KINNITATUD
Ravimiameti peadirektori
juuli 2026
käskkirjaga nr 24

INFOTURVAPOLIITIKA

SISUKORD

1. EESMÄRK JA ÜLDPÕHIMÕTTED

1.1 Infoturvapoliitika eesmärk on määratleda infoturbe põhimõtted, rollid ja vastutused, et kaitsta teavet, infosüsteeme ja teenuseid volitamata kasutamise, muutmise, avalikustamise, katkestuste või hävimise eest, tagada õiguslike ja lepinguliste nõuete täitmine ning vähendada infoturberiskidest tulenevat mõju.

1.2 Infoturvapoliitika lähtub:
- 1.2.1 Küberturvalisuse seadusest;
- 1.2.2 Vabariigi Valitsuse 09. detsembri 2022. a määrusest nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“;
- 1.2.3 Vabariigi Valitsuse 03. jaanuari 2024. a määrusest nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“;
- 1.2.4 Vabariigi Valitsuse 15. märtsi 2012. a määrusest nr 26 „Infoturbe juhtimise süsteem“;
- 1.2.5 Eesti infoturbestandardi (E-ITS) kehtivast versioonist;
- 1.2.6 Isikuandmete kaitse üldmäärusest ja avaliku teabe seadusest.

1.3 Infoturvapoliitika järgimine on kõigile Ravimiameti (edaspidi amet) ametnikele ja töötajatele (edaspidi koos teenistujad) ning käsundus- või muu lepingu alusel teenust osutavatele osapooltele kohustuslik.

1.4 Infoturvapoliitika kehtestab kaitseala turvaeesmärgid, turbestrateegia ja rollid. Kaitseala hõlmab kogu ameti vastutusalas olevat tegevust, sh ka väliste teenuseosutajate pakutavaid IT-teenuseid, kaugjuurdepääse ja tööd kodukontoris või välislähetuses.

1.5 Kaitseala sihtobjektide turvariskid ning kaitsetarve on määratud ja dokumenteeritud kaitsetarbe protokollides. Rakendatakse standardturvet ja riskipõhiselt kõrgendatud turvet.

Etalonturbe meetmete rakendamine, rakendamata jätmise põhjendamine ja riskihaldus toimub vastavalt *Riskide haldamise korrale*.

1.6 Ameti infovarale rakendatakse otstarbekohaseid turvameetmeid koostöös teenuseosutajatega, lähtudes ameti ja teenuseosutajate vahelistest lepingutest ja teenustaseme kokkulepetest (SLA).

1.7 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 tegevuseesmärkidele 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 andmekogud, infosüsteemid, rakendused jm infotehnoloogilised 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 Juurdepääsupiiranguga teave – teave ja andmed, millele on kehtestatud juurdepääsupiirang lepingu või seaduse alusel, sisaldab asutusesiseseks kasutamiseks määratletud teavet, eriliigilisi isikuandmeid ja ärisaladust.

2.6 Sihtobjekt – objekt, mida kaitstakse ja millele infoturvet rakendatakse (nt protsess, teenus, andmekogu, infosüsteem, rakendus, töökoht, ruum vm).

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

2.8 Äriprotsessi omanik – isik, kes vastutab äriprotsessi (teenuse) toimimise ja tulemuslikkuse eest ning määrab äriprotsessiga (teenusega) seotud sihtobjektide turvanõuded.

3. INFOTURBE KORRALDUS JA VASTUTUS

3.1 Ameti üldised 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 tagada teenistujate infoturbealane teadlikkus ja usaldusväärsete teenuseosutajate kasutamine;
- 3.1.4 säilitada ameti kuvand.

Täpsemad eesmärgid lepitakse kokku iga-aastase tööplaanide koostamise käigus.

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 teenuseosutajatega;
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 infoturbe riskide hindamiseks vajadusel IT-projektides, uue infovara või teenuseosutaja kasutuselevõtul ning IT-süsteemide arendusprotsessis.

