TARBIJAKAITSE JA
TEHNILISE JÄRELEVALVE
AMET

KÄSKKIRI

20.02.2024 nr 1-2/24-015

Infoturbepoliitika kinnitamine

Vabariigi Valitsuse 15. märtsi 2012. a määruse nr 26 „Infoturbe juhtimise süsteem“ § 3 p-de 1 ja 2 ning majandus- ja taristuministri 7. detsembri 2018. a määruse nr 62 „Tarbijakaitse ja Tehnilise Järelevalve Ameti põhimäärus“ § 5 lg 3 p 1 alusel:

kinnitan

Tarbijakaitse ja Tehnilise Järelevalve Ameti infoturbepoliitika (lisatud).

(allkirjastatud digitaalselt)
Kristi Talving
peadirektor

Koostaja: Mariko Männa

KINNITANUD
peadirektor
20.02.2024
käskkirjaga nr 1-2/24-015

TARBIJAKAITSE JA TEHNILISE JÄRELEVALVE AMETI INFOTURBEPOLIITIKA

2024

1. Üldsätted

1.1. Tarbijakaitse ja Tehnilise Järelevalve Ameti (edaspidi TTJA) infoturbeprotsess on algatatud käesoleva poliitika kehtestamisega.
1.2. TTJA infoturbepoliitika (edaspidi poliitika) on juhtdokument, mis kirjeldab TTJA infoturbe eesmärgid, vajadused ja põhimõtted ning mille eesmärk on organisatsiooni väärtuste ja põhitegevuse kaitse.
1.3. TTJA infoturbe halduse süsteemi (ISMS) eesmärk on tagada elementaarne turbetase, võimaldades seeläbi ametil seadusest tulenevate ülesannete täitmist.
1.4. Poliitika on koostatud kooskõlas järgmiste õigusaktidega:
  1.4.1 Küberturvalisuse seadus;
  1.4.2 Avaliku teabe seadus;
  1.4.3 Isikuandmete kaitse seadus;
  1.4.4 Euroopa parlamendi ja nõukogu 27.04.2016 määrus nr 2016/679 „Isikuandmete kaitse üldmäärus“;
  1.4.5 Riigisaladuse ja salastatud välisteabe seadus;
  1.4.6 Vabariigi Valitsuse 16.12.2022 määrus nr 101 „Eesti infoturbestandard“;
  1.4.7 Vabariigi Valitsuse 19.06.2020 määrus nr 11 „Arvutite ja kohtvõrkude kaitse nõuded“;
  1.4.8 Vabariigi Valitsuse 15.03.2012 määrus nr 26 „Infoturbe juhtimise süsteem“;
  1.4.9 Vabariigi Valitsuse 20.12.2007 määrus nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“.
1.5. Poliitikat viiakse ellu, võttes arvesse järgmisi infoturbestandardeid ja nendest tulenevaid põhimõtteid:
  1.5.1 Eesti infoturbestandard (edaspidi E-ITS);
  1.5.2 ISO 27000-seeria infoturbestandardid.
1.6. Poliitika on täitmiseks kõigile TTJA teenistujatele, praktikantidele, töövõtu- või muu lepingu alusel teenust osutavatele isikutele ja kõigile teistele isikutele, kes osalevad TTJA töös (edaspidi koos teenistuja).
1.7. Käesolevas poliitikas kasutatud mõistete definitsioonid on alljärgnevad:

Mõiste	Definitsioon
Etalonturve	Metoodika turbehalduse süsteemi rajamiseks ning infosüsteemide turbeks tüüpmeetmetega.
Infoturbe halduse süsteem (ISMS)	Süsteem, mis koosneb poliitikatest, protseduuridest, juhistest ning nendega seotud ressurssidest ja tegevustest, mida organisatsioon kollektiivselt haldab, et kaitsta oma infovarasid. ISMS on suunatud ärieesmärkide saavutamisele ning kujutab endast süstemaatilist lähenemi infoturbe rajamisele, käigushoiule, seirele, hooldamisele ja täiustamisele.
Infovara	Miski, millel on organisatsiooni jaoks väärtus; näiteks teave, andmed, tarkvara, füüsiline vara (taristu, hoone, riistvara, sisseseade vm), rahaline vara, teenus, inimressurss (inimesed, kvalifikatsioon, oskused, kogemused), oskusteave, mitteaineline vara (maine, kuvand jms).
Kaitseala	Turbekontseptsiooni koostamise ja rakendamise käsitlusala. Organisatsioon liigitab kaitsealasse kogumi sihtobjekte, mida turbeprotsess hakkab edaspidi kaitsma.
Kaitsetarve	Näitab, milline kaitse on äriprotsessile, selles töödeldavale informatsioonile ja rakendatavale infotehnoloogiale piisav ja sobiv.
Konfidentsiaalsus	Teabe omadus olla kättesaamatu või paljastamatu volitamata isikutele ja protsessidele. Üks kolmest turvalisuse põhikategooriast.

