KINNITATUD
Ravimiameti peadirektori
detsembri 2023
käskkirjaga nr 37

INFOTURVAPOLIITIKA

SISUKORD

1. EESMÄRK JA ÜLDPÕHIMÕTTED

1.1 Infoturvapoliitika kehtestab turvaeesmärgid, turbe strateegia ja rollid Ravimiameti (edaspidi amet) tööprotsesside ja infovara kaitseks.

1.2 Amet juhindub Sotsiaalministeeriumi (edaspidi ministeerium) ja selle valitsemisala infoturvapoliitikast, mille elluviimine on Tervise ja Heaolu Infosüsteemide Keskuse (TEHIK) põhimäärusest tulenev ülesanne. Ameti infovarale rakendatakse otstarbekohaseid turvameetmeid koostöös TEHIKuga.

1.3 Infoturvapoliitika lähtub lisaks ministeeriumi ja selle valitsemisala infoturvapoliitikale
- 1.2.1 küberturvalisuse seadusest;
- 1.2.2 Vabariigi Valitsuse 15. märtsi 2012. a määrusest nr 26 „Infoturbe juhtimise süsteem“;
- 1.2.3 Eesti infoturbestandardi (E-ITS) kehtivast versioonist;
- 1.2.4 isikuandmete kaitse üldmäärusest ja avaliku teabe seadusest.

1.4 Turvameetmete planeerimisel ja rakendamisel arvestatakse, et need oleks majanduslikult õigustatud ja proportsioonis võimalikest ebapiisavatest meetmetest tekkida võiva kahjuga ning et nende häiriv toime ameti tegevusele ning ameti teenistujate tööle oleks võimalikult väike.

1.5 Infoturvapoliitika kehtib kogu ametis ning selle järgimine on kõigile ameti ametnikele ja töötajatele (edaspidi koos teenistujad) ning käsundus- või muu lepingu alusel teenust osutavatele isikutele kohustuslik.

2. MÕISTED

2.1 Infoturve - riskihalduslik tegevus teabe turvalisuse säilitamiseks ning andmete tervikluse, käideldavuse ja konfidentsiaalsuse tagamiseks, kus

2.1.1 käideldavus on infovara õigeaegne kättesaadavus ja kasutatavus selleks volitatud isikutele;
2.1.2 terviklus on infovara täielikkus, õigsus ja ajakohasus, sealjuures lubamatute muudatuste puudumine;
2.1.3 konfidentsiaalsus on infovara kättesaadavus ainult selleks volitatud isikutele.

2.2 Infovara – informatsioon ja andmed ning nende töötlemiseks vajalikud infotehnoloogilised rakendused ja tehnilised vahendid.

2.3 Infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem.

2.4 Infoturbe juhtimise süsteem – meetmete kompleks, mis võimaldab tagada asutuse põhitegevuse jätkusuutlikkuse ja infovarade kaitstuse.

2.5 Andmete omanik – isik, kes vastutab andmete eest terve nende elutsükli jooksul (mh andmete töötlemise korraldamise ja vastava infosüsteemi administreerimise delegeerimise eest).

2.6 Turvaintsident – mistahes sündmus, mis ohustab või halvab infovara turvalisust, põhjustades käideldavuse, tervikluse või konfidentsiaalsuse kao ning kahjustades ameti teavet, vara või teenuseid.

2.7 Juurdepääsupiiranguga teave – konfidentsiaalne teave ja andmed, millele on kehtestatud juurdepääsupiirang lepingu või seaduse alusel.

3. INFOTURBE KORRALDUS JA VASTUTUS

3.1 Ameti infoturbealased eesmärgid on:
3.1.1 tagada ameti põhitegevuse toimimine ja teenuste osutamine;
3.1.2 tagada protsesside ja infovara konfidentsiaalsus, terviklus ja käideldavus;
3.1.3 säilitada ameti kuvand.