3.4 Osakonnajuhataja, valdkonnajuhi ja äriprotsessi omaniku 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. Tooteomanikud omavad ülevaadet infosüsteemi funktsioonidest, tegelevad rikete korral erinevate osapooltega info jagamisega ja panustavad infosüsteemi arendustesse.

3.8 Teadlikud ja põhjendatud kõrvalekaldumised infoturbejuhenditest või -meetmetest tuleb kooskõlastada ameti infoturbe eest vastutava isikuga, kes vajadusel korraldab riskide hindamise koos teenuseosutaja ja/või ameti juhtkonnaga. Erandid koos põhjendusega dokumenteeritakse riskiregistris ja erandist teavitatakse kõiki asjassepuutuvaid teenistujaid. Riskiregistris hoitakse erandite ülevaadet kuni kehtivuse lõppemiseni, vajadus ja sellega kaasnevad riskid hinnatakse üle vähemalt kord aastas.

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*. Välisauditi teenus ostetakse sisse koostöös Tervise ja Heaolu Infosüsteemide Keskusega (TEHIK).

4. VÄLJASTTELLIMISE TURVE

4.1 Amet tellib infovara vastavalt *Hankekorrale*, hankeplaanile, *Infovara kasutuselevõtu ja arendamise korrale*, teenuseosutajatega sõlmitud teenuslepingutele ja Sotsiaalministeeriumi digiarenduste koordineerimise protsessile.

4.2 Väljast tellimisel hinnatakse võimalikke riske, arvestatakse andmete ja infovara kaitsetarvet. Asjakohaseid turbemeetmeid ja nõudeid kaalutakse võimalike pakkujate valikul ja seatakse tingimus(t)eks lepingupartneri(te)le.

4.3 Pilveteenuste ja tehisintellekti rakenduste väljast tellimine on lubatud:

- läbi riigi IT-maja (TEHIK, RIT) või EL pädevate asutuste võrgustiku - madal risk, võib tugineda teenuseandja riski- ja andmekaitse mõjuhinnangutele, või
- teiste heakskiidetud teenuseandjate kaudu - kõrge risk, peab olema RA enda poolt koostatud riski- ja/või andmekaitsealane mõjuhinnang, teenuseandja usaldusväärsuse hinnang, tagatud EL õigusruumi nõuete täitmine teenuseandja poolt.

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

4.5 Väljast tellimise tulemuslikkust hinnatakse ameti ja teenuseosutaja vahelistel koosolekutel või muu infovahetuse tulemusena, juhtkonna iganädalastel koosolekutel, juhtkonna arengupäeval või vajaduspõhiselt.

4. INFOVARA TURVE

4.1 Infovara tehniliste turbenõuete rakendamise tagab teenuseosutaja.

4.2 Teenistujate kohustused infovara kasutamisel on toodud ameti *Sisekorraeeskirjas* ning *Infovara kasutamise korras*. Kasutusjuhendid (printerid, konverentsiseadmed jm) on kättesaadavad siseveebist ja IT-abi rakendusest 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 ja 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 toimub vastavalt avaliku teabe seadusele, isikuandmete kaitse üldmäärusele ja muudes seadustes sätestatud tingimustele. Ametis peetakse arvestust eriliigiliste isikuandmete töötlemistoimingute üle vastavas registris, mida haldab andmekaitsespetsialist.

5.5 Välised digitaalsed andmekandjad on vaikimisi keelatud. Vältimatul vajadusel võib kasutamise taotleda, lubatud on ainult Riigi IT Keskuse (RIT) poolt heaks kiidetud vahendid. 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 andmevahetust tuleb informatsioon andmekandjalt turvaliselt kustutada või andmekandja füüsiliselt hävitada.

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

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

5.8 Eriliigiliste isikuandmete ja muu konfidentsiaalse või juurdepääsupiiranguga informatsiooni edastamine telefoni teel on keelatud.

5.9 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.

