muudatused jne). Tasemel „kõrge“ intsidentidest tuleb teavitada telefoni ja e-maili teel, madalamatest e-maili teel vastavalt Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 "Infosüsteemi turvameetmete süsteem" kehtestatud rakendusjuhendile.
 - 3.7.6. teavitada Riigi Infosüsteemi Ameti infoturbeintsidentide käsitlemise osakonda (CERT-EE) olulistest turvaintsidentidest vastavalt Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 "Infosüsteemi turvameetmete süsteem" kehtestatud rakendusjuhendile;
 - 3.7.7. nõustada füüsilise turbe eest vastutavaid isikuid organisatsioonide ja füüsiliste infoturbemeetmete rakendamise osas;
 - 3.7.8. teha oma ülesannete täitmisel koostööd tellija infoturbe eest vastutavate isiku(te)ga, isikuandmete töötlemise eest vastutavate isiku(te)ga ning teiste asjakohaste partneritega.
- 3.8. Infoturbealane vastutus on igal tellija töötajal ja teenistujal ning seisneb antud valdkonda reguleerivate seaduste, kordade ja juhiste järgimises.
- 3.9. Tellija struktuuriüksuste juhid vastutavad infoturbe rakendamise eest oma struktuuriüksustes. Struktuuriüksuse juhi infoturbealased kohustused on muuhulgas:
 - 3.9.1. arvestada infoturbe alaseid nõudeid IT-teenuste arendamise, soetamise, kasutusele võtmise ja hooldusega seotud tegevustes;
 - 3.9.2. nõuda, et kõik tema struktuuriüksuse töötajad ja teenistujad oleks tutvunud ja täidaksid asutuses kehtivaid infoturbealaseid kordi, nende tööd puudutavaid õigusakte ning omaksid nende töö- või ametiülesannete täitmiseks vajalikke infoturbealaseid teadmisi.

3.10. Füüsilise turbe eest vastutav isik täidab infoturbealaseid kohustusi lähtuvalt käesolevast dokumendist või muust antud valdkonda reguleerivast õigusaktist ning kohustub täitma vähemalt järgmisi infoturbealaseid ülesandeid:

3.10.1. korraldada ISKE IT-valdkonda mittekuuluvate turvameetmete rakendamist juhindudes infoturbejuhtide soovitustest;

3.10.2. kontrollida, et asutuses tutvustatakse ja täidetakse füüsilise turbega seotud poliitikaid, standardeid, eeskirju ja kordasid.

4. Riskihaldus ja standardid

4.1. Riskihaldus ja infoturbe meetmete rakendamine põhineb ISKE-I vastavalt Vabariigi Valitsuse 20. detsembri 2007. a määrusele nr 252 "Infosüsteemi turvameetmete süsteem". ISKE-ga määratakse ära minimaalsed turvameetmed, mida tuleb rakendada IT-teenusele ettenähtud turvataseme saavutamiseks ja säilitamiseks.

4.2. Kui mõnda ISKE poolt ettekirjutatud turvameedet ei ole võimalik või otstarbekas täita, peab leidma alternatiivsed meetmed riski maandamiseks või peab kantslerite kogu aktsepteerima meetme täitmata jätmisega tekkinud jääkriski.

5. Infoturbeintsident ja kontrollijäljed

5.1. Infoturbeintsidentide avastamise üheks eelduseks on kontrollijälgede jälitatavuse toimivus. Jälitatavuse tagamiseks salvestatakse ja säilitatakse IT-teenuste haldamise ja kasutamisega seotud toimingute teostamise kohta kontrollijälgi.

5.2. Infoturbeintsidendi lahendamiseks tagatakse infoturbejuhtidele juurdepääs intsidendi lahendamiseks vajalikele kontrollijälgedele ja muule arvutivõrgus olevale informatsioonile.

5.3. Intsidendi lahendamise käigus kogutud informatsioon dokumenteeritakse ja analüüsitakse eesmärgiga vältida sarnaste intsidentide aset leidmist tulevikus ning otsustada täiendavate turvameetmete rakendamise vajaduse üle.

5.4. Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo või distsiplinaarsüüteo või töölepingu rikkumise tunnuseid, antakse juhtum edasi menetlemiseks vastava menetluse läbiviimise õigust omavale asutusele või isikule.