Käideldavus	Teabe, IT-süsteemide, inimeste, protsesside teovõime ja kättesaadavus volitatule siis, kui ta neid vajab. Üks kolmest turvalisuse põhikategooriast.
Risk	Määramatuse toime eesmärkidele. Sageli iseloomustatakse riski võimalike sündmuste ja tagajärgedega või mingi sündmuse tagajärgede ja selle sündmuse võimalikkuse kombinatsiooniga.
Sihtobjekt	Infosüsteemi osa, millega tuleb modelleerimise raames seada vastavusse üks või mitu moodulit etalonturbe kataloogist. Sihtobjekt võib olla füüsiline, näiteks võrk või IT-süsteem. Sageli on aga sihtobjektideks loogilised objektid, näiteks organisatsiooni allüksused, rakendused või kogu infosüsteem.
Standardturve	Eesti infoturbestandardis esitatud etalonturbe metoodika, millega kaitstakse organisatsiooni infovarasid läbi standardmeetmete rakendamise.
Terviklus	Lubamatute muudatuste puudumine, hõlmab ka autentsust ja salgamatust, üks teabe turvalisuse kolmest põhikomponendist.
Turvasündmus	Süsteemi, teenuse või võrgu sellise oleku ilming, mis viitab võimalikule TTJA kehtestatud reeglistiku rikkumisele või turvameetmete tõrkele või senitundmatule olukorrale, mis võib puudutada teabe turvalisust.
Äriprotsess	Kogum loogiliselt seotud tegevusi (ülesandeid, töövooge), mis sooritatakse teatavate äriliste või organisatsiooniliste eesmärkide saavutamiseks.

2. Infoturbe eesmärgid ja strateegia

2.1. TTJA infoturbe eesmärk on tagada ameti põhitegevuse (äriprotsesside) jätkuvus ja minimeerida võimalik kahju turvasündmuste vältimise ja nende mõju vähendamise abil. Selle saavutamiseks:
- 2.1.1 TTJA kehtestab toimingud ja reeglid ning nende rakendamist kontrollitakse regulaarselt läbi järelevalve tegevuste;
- 2.1.2 infoturberiskid on hallatud vastavalt TTJA riskiregistris sätestatule;
- 2.1.3 infoturve on tagatud läbi meetmete, mis loovad äriprotsesside käitamiseks sobiliku ja turvalise töökeskkonna ning on vastavuses sihtobjekti kaitsetarbe ja nõuetega.

2.2. Infoturbe strateegiaks on saavutada eesmärgid infovarade käideldavuse, tervikluse ja konfidentsiaalsuse tagamise kaudu.

2.3. TTJA infoturbe kaitsealasse kuuluvad kõik asutuse äriprotsessid, IT süsteemid, rakendused, ressursid ja sõltuvused (sh liidestused välispartneritega).

3. Infoturbe korralduse põhimõtted

3.1. Läbiv infoturbe vastutus on TTJA teenistujal, kes järgib oma tegevustes valdkonda reguleerivaid juhendeid ning teavitab infoturbeintsidentidest aadressil klienditugi@ttja.ee.

3.2. TTJA peadirektor vastutab infoturbe halduse süsteemi toimimise eest, tagab infoturbe sõltumatuse asutuse muust tööst ning täidab muid õigusaktides sätestatud ülesandeid.

3.3. TTJA infoturbejuhi ülesandeid täidab Riigi Info- ja Kommunikatsioonitehnoloogia Keskuse (edaspidi RIT) määratud teenistuja.