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

6. RUUMIDE TURVE

6.1 Ametis on kehtestatud korrad ja juhendid, mille eesmärgiks on tagada inimeste, kogu infrastruktuuri ja infovara kaitsmine füüsiliste ohtude eest (näiteks volitamata sisenemine, ruumide või ruumides paikneva vara väärkasutus või rikkumine, vargused, tule- ja veekahjustused). Ameti ruumide ohuolukordade vastased ennetus- ja kaitsemeetmed ning käitumise juhised on toodud ameti *Toimepidevuse tagamise korras* ning *tuleohutuse juhendites*.

6.2 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.

6.3 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 koostöös teenusepakkujaga (Tartu Ülikool).

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

6.5 Tingimused ameti ruumide hooldus- ja remonditöödeks on sätestatud hoone haldajaga sõlmitud lepingutes. Üldjuhul on ruumide haldajal ja 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.

6.6 Ameti ruumides asuvale infovarale juurdepääsu korral peavad välised teenuseosutajad allkirjastama konfidentsiaalsuskohustuse kinnituse (vt lisa 1) või tõendama teenuslepingu raames juba allkirjastatud konfidentsiaalsuskohustust.

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 peavad kõik ameti infovara kasutavad (sh ka püsivalt kaugtööl ja pikaajalises välislähetuses viibivad) teenistujad läbima infoturbealase koolituse teenistusse asudes 2 nädala jooksul ja edaspidi kord aastas. Ameti peadirektor läbib lisaks kord aastas infoturbealaste riskide teadvustamise ja juhtimisega seotud koolituse (nt Digiriigi Akadeemia) küberturvalisuse seaduse tähenduses.

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 Reisimise vaates jagunevad riigid kolmeks: lubatud riigid (EL, NATO ja OECD), keelatud riigid (Hiina Rahvavabariik, Venemaa Föderatsioon, Valgevene Vabariik, Korea Rahvademokraatlik Vabariik või nende riikide mõjusfääris olevad piirkonnad) ja riigid, kuhu reisides on tarvis luba taotleda ja kus on võimalik piiratud kujul teenuse kasutamine.

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

8.3 Juurdpääsupiiranguga ja konfidentsiaalse teabe töötlemisel kasutatakse võimalusel võrguühenduseks ainult telefoni kuumkoha jagamist. Seadmete sinihamba ühendus peab olema alaliselt väljalülitatud.

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

9. TEGEVUSTE KATKEMATUS

9.1 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.

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

9.3 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.

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

9.5 Kõigist ameti andmetest teevad teenuseosutajad perioodiliselt varukoopiaid. Kõikide infosüsteemide kohta on välja töötatud taasteplaanid, mille alusel on võimalik kõiki andmeid taastada. Taasteplaane testitakse regulaarselt.

10. TURVAINTSIDENTIDE KÄSITLEMINE

10.1 Turvaintsidendi avastamisel on teenistuja kohustatud viivitamatult teavitama intsidendist või selle kahtlusest RIT IT-kasutajatuge telefonil 663 6464 või e-postil itabi@rit.ee (arvutitöökohateenus) või TEHIKu IT-kasutajatuge telefonil 794 3913 või e-postil itabi@tehik.ee (infosüsteemid) ja ameti infoturbe eest vastutavat isikut. Vajadusel tuleb teavitada Häirekeskust telefonil 112.

10.2 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.*

10.3 Tehnilisi turvaintsidente haldavad ja asjakohase info ametile edastavad teenuseosutajad. Ametis tuvastatud turvaintsidendid (ruumid, personal vm) käsitleb infoturbe eest vastutav isik, registreerides juhtumi ja vajalikud tegevused Turvaintsidentide registris (Lisa 2). Üldjuhul liigitatakse intsidendid olemuse (käideldavus, konfidentsiaalsus või terviklus) ja mõju prioriteetsuse (madal, keskmine, kõrge) alusel.

10.4 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.

10.5 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).

11. INFOTURBEALANE TEAVITUS

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

11.2 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.