3.2 Ameti peadirektor vastutab infoturbe eest asutuses, sealhulgas:
3.2.1 määrab infoturbe eest vastutava isiku ja vajadusel teised infoturbega seotud rollid asutuses;
3.2.2 tagab infoturbe eest vastutavale isikule ülesannete täitmiseks vajalikud tingimused ja ressursid, ligipääsu teabele ja objektidele;
3.2.3 tagab, et asutuse teenistujad on asutuses kehtivate infoturbealaste õigusaktidega tutvunud ja täidavad neid ning omavad enda tööülesannete täitmiseks infoturbealaseid teadmisi;
3.2.4 tagab asutuses infovara kaitseks nõuetele vastavate turvameetmete rakendamise ja eraldab selleks vajalikud ressursid.

3.3 Ameti infoturbe eest vastutav isik täidab ametis järgmiseid infoturbealaseid kohustusi:
3.3.1 mõistab asutuse tööprotsesse ja andmeid ning nende kaitse vajadust;
3.3.2 koostab ja kaasajastab asutuse infoturbealaseid kordi ja dokumentatsiooni, sh infoturvapoliitika ja protsesside kaitsetarbe regulaarne ülevaatus (vähemalt kord aastas või oluliste muudatuste puhul);
3.3.3 töötab välja infoturbemeetmete rakendusplaani (sh prioriteedid ja teostusjärjekord), korraldab selle elluviimise ja ülevaatuse ning tagab, et rakendatavad infoturbemeetmed on kooskõlas kehtivate nõuetega;
3.3.4 koordineerib infoturbeintsidendi lahendamist asutuses;
3.3.5 teavitab asutuse teenistujaid infoturbe olulisusest ja turvameetmete rakendamise vajalikkusest, tagab, et kõik asutuse teenistujad on oma infoturbealastest kohustustest teadlikud ja nõustab teenistujaid turvameetmete rakendamisel;
3.3.6 korraldab teenistujate infoturbealast esmast ja täiendavat koolitust;
3.3.7 kontrollib, et infoturbealaseid õigusakte ning kohustusi täidetakse ja ei esine infovara volitamata kasutamist;

3.3.8 esitab juhtkonnale ja TEHIKule ülevaateid infoturbe olukorrast, sh turbeprotsessi toimivusest ja tõhususest, turvaintsidentide ja riskide käsitlemisest nii jooksvalt kui kokkuvõtvalt kord aastas;
3.3.9 teeb infoturbe alal koostööd andmekaitsespetsialisti ja väliste osapooltega;
3.3.10 koordineerib infoturbealaseid tegevusi uute protsesside juurutamisel ja olemasolevate protsesside muutmisel, on vajalikul määral kaasatud infoturvet sisaldavate valdkondlike otsuste tegemisse;
3.3.11 osaleb vajadusel IT-projektides ning IT-süsteemide arendusprotsessis.

3.4 Osakonnajuhataja ja valdkonnajuhi kohustuseks on infoturvet reguleerivate õigusaktide täitmise tagamine juhitavas valdkonnas ning infoturbealastest probleemidest teatamine, vastavate ettepanekute tegemine ja tagasiside andmine turbealaste juhendite toimimise kohta.

3.5 Teenistuja vastutab kehtestatud kordade täitmise eest ning tema valduses oleva infovara turvalisuse eest, samuti turvalisuse eest oma teenistus- ja töökohal ning ülesannete täitmisel. Teenistuja võib esitada ettepanekuid turvameetmete kavandamiseks ja rakendamiseks.

3.6 Infovarasid on lubatud kasutada ainult teenistus- või tööülesannete täitmiseks. Infovara juurdepääsuõiguste andmine ja lõpetamine toimub vastavalt *Infovara juurdepääsuõiguste haldamise korrale*. Paberdokumentide, elektrooniliste dokumentide ja elektrooniliste andmekandjate kättesaadavus on tagatud ainult volitatud isikutele.

3.7 Ameti infosüsteemidele määratakse tooteomanikud ametikoha täpsusega. Tooteomanikud omavad ülevaadet infosüsteemi funktsioonidest, tegelevad rikete korral erinevate osapooltega info jagamisega ja panustavad infosüsteemi arendustesse.

3.8 Teadlikud ja põhjendatud kõrvalekaldumised infoturbejuhenditest kooskõlastatakse ameti infoturbe eest vastutava isikuga, kes vajadusel kooskõlastab erandi eelnevalt TEHIKu infoturbejuhiga ja/või ameti juhtkonnaga. Erandid koos põhjendusega dokumenteeritakse ja erandist teavitatakse kõiki asjassepuutuvaid teenistujaid.

3.9 Infoturbealased jääkriskid hinnatakse ja aktsepteeritakse lähtudes ameti juhendist *Riskide haldamise põhimõtted*.

3.10 Infoturvapoliitika ja infoturbe korralduse toimivust, täielikkust ja ajakohasust kontrollitakse regulaarselt läbi sise- ja välisauditite. Siseauditid korraldatakse vastavalt ameti *Auditite planeerimise ja läbiviimise korrale* või ostetakse vastav teenus sisse koostöös TEHIKuga. Välisauditi teenus ostetakse sisse koostöös TEHIKuga.

4. RIIST- JA TARKVARA NING TÖÖVAHENDITE TURVE

4.1 Vajalike IKT vahenditega varustab ametit TEHIK, kes tagab ka IKT vahendites vajalike turbenõuete rakendamise (vt lisaks *Infovara kasutamise kord*).

4.2 TEHIK vastutab riist- ja tarkvara soetamise, paigaldamise, konfigureerimise ja haldamise ning kurivaratõrje programmide eest.

4.3 Teenistujate kohustused töövahendite kasutamisel on toodud *ameti sisekorraeeskirjas* ning *Infovara kasutamise korras*.

5. INFOVAHETUSE TURVE

5.1 Ametis käideldav informatsioon jaguneb avalikuks ning juurdepääsupiiranguga infoks ehk asutusesiseseks kasutamiseks tunnistatud teabeks. Viimane on informatsioon, mis sisaldab eriliigilisi isikuandmeid, isikuandmeid, ärisaladust vms infot.

5.2 Amet töötleb ainult informatsiooni, mis on vajalik õigusaktidega ettenähtud ülesannete täitmiseks ja ameti toimivuse tagamiseks.

5.3 Dokumentide loomise, haldamise, arhiveerimise ja hävitamise nõuded ja juhised ning teabe asutusesiseseks kasutamiseks tunnistamise kord on sätestatud ameti *Dokumendihalduse korras*. Juurdepääsupiiranguga teavet sisaldavad dokumendid on määratletud *Dokumentide liigitusskeemis*. Juurdepääsupiiranguga teabe edastamisel peab olema välistatud andmete tervikluse ja konfidentsiaalsuse kadu.

5.4 Isikuandmete ja eriliigiliste isikuandmete edastamine kolmandatele isikutele peab toimuma vastavalt avaliku teabe seadusele, isikuandmete kaitse üldmäärusele ja muudes õigusaktides sätestatud tingimustele. Ametis peetakse arvestust isikuandmete töötlemistoimingute üle vastavas registris (*register asub S-kettal*).

5.5 Andmekandjatel edastatud dokumentide puhul järgitakse kõiki dokumentidele kehtivaid reegleid, kusjuures andmekandja saaja/saatja on kohustatud täitma täiendavaid turvanõudeid, mis on toodud *Infovara kasutamise korras*. Juurdepääsupiiranguga teave tuleb andmevahetuse jaoks krüpteerida. Pärast andmevahetuse teostamist tuleb informatsioon andmekandjalt turvaliselt kustutada või andmekandja füüsiliselt hävitada.

5.6 Andmete elektroonsel töötlemisel võib kasutada ainult TEHIKu poolt aktsepteeritavaid info- ja kommunikatsioonitehnoloogia vahendeid (nt riistvara, tarkvara, andmekandjad, arvutivõrk jms).

5.7 Ameti sisemise infovahetuse nõuded on reguleeritud ameti *Kommunikatsioonijuhendis*.

5.8 Suulise suhtluse puhul tuleb väljaspool tööruume ja kõrvaliste isikute juuresolekul vältida juurdepääsupiiranguga informatsiooni käsitlevaid teemasid. Juurdepääsupiiranguga informatsiooni käsitlemisel tuleb välistada volitamata isikute pealtkuulamise võimalus.

5.9 Juurdepääsupiiranguga informatsiooni edastamine telefoni teel on keelatud.

5.10 Kõigil töökohtadel tuleb juurdepääsupiiranguga teabe osas järgida nn tühja laua printsiipi, see tähendab, et enne ruumist lahkumist kõrvaldada laualt ja muudest nähtavatest kohtadest kõik vastavaid andmeid sisaldavad dokumendid ja andmekandjad. Juurdepääsupiiranguga teavet sisaldavaid andmekandjaid hoitakse võimalusel lukustatud kapis, sahtlis või seifis. Töökohalt ajutiselt lahkudes tuleb arvuti lukustada ja pikemaks ajaks lahkudes tuleb arvutist välja logida.

6. RUUMIDE TURVE

6.1 Ruumide turbe all peetakse silmas ruumide füüsilist turvet kõige tõenäolisemate ohtude eest, nagu näiteks volitamata sisenemine, ruumide või ruumides paikneva vara väärkasutus või rikkumine, vargused, tule- ja veekahjustused.

6.2 Ametis on kehtestatud korrad ja juhendid, mille eesmärgiks on tagada inimeste, kogu infrastruktuuri ja infovara kaitsmine nimetatud ohtude eest. Ameti ruumide õnnetuste vastased

ennetus- ja kaitsemeetmed ning õnnetuste puhul käitumise juhised on toodud ameti *Toimepidevuse tagamise korras* ning *tuleohutuse juhendites*.

6.3 Ameti ruumide kirjeldused ja nende kasutamise kord on kehtestatud ameti *Sisekorraeeskirjas*, *Toimepidevuse tagamise korras* ja *Dokumendihalduse korras*.

6.4 Sissepääs tööruumidesse on tagatud vastavalt tööalase vajaduse ja vastutuse alusel. Sissepääs toimub kiipkaardiga, mille väljastamise ja tagastamise üle peab dokumenteeritud arvestust üldosakonna sekretär. Teenistujad on kohustatud kiipkaarti ja selle parooli hoidma viisil, mis välistab nende volitamata kasutamise, kadumise või varguse.

6.5 Ruumid on varustatud valvesüsteemiga. Ruumide valvestamise kord on sätestatud ameti *Sisekorraeeskirjas*.

6.6 Tingimused ameti ruumide hooldus- ja remonditöödeks on sätestatud hoone haldajatega sõlmitud lepingutes. Üldjuhul on ruumide haldajatel ja nende volitatud isikutel õigus ruumidesse siseneda enda tööülesannete täitmise eesmärgil (näiteks puhastusteenindajal koristustöödeks jne). Vajadusel sõlmitakse tööde teostajatega eraldi lepingud (nt kui tööd tellitakse kolmandalt osapoolelt vms), kus sätestatakse vajalikud õigused, kohustused ja vastutus.

7. PERSONALI TURVE

7.1 Pädevate ja usaldusväärsete teenistujate värbamiseks on ametis kehtestatud *Värbamise ja valiku kord*. Teenistujate üldised käitumiseeskirjad ja nõuded konfidentsiaalsusele on kirjas ameti *Sisekorraeeskirjas* ja *Käitumiskoodeksis*.

7.2 Kõigile uutele teenistujatele tehakse sissejuhatav ja esmane juhendamine vastavalt *Juhtimissüsteemi käsiraamatus* kehtestatud korrale. Uuele teenistujale tutvustab infoturvet reguleerivaid kordasid, kehtivaid eeskirju ja tegevusjuhiseid ameti infoturbe eest vastutav isik.

7.3 Kõigile teenistujatele võimaldatakse ligipääs ameti ruumidele, seadmetele, infosüsteemidele ja andmetele selles ulatuses, mis on vajalik teenistus- või tööülesannete täitmiseks.

7.4 Teenistuja peab teenistus- või töösuhte ajal ja pärast vabastamist hoidma talle teenistus- ja tööülesannete tõttu teatavaks saanud juurdepääsupiiranguga teavet konfidentsiaalsena.

7.5 Lepinguliste töötajate ja ekspertide puhul lisatakse töövõtu- või käsunduslepingusse asjakohased turvanõuded, sh tähtajatu konfidentsiaalsuskohustus.

7.6 Teenistujate pädevuse hoidmiseks ja tõstmiseks on ametis välja töötatud koolituspõhimõtted, mis on kirjeldatud *Koolituste korras*. Vajaliku turvateadlikkuse taseme saavutamiseks ja hoidmiseks on TEHIK välja töötanud infoturbe e-õppe koolitusprogrammi, mille kõik ameti teenistujad peavad läbima kord aastas.

7.7 Asendamiste kord puhkuste, lähetuste või muude teenistusest või töölt puudumiste korral on kehtestatud põhimääruses, ameti *palgajuhendis* ja peadirektori asendamise käskkirjas, teenistujate ametijuhendites ning asendusskeemis.

7.8 Teenistus- või töösuhte lõppedes tuleb teenistujal viimase tööpäeva lõpuks tagastada kõik tema valduses olevad varad ja pääsuvahendid. Samuti suletakse kõik teenistuja arvutivõrgu ja infosüsteemide kasutajaõigused. Tööks vajalike dokumentide ja informatsiooni kiire ning

efektiivse üleandmise tagamiseks teenistus- või töösuhte lõppemisel või peatumisel on *Dokumendihalduse korras* kehtestatud nõuded asjaajamise üleandmisele.

8. TEGEVUSTE KATKEMATUS

8.1 Amet arvestab oma tööde ja ressursside planeerimisel kõige tõenäolisemate võimalike ohtudega ning võtab mõistlikkuse põhimõttel kasutusele meetmeid ohtude vältimiseks ja asutuse töö jätkumiseks ootamatute takistuste ja rikete korral.

8.2 Ameti tööprotsesside jätkusuutlikkuse tagamiseks on kehtestatud nõuded eeskirjades ja juhendites ning protsessid on kirjeldatud tööjuhendites. Nõudeid kehtestavate dokumentide jaotus ja kirjeldused on esitatud *Juhtimissüsteemi käsiraamatus*. Infosüsteemide puhul lähtutakse lisaks *TEHIKu infosüsteemide talitluspidevuse haldamise korrast*.

8.3 Tööalased tegevused ja oluline info, mille kohta ei ole eraldi reegleid kehtestatud, tuleb teenistujal endal dokumenteerida sellises ulatuses ja vormis, et tema töölt puudumise korral saaks tema asendaja kiiresti tööd jätkata.

8.4 Kõigist ameti andmetest teeb TEHIK perioodiliselt varukoopiaid lähtudes TEHIKu infosüsteemide ja arvutivõrgu varundamist reguleerivatest kordadest.

8.5 Kõikide infosüsteemide kohta on TEHIKul välja töötatud taasteplaanid, mille alusel on võimalik kõiki andmeid taastada. Taasteplaane testitakse regulaarselt.

9. TURVAINTSIDENTIDE KÄSITLEMINE

9.1 Turvaintsidendid võivad esineda näiteks järgmistel juhtudel:
- teenistuja vale käitumine, mille tagajärjeks on andmete kadu või turvakriitiline süsteemiparameetrite muutmine;
- turvaaukude esinemine riist- või tarkvarakomponentides;
- massiline viiruste esinemine;
- internetiserverite ründamine;
- konfidentsiaalsete andmete avalikustamine;
- personali puudumine;
- sissemurdmine, vargus seoses IT-ga.

9.2 Turvaintsidendi avastamisel on teenistuja kohustatud viivitamatult teavitama intsidendist või selle kahtlusest TEHIKu IT-kasutajatuge telefonil 794 3913 või e-postil itabi@tehik.ee ja ameti infoturbe eest vastutavat isikut. Vajadusel tuleb teavitada Häirekeskust telefonil 112.

9.3 Võimaluse ja oskuste korral peab teenistuja võtma tarvitusele vajalikud abinõud turvaintsidendi likvideerimiseks või selle mõju laienemise ärahoidmiseks, seadmata seejuures ohtu enese või teiste isikute elu või tervist.

9.4 Turvaintsidentide vältimiseks tuleb rakendada asjakohased turvameetmed. Intsidente tuleb käsitleda viisil, mis minimeerib ja/või piirab intsidentidest tekkida võivaid kahjusid ning taastab rakenduste ja süsteemide töö võimalikult kiiresti.

9.5 IT-teenuste, seadmete ja tarkvaraga seotud turvaintsidente haldab TEHIK. Ameti muud turvaintsidendid (ruumid, personal vm) käsitleb infoturbe eest vastutav isik, registreerides juhtumi ja vajalikud tegevused Turvaintsidentide registris (Lisa 1).

9.6 Turvaintsidendi lahendamisel selgitatakse esmalt välja juhtumi olemus. Seejärel võetakse koheselt kasutusele hädavajalikud abinõud intsidendi likvideerimiseks või mõju laienemise vältimiseks ning selgitatakse välja intsidendi põhjus. Vajadusel teavitatakse asjaomaseid või intsidendiga seotud isikuid ja normaliseeritakse olukord võimalikult lühikese ajaga. Intsidendi asitõendid säilitatakse ning juhtumiga seotud faktid, kahjustatud vara ja kahju suurus dokumenteeritakse. Lõpetuseks viiakse läbi juhtumi analüüs ja koostatakse intsidendi aruanne. Pärast intsidendi lahendamist rakendatakse parandustoiminguid intsidendi edaspidiseks vältimiseks.

10. INFOTURBEALANE TEAVITUS

10.1 Asutuse infoturbe eest vastutav isik annab vajadusel olulisematest turvaintsidentidest, ilmnenud turvariskidest ja intsidentide ning riskide maandamismeetmete rakendamisest ülevaate asutuse juhtkonna koosolekul.

10.2 Ameti teenistujate operatiivne infoturbealane teavitus toimub ameti siseveebi ja/või sisemise meililisti kaudu. Teatatakse olulistest turvaintsidentidest, turvasituatsiooni muudatustest, teenistujate teenistusse ja tööle võtmisest ja vabastamisest ning pikemaajalistest külastajatest ameti tööruumides.

10.3 IT teenuste infoturbeintsidentidest teeb ametile kvartaalseid ülevaateid TEHIK.

10.4 Iga aasta esimeses kvartalis koostab ameti infoturbe eest vastutav isik ameti juhtkonnale ülevaate infoturbesüsteemi toimivuse kohta tuues välja järgneva:

- eelneval aastal toimunud infoturbealane tegevus,
- eelneval aastal toimunud turvaintsidendid ja nende lahendamine,
- eelneval aastal läbi viidud teenistujate infoturbealased koolitused ja/või juhendamised,
- eelneval aastal läbi viidud E-ITS auditid ja nende ülevaade,
- infoturbealaste kordade ja dokumentatsiooni hetkeseis ning nendes tehtud ja kavandatavad muudatused,
- ettepanekud edasiste infoturbealaste tegevuste osas, sh prioriteedid ja hinnang realiseerimise aja ja töömahu kohta.