3.4. TTJA juhtkond aktsepteerib töötajate põhitööga kaasnevaid infoturbekohustusi.

4. Infoturbe rakendamine

4.1. Poliitika alusel kehtestab TTJA peadirektor käskkirjaga juhendeid ja protsessikirjeldusi.
4.2. TTJA infoturbe tagamisega seotud juhendid ja dokumentatsioon on kättesaadavad siseveebist ja dokumendihaldussüsteemist.
4.3. Infoturbejuht tagab regulaarsed infoturbe ülevaated TTJA juhtkonnale ning olulised infoturbealased otsused kommunikeeritakse kogu personalile.
4.4. TTJA infoturbe aluseks on infovarade riskihaldus, mis tugineb E-ITS etalonturbe metoodikale ja riskihaldusjuhendile.
4.5. Riskide leevendamiseks või muul moel muutmiseks rakendatakse turvameetmeid vastavalt infovaradele määratud kaitstuse vajadusele.
4.6. Infoturbe halduse ja selle alamprotsesside kirjeldused ning nendele esitatavad nõuded kehtestatakse eraldi infoturbekontseptsiooniga.
4.7. Infovarade ja kaitseala kaardistamiseks võtab TTJA äriprotsessidena arvele tegevuspõhise kulujuhtimise ja eelarvestamise raames määratud teenused.
4.8. TTJA-le kohaldatav kaitsetarve on väga suur, täpsema määranguga C3-I3-A2.
4.9. Kaitsetarvete määramise akte hoiustatakse TTJA infoturbe lehel *sharepoint* keskkonnas. Ülevaade kaitsetarvete määramise tulemustest teenuste lõikes on käesoleva poliitika lisas 1.
4.10. Lähtuvalt kaitsetarbe määrangust rakendatakse TTJA äriprotsesside kaitseks standardturvet.
4.11. Käesolevat poliitikat ja selle täitmiseks koostatud juhendite sisu ajakohasust hinnatakse vähemalt kord aastas või infoturbe süsteemi oluliste muutuste aset leidmisel.

Lisa 1
KINNITANUD
peadirektor
20.02.2024
käskkirjaga nr 1-2/24-015

Tarbijakaitse ja Tehnilise Järelevalve Ameti kaitsetarvete koondülevaade

Digiühiskonna programmi teenuste kaitsetarbed on järgmised:

Digilahenduste ligipääsetavuse järelevalve	C2-I2-A2
Küberturbe sertifitseerimine	C3-I2-A1
Digiühiskonna tegevus- ja kasutusõiguse andmine	C2-I2-A2
Elektroonilise side tururegulatsioon	C3-I3-A2
Digiühiskonna järelevalve	C2-I2-A2
Sidevaldkonna järelevalve	C2-I2-A2
Tegevus- ja kasutusõiguse andmine (raadioside sagedusload ja sidevaldkonna load)	C2-I2-A2
Numeratsiooni kasutuse pikaajaline planeerimine	C2-I2-A2

Ettevõtluse programmi teenuste kaitsetarbed on järgmised:

Ettevõtlusvaldkonna järelevalve	C2-I2-A2
Tarbijate nõustamine ja kohtuväline vaidluste lahendamine	C2-I2-A2
Ettevõtluse valdkonna tegevusõiguse andmine	C2-I2-A2

Transpordi konkurentsivõime ja liikuvuse programmi teenuste kaitsetarbed on järgmised:

Tegevus- ja kasutusõiguse andmine (raudteeohutus)	C2-I2-A2
Raudtee tururegulatsioon	C2-I2-A2
Rail Baltic arendamise riiklik järelevalve	C1-I2-A2
Raudteeohutuse järelevalve korraldamine	C2-I2-A2

Ehituse programmi teenuste kaitsetarbed on järgmised:

Ehitusvaldkonna järelevalve (sh energiatõhususe järelevalve)	C2-I2-A2
Tegevus- ja kasutusõiguse andmine (ehitusohutus)	C2-I2-A2

Sisemiste tugiprotsesside kaitsetarbed on järgmised:

Finantshaldus	C2-I2-A2
Teabehaldus	C2-I2-A2
Personalihaldus	C2-I2-A2