11.3 Infosüsteemide infoturbeintsidentidest teeb ametile ja vajadusel CERT-EEle ülevaateid TEHIK, arvutitöökohateenusega seonduvalt RIT. Muus osas teavitab amet CERT-EEd ise veebikeskkonnas raport.cert.ee või saates e-kirja cert@cert.ee.

11.4 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 eesmärgid, prioriteedid ja hinnang realiseerimise aja ja töömahu kohta.

Lisa 1. Konfidentsiaalsuskohustuse kinnitus

KONFIDENTSIAALSUSKOHUSTUSE KINNITUS

Mina, [*Ees- ja perekonnanimi*], [*isikukood*],[*Ettevõtte nimi*] (edaspidi „Teenuseosutaja“) esindaja / töötaja kinnitan käesolevaga, et seoses [Ravimiameti, registrikood 70003477], (edaspidi „Tellija“) juures hanke või tellimuse korras töö teostamisega Tellija ruumides või infosüsteemides kohustun järgima konfidentsiaalsusnõudeid alljärgnevalt:

1. Konfidentsiaalne teave. Pean konfidentsiaalseks kogu teavet, mis mulle töö teostamise käigus teatavaks saab ja mis ei ole avalik, sealhulgas:

- isikuandmed (sh eriliigilised isikuandmed);
- analüüside tulemused, analüüsitavate ravimite informatsioon, labori metoodikad;
- informatsioon Tellija töötajate või klientide kohta;
- ärisaladus (sh igasugune Tellijat, teisi pädevaid asutusi või ettevõtteid puudutav tehniline, kaubanduslik või organisatsiooniline teave);
- süsteemid ja juurdepääsud;
- muu teave, mida mõistlikult võib pidada konfidentsiaalseks.

2. Kohustused. Kinnitan, et:

- kasutan konfidentsiaalset teavet üksnes Tellijale töö teostamiseks;
- ei avalda ega edasta konfidentsiaalset teavet kolmandatele isikutele ilma Tellija eelneva kirjaliku loata;
- ei tee fotosid, videoid ega muid salvestisi ilma Tellija eelneva kirjaliku loata;
- hoian saladuses kõik töö käigus teatavaks saanud isikuandmed ja ärisaladuse;
- rakendan asjakohaseid meetmeid teabe kaitseks ning väldin loata juurdepääsu, avalikustamist või muutmist;
- tagan, et kõik minu poolt kaasatud töötajad ja/või koostööpartnerid, kes osalevad Tellija juures töö teostamisel, on käesolevas dokumendis sätestatud nõuetest teadlikud ja järgivad neid;
- teavitan viivitamata Tellijat, kui mulle saab teatavaks konfidentsiaalsuskohustuse rikkumine või oht selleks;
- töö lõpetamisel tagastan Tellijale koheselt kõik töö käigus saadud materjalid ja andmed (dokumendid, koopiad, digitaalsed andmed jms) või hävitan need Tellija juhiste kohaselt.

3. Isikuandmete ja ärisaladuse kaitse. Kinnitan, et töötlen isikuandmeid üksnes töö teostamise eesmärgil ning kooskõlas kehtivate õigusaktidega, sealhulgas avaliku teabe seaduse (AvTS), isikuandmete kaitse seaduse (IKS), isikuandmete kaitse üldmäärusega (GDPR) ja ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadusega (EKTÄKS).

4. Kohustuse kehtivus. Käesolev konfidentsiaalsuskohustus jõustub allkirjastamisest ning kehtib tähtajatult. Kohustus ei lõppe teenuse osutamise lepingu lõppemisega v.a kui teave muutub avalikuks seaduslikul viisil.

5. Vastutus. Olen teadlik, et konfidentsiaalsuskohustuse rikkumise korral vastutan tekitatud kahju eest vastavalt kehtivale õigusele.

Kinnitan, et olen eeltoodust aru saanud ja kohustun seda täitma.

Allkiri:
Nimi:
Kuupäev: