KINNITATUD
Ravimiameti peadirektori
veebruari 2025
käskkirjaga nr 19

INFOTURVAPOLIITIKA

SISUKORD

1. EESMÄRK JA ÜLDPÕHIMÕTTED

1.1 Infoturvapoliitika lähtub:
- 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.

1.2 Infoturvapoliitika kehtib kogu Ravimiametis (edaspidi amet) ning selle järgimine on kõigile ameti ametnikele ja töötajatele (edaspidi koos teenistujad) ning käsundus- või muu lepingu alusel teenust osutavatele osapooltelele kohustuslik.

1.3 Infoturvapoliitika kehtestab turvaeesmärgid, turbe strateegia ja rollid kaitsealale, mille sihtobjektideks on kõik ameti protsessid, teenused ja varad. Kaitseala hõlmab ka väliste teenuseandjate pakutavaid IT-teenuseid, kaugjuurdepääse ja tööd kodukontoris või välislähetuses.

1.4 Protsesside, teenuste ja neid teenindavate varade peamised turvariskid ning kaitsetarve on määratud kaitsetarbe protokollides. Turbeviisiks on standardturve. Rakendamata etalonturbe meetmete ja etalonturbe väline riskihaldus toimub vastavalt *Riskide haldamise korrale*.

1.5 Ameti infovarale rakendatakse otstarbekohaseid turvameetmeid koostöös Tervise ja Heaolu Infosüsteemide Keskusega (TEHIK), lähtudes ameti ja TEHIKu vahelisest lepingust, teenustaseme kokkulepetest (SLA) ja toimemudelist.

1.6 Turvameetmete planeerimisel ja rakendamise prioriteetide ja teostusjärjekorra määramisel 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.

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 halduse süsteem (*Information Security Management System*, edaspidi ISMS) – ameti juhtimissüsteemiga integreeritud süstemaatiline lähenemine infoturbe rajamisele, käigus hoiule, seirele ja täiustamisele, et maandada riske, kaitsta infovara, tagada põhitegevuse jätkusuutlikkus ja saavutada eesmärgid.

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

2.6 Juurdepääsupiiranguga teave – 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 kaitsetarbe protokollide 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 ja koostöös TEHIKuga;

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 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 korraldab riskide hindamise, kooskõlastab erandi eelnevalt TEHIKu infoturbejuhiga ja/või ameti juhtkonnaga. Erandid koos põhjendusega dokumenteeritakse ja erandist teavitatakse kõiki asjassepuutuvaid teenistujaid.

3.9 Infoturbealased riskid hinnatakse, maandatakse ja aktsepteeritakse lähtudes ameti *Riskide haldamise korrast*.

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.

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*. Kasutusjuhendid (printerid, konverentsiseadmed jm) on kättesaadavad siseveebist ja IT-abi KKKst iga teenistuja sülearvuti töölaualt.

5. INFOVAHETUSE TURVE

5.1 Amet töötleb ainult informatsiooni, mis on vajalik õigusaktidega ettenähtud ülesannete täitmiseks ja ameti toimivuse tagamiseks. Ametis käideldav informatsioon jaguneb avalikuks, juurdepääsupiiranguga infoks ehk asutusesiseseks kasutamiseks tunnistatud teabeks ning konfidentsiaalseks infoks. Viimane on informatsioon, mis sisaldab eriliigilisi isikuandmeid, isikuandmeid või ärisaladust.

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

5.3 Enne teabe edastamist asutusevälisele partnerile veendutakse vastuvõtja õigustes teavet vastu võtta ja töödelda. Enne konfidentsiaalse teabe edastamist teavitatakse vastuvõtjat, et teave on mõeldud kasutamiseks ainult ette nähtud eesmärgil. Konfidentsiaalne teave tuleb krüpteerida või küsida andmesubjekti nõusolek krüpteerimata kujul teabe edastamiseks.

5.4 Isikuandmete ja eriliigiliste isikuandmete edastamine kolmandatele isikutele peab toimuma vastavalt avaliku teabe seadusele, isikuandmete kaitse üldmäärusele ja muudes seadustes 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*. Konfidentsiaalne 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 Koosolekul või koolitusel tehtava esitluse eel suletakse võimaliku juhusliku andmelekke vältimiseks kõik mittevajalikud rakendused ja andmesideühendused. Pärast koosoleku või ürituse lõppu võetakse kaasa või kõrvaldatakse turvaliselt kõik tundlikku teavet sisaldada võivad materjalid.

5.11 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 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 ohuolukordade vastased ennetus- ja kaitsemeetmed ning käitumise juhised on toodud ameti *Toimepidevuse tagamise korras* ning *tuleohutuse juhendites*.

6.3 Ameti ruumide kirjeldused, nende kasutamise ja valvestamise kord on kehtestatud ameti *Sisekorraeeskirjas*, *Toimepidevuse tagamise korras* ja *Dokumendihalduse korras*. Ruumide valvestamise *tehniline juhend on kättesaadav siseveebis.*

6.4 Sissepääs tööruumidesse on tagatud tööalase vajaduse ja vastutuse alusel. Sissepääs toimub kiipkaardi või võtmega, mille väljastamise ja tagastamise üle peab dokumenteeritud arvestust sekretär. Teenistujad on kohustatud võtmeid, kiipkaarti ja selle parooli hoidma viisil, mis välistab nende volitamata kasutamise, kadumise või varguse. Kadumise või varguse korral tuleb koheselt teavitada sekretäri, kes korraldab blokeerimise ja/või asendamise.

6.5 Külastajad pääsevad vastuvõturuumi ja koosolekuruumidesse, sissepääs tööruumidesse on lubatud vaid saatjaga. Enam kui 1 tööpäeva pikkused külastused registreeritakse ja väljastatakse külaliskaart.

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*. Enne lõppvalikut teeb personalispetsialist kandidaadi nõusolekul vajadusel tema kohta eelneva taustauuringu. Lepinguliste töötajate ja ekspertide puhul lisatakse töövõtu- või käsunduslepingusse asjakohased turvanõuded, sh tähtajatu konfidentsiaalsuskohustus, ametnikud allkirjastavad konfidentsiaalsuskokkuleppe.

7.2 Kõigile uutele teenistujatele tehakse sissejuhatav ja esmane juhendamine vastavalt *Kvaliteedikäsiraamatus* kehtestatud korrale. Teenistujate üldised käitumiseeskirjad ja nõuded konfidentsiaalsusele on kirjas ameti *Sisekorraeeskirjas* ja *Käitumiskoodeksis*. 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 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 infovara kasutavad (sh ka püsivalt kaugtööl ja pikaajalises välislähetuses viibivad) teenistujad peavad läbima teenistusse asudes 2 nädala jooksul ja edaspidi kord aastas.

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

7.7 Teenistus- või töösuhte lõppedes tuleb teenistujal viimase tööpäeva lõpuks tagastada kõik tema valduses olevad varad ja pääsuvahendid. Samuti suletakse kõik teenistuja võrgu ja infosüsteemide kasutajaõigused. Tööks vajalike dokumentide ja informatsiooni kiire ning efektiivse üleandmise tagamiseks teenistus- või töösuhte lõppemisel või peatumisel on aluseks *Dokumendihalduse korras* kehtestatud nõuded.

8. VÄLISLÄHETUSTE TURVE

8.1 Teise riiki minemisel transporditakse seadmeid, tagades kontrolli seadme üle ja alalise teadmise seadmete hetkeasukohast (nt lennukis käsipagasis).

8.2 Juurdepääsupiiranguga ja konfidentsiaalset teavet töödeldakse välislähetuses olles vaid privaatvõrgus (VPN). Võimalusel kasutatakse võrguühenduseks ainult telefoni kuumkoha jagamist. Seadmete Bluetooth ühendus peab olema alaliselt väljalülitatud.

8.3 Kui sihtkohariigis ei ole võimalik tagada andmekandjate hävitamist ettenähtud viisil, hoitakse need tagasipöördumiseni alles ning hävitatakse või utiliseeritakse vastavalt *Dokumendihalduse korras* ettenähtud nõuetele.

8.4 Reisides Hiina Rahvavabariiki, Venemaa Föderatsiooni, Valgevene Vabariiki või Korea Rahvademokraatlikusse Vabariiki või nende riikide mõjusfääris olevatesse piirkondadesse (Transnistriasse, Krimmi, Ida-Ukrainasse, Abhaasiasse või Lõuna-Osseetiasse), tuleb sülearvuti kaasavõtmine kooskõlastada vahetu juhi, infoturbe eest vastutava isiku ja IT-abiga, vajaduse kinnitamisel väljastatakse asendusarvuti.

9. VÄLJASTTELLIMISE TURVE

9.1 Amet tellib tooteid ja teenuseid vastavalt *Hankekorrale*, hankeplaanile, *IT arenduste haldamise korrale*, TEHIKuga sõlmitud teenuslepingule ja Sotsiaalministeeriumi digiarenduste koordineerimise protsessile.

9.2 Väljasttellimisel hinnatakse võimalikke riske, arvestatakse seonduvate andmete ja infovara kaitsetarvet, asjakohaseid turbemeetmeid ja nõudeid kaalutakse võimalike pakkujate valikul ja seatakse tingimus(t)eks lepingupartneri(te)le.

9.3 Väliste partnerite loetelu, suhtlusteed, kokkulepped ja kvaliteedinõuded on toodud dokumendihaldussüsteemis registreeritud lepingutes, siseveebis ja/või ameti *Infovara registris* (*Infovara juurdepääsuõiguste haldamise korra* Lisa 1).

9.4 Väljasttellimise tulemuslikkust hinnatakse ameti ja TEHIKu korralistel koosolekutel, juhtkonna iganädalastel koosolekutel, juhtkonna arengupäeval või vajaduspõhiselt.

10. TEGEVUSTE KATKEMATUS

10.1 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.

10.2 Ameti tööprotsesside jätkusuutlikkuse tagamiseks on kehtestatud nõuded eeskirjades ja juhendites ning kirjeldatud tööjuhendid. Nõudeid kehtestavate dokumentide jaotus ja kirjeldused on esitatud *Kvaliteedikäsiraamatus*.

10.3 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.

10.4 Infovara asukoha muutmisel või kolimisel hinnatakse turvameetmete vajadust, teavitatakse teenistujaid ja teenusepakkujaid, kontrollitakse infovara seisundit ja testitakse toimimist uues asukohas.

10.5 Kõigist ameti andmetest teeb TEHIK perioodiliselt varukoopiaid. Kõikide infosüsteemide kohta on TEHIKul välja töötatud taasteplaanid, mille alusel on võimalik kõiki andmeid taastada. Taasteplaane testitakse regulaarselt.

11. TURVAINTSIDENTIDE KÄSITLEMINE

11.1 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;
- õngitsus, sissemurdmine, vargus.

11.2 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.

11.3 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. Esmased juhised turvaintsidentide korral tegutsemiseks on toodud *Toimepidevuse tagamise korras.*

11.4 IT-teenuste, seadmete ja tarkvaraga seotud turvaintsidente haldab ja asjakohase info ametile edastab TEHIK. Ameti muud turvaintsidendid (ruumid, personal vm) käsitleb infoturbe eest vastutav isik, registreerides juhtumi ja vajalikud tegevused Turvaintsidentide registris (Lisa 1). Üldjuhul liigitatakse intsidendid olemuse (käideldavus, konfidentsiaalsus või terviklus) ja prioriteetsuse (madal, keskmine, kõrge) alusel.

11.5 Turvaintsidendi lahendamisel selgitatakse esmalt välja juhtumi olemus. Seejärel võetakse koheselt kasutusele hädavajalikud abinõud intsidendi likvideerimiseks või mõju piiramiseks ning selgitatakse välja intsidendi põhjus. Vajadusel teavitatakse asjaomaseid või intsidendiga seotud isikuid ja kogutakse täiendavat infot, nt logiandmete analüüs vm. Käsitlemise käigus püütakse minimeerida tekkida võivaid kahjusid ning taastada rakenduste ja süsteemide töö võimalikult kiiresti. Intsidendi asitõendid säilitatakse ning juhtumiga seotud faktid, kahjustatud vara ja kahju suurus dokumenteeritakse. Rakendatakse kõik asjakohased toimingud ja turvameetmed intsidendi edaspidiseks vältimiseks.

11.6 Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo või distsiplinaarsüüteo tunnused, kaasab infoturbe eest vastutav isik andmekaitsespetsialisti, õigusosakonna juhataja ja peadirektori ning korraldab vajadusel juhtumi edasiandmise vastava menetluse läbiviimise õigust omavale asutusele (Andmekaitse Inspektsioon, Politsei- ja Piirivalveamet vm).

12. INFOTURBEALANE TEAVITUS

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

12.2 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.

12.3 IT teenuste infoturbeintsidentidest teeb ametile ja vajadusel CERT-EEle ülevaateid TEHIK.

12.4 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.