

## INFOTURBEPOLIITIKA

### SISUKORD

1.	EESMÄRK JA ÜLDPÕHIMÕTTED .....	1
2.	MÕISTED .....	2
3.	ORGANISATSIOON.....	3
4.	RUUMIDE TURVE .....	3
5.	TÖÖVAHENDITE TURVE .....	4
6.	INFOVAHETUSE TURVE .....	4
7.	PERSONALITURVE.....	4
8.	TEGEVUSTE KATKEMATUS .....	5
9.	INFOTURBEALANE TEAVITUS .....	5
10.	INFOTURBE DOKUMENTATSIOON .....	6

### 1. EESMÄRK JA ÜLDPÕHIMÕTTED

- 1.1 Infoturbe eesmärk on tagada Ravimiameti (edaspidi „amet“) infovarade turvalisus ja säilimine sellises ulatuses, et amet saaks kõige tõenäolisemate ohtude tingimustes tegutseda oma põhiülesannete täitmisel normaalselt ja katkestusteta.
- 1.2 Infoturbepoliitika kirjeldab ameti infovarade kaitse korraldamise põhimõtteid.
- 1.3 Infoturbepoliitika kehtib kogu ameti töö korraldamisel ning teiste asutuste või isikutega suhtlemisel. Kõiki turvanõudeid arvestatakse ka teenuste, tarkvara, inventari ja muu vara sisseostmisel. IT-teenuste sisseostmise nõuded on toodud IT-teenindamise eeskirja lisas 4 „IT-teenuste ostmise kord“.
- 1.4 Infoturbealaste riskide analüüsi ning infoturbemeetmete valimise, rakendamise, halduse ja kontrolli aluseks on Vabariigi Valitsuse 20. detsembri 2007. a määrusega nr 252 “Infosüsteemide turvameetmete süsteem” kehtestatud infosüsteemide kolmeastmeline etaloniturbe süsteemi (ISKE) uusim versioon ja Vabariigi Valitsuse 15. märtsi 2012. a määrus nr 26 „Infoturbe juhtimise süsteem“.
- 1.5 Turvameetmete planeerimisel ja rakendamisel arvestatakse, et need oleks majanduslikult õigustatud ja proportsioonis võimaliku kahjuga, mis võib tekkida meetmete puudulikkuse tõttu, ning et nende häiriv toime ameti tegevusele ning ameti ametnike ja töötajate (edaspidi koos nimetatud „teenistujad“) tööle oleks võimalikult väike.
- 1.6 Turvameetmed vaadatakse üle ja korrigeeritakse vähemalt kord aastas ja iga kord, kui tehakse suuremaid muudatusi IT-lahendustes, infrastruktuuris või organisatsioonis.
- 1.7 Kõiki infovarasid on lubatud kasutada ainult teenistus- või tööülesannete täitmiseks. Infovarade kasutamisoigused antakse töölase kasutamisevajaduse alusel.
- 1.8 Andmetele määratakse andmekogude kaupa individuaalsed andmete omanikud. Vastav teave dokumenteeritakse andmekogude kaardistuses.

- 1.9 Teadlikud ja põhjendatud kõrvalekaldumised infoturbejuhenditest kooskõlastatakse turbejuhiga, kes vajadusel kooskõlastab erandi eelnevalt IT-teenindajate ja/või juhtkonnaga. Erandid koos põhjendusega dokumenteeritakse ja erandist teavitatakse kõiki asjassepuutuvaid teenistujaid.
- 1.10 Turvanõuete järgimine on kõigile teenistujatele ja lepingulistele töötajatele kohustuslik. Turvanõuete rikkumisel kohaldatakse süüdlasele karistus vastavalt õigusaktidele.

## 2. MÕISTED

- 2.1 Infoturve ehk andmekaitse tähendab andmete kolme põhiomaduse – tervikluse, käideldavuse ja konfidentsiaalsuse tagamist, kus:
- 2.1.1 käideldavus tähendab informatsiooni kasutuskõlblikkust ja õigeaegset kättesaadavust volitatud isikule;
- 2.1.2 terviklus tähendab, et info pärineb autentsest allikast ning seda ei ole volitamatu muudetud ega kustutatud;
- 2.1.3 konfidentsiaalsus tähendab, et informatsioon on kättesaadav vaid volitatud isikutele.
- 2.2 Infovarad – ameti töö jaoks vajalik vara, sh andmed, andmebaasid, rakendustarkvara, süsteemitarkvara, arvutid, serverid, andmekandjad jmt.
- 2.3 Andmete omanik ehk peakasutaja – isik, kes vastutab andmete eest terve nende elutsükli jooksul (mh andmete töötlemise korraldamise ja vastava infosüsteemi administreerimise delegeerimise eest).
- 2.4 Turvaintsident – sündmus, mis võib oluliselt takistada ameti tööd või tekitada varalist kahju. Turvaintsidentid võivad esineda näiteks järgmistel juhtudel:
- kasutaja 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, väljapressimine seoses IT-ga.
- 2.5 Infoturbeintsidentiks loetakse kõiki reaalse või potentsiaalse kahju juhtumeid, mis võivad ohustada või halvata infovara turvalisust, põhjustades nende käideldavuse (töökindlus), tervikluse (andmete õigsuse ja muutumatuse) või konfidentsiaalsuse (andmete salastatuse) kao. Infoturbeintsidentideks loetakse muuhulgas ka toimingud, mis ei ole infoturbe valdkonda reguleerivate õigusaktidega kooskõlas.
- 2.6 Konfidentsiaalseks ehk avaldamisele mitte kuuluvaks teabeks peetakse selliseid andmeid, millele on juurdepääs lepingu või seaduse alusel või mis on mõnel muul alusel kuulutatud mitteavalikuks.

### **3. ORGANISATSIION**

- 3.1 Koguvastutus ameti infoturbe eest on peadirektoril.
- 3.2 Ameti infoturbe infrastruktuur peab tagama optimaalsed kulutused turvanõuete täitmiseks ja varade kaitseks.
- 3.3 Infoturbe jääkriskid hinnatakse vastavalt punktile 9.5.
- 3.4 Üldise IT-turvalisuse eest vastutab ametis peadirektori poolt määratud turbejuht, kelle ülesanded on:
- infoturbe ja selle järelevalve järjepidev planeerimine ja korraldamine, sh infoturbealaste ettepanekute tegemine juhtkonnale;
  - infoturbealase dokumentatsiooni koostamine ja kaasajastamine, sh regulaarne ülevaatamine vähemalt kord aastas;
  - ISKE rakendusjuhendi alusel organisatsiooniliste, füüsiliste ja infotehnoloogiliste turvameetmete rakendamise järjepidev korraldamine;
  - turvajuhenditest kõrvalekaldumiste vajaduse ja põhjendatuse analüüs ja kooskõlastamine ning vastavate erandite dokumenteerimine;
  - infoturbealase teadlikkuse tõstmise korraldamine ametis;
  - infoturbeintsidentide menetlemine;
  - juhtkonnale, sotsiaalministeeriumile ja Riigi Infosüsteemi Ametile aruannete esitamine turvaintsidentide ja turbealase tegevuse kohta;
  - teiste õigusaktides sätestatud infoturbe ülesannete täitmine.

### **4. RUUMIDE TURVE**

- 4.1 Ruumide turbe all peetakse silmas ruumide füüsilist turvet kõige tõenäolisemate ohtude eest, nagu volitamata sisenemine, ruumide või ruumides paikneva vara väärkasutus või rikkumine, vargused, tule- ja veekahjustused jms.
- 4.2 Ametis on kehtestatud korrad ja juhendid, mille eesmärgiks on tagada inimeste, kogu infrastruktuuri ja infovarade kaitsmine nimetatud ohtude eest.
- 4.3 Ameti ruumide kirjeldused ja nende kasutamise kord on kehtestatud sisekorraeeskirjas ja kvaliteedikäsiraamatus, serveriruumide kasutamise kord IT-teenindamise eeskirjas, arhiiviruumi kasutamine asjaajamiskorras.
- 4.4 Ameti ruumide õnnetuste vastased ennetus- ja kaitsemeetmed ning õnnetuste puhul käitumise juhised on toodud ameti õnnetusjuhtumite korral tegutsemise juhendis ja tuleohutuse juhendites.
- 4.5 Tingimused ameti ruumide hooldus- ja remonditöödeks on sätestatud hoone haldajaga sõlmitud lepingus.
- 4.6 Haldajaga sõlmitud lepinguga katmata hoolde- ja remondipersonal lubatakse töid teostama pärast vastavate lepingute allakirjutamist, kus on sätestatud töövõtja ja tellija kohustused (sh konfidentsiaalsuskohustus), õigused ja vastutus.
- 4.7 Väikesemahuliste ja avariitööde puhul piisab suulisest leppest ning töö teostajale kehtivad kõik sisekorraeeskirjas toodud külastajate puhul rakendatavad meetmed.
- 4.8 Korraga antakse töödeks ligipääs ainult minimaalselt vajalikule arvule ruumidele.

## **5. TÖÖVAHENDITE TURVE**

- 5.1 Amet varustab kõik teenistujad vajalike töövahenditega, mille soetamise, kasutuskorda seadmise, hooldamise ja kasutusest kõrvaldamisega tegeleb üldosakond, võttes arvesse käesolevas dokumendis, IT-teenindamise eeskirjas ja ameti hankekorras sätestatud.
- 5.2 Kasutajate kohustused töövahendite kasutamise osas on toodud sisekorraeeskirjas ja IT-teenuste kasutamise eeskirjas.
- 5.3 Juurdepääsupiiranguga teavet sisaldavaid dokumente ja andmekandjaid ning väikesemõõtmelisi väärtuslikke füüsilisi varasid hoitakse võimalusel lukustatud kapis või sahtlis.

## **6. INFOVAHETUSE TURVE**

- 6.1 Dokumentide loomise, haldamise ja turvalise hävitamise nõuded ja juhised on sätestatud ameti asjaajamiskorras.
- 6.2 Andmekandjatel edastatud dokumentide puhul järgitakse kõiki dokumentidele kehtivaid reegleid, kusjuures andmekandja saaja/saatja on kohustatud täitma täiendavaid turvanõudeid, mis on toodud IT-teenuste kasutamise eeskirjas.
- 6.3 Ameti sisemise infovahetuse nõuded on reguleeritud kommunikatsioonijuhendis.
- 6.4 Suulise suhtluse puhul tuleb väljaspool tööruume ja kõrvaliste isikute juuresolekul vältida juurdepääsupiiranguga informatsiooni käsitlevaid teemasid. Telefoni ja faksi teel info edastamine on reguleeritud IT-teenuste kasutamise eeskirjas.

## **7. PERSONALITURVE**

- 7.1 Pädevate ja usaldusväärsete teenistujate väljaavalimiseks on ametis kehtestatud personali värbamise ja valiku kord.
- 7.2 Kõigile uutele teenistujatele tehakse sissejuhatav ja esmane juhendamine vastavalt kvaliteedikäsiraamatus kehtestatud korrale.
- 7.3 Kõigile teenistujatele võimaldatakse ligipääs ameti ruumidele, seadmetele, infosüsteemidele ja andmetele selles ulatuses, mis on vajalik teenistus- või tööülesannete täitmiseks.
- 7.4 Tööks vajalike dokumentide ja informatsiooni kiire ning efektiivse üleandmise tagamiseks teenistus- või töösuhte lõppemisel või peatumisel on asjaajamiskorra raames kehtestatud nõuded asjaajamise üleandmisele.
- 7.5 Asendamiste kord puhkuste, lähetuste või muude teenistusest või töölt puudumiste korral on kehtestatud põhimääruses ja peadirektori asendamise käskkirjas, teenistujate ametijuhendites ning asendusskeemis.
- 7.6 Teenistujate pädevuse hoidmiseks ja tõstmiseks on ametis välja töötatud koolituspõhimõtted, mis on kirjeldatud koolituste korras.
- 7.7 Lepinguliste töötajate ja ekspertide puhul lülitatakse töövõtu- või käsunduslepingusse asjakohased turvanõuded, sh tähtajatu konfidentsiaalsuskohustus ja sanktsioonid.

## 8. TEGEVUSTE KATKEMATUS

- 8.1 Amet arvestab oma tööde ja ressursside planeerimises kõige tõenäolisemate võimalike ohtudega ja võtab kasutusele mõistlikkuse printsiibil meetmeid ohtude vältimiseks ja ootamatute takistuste ja rikete korral asutuse töö jätkumiseks.
- 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 kvaliteedikäsiraamatus.
- 8.3 Tööalased tegevused ja oluline info, mille kohta ei ole eraldi dokumenteeritud protseduuri reegleid, tuleb teenistujal endal dokumenteerida sellises ulatuses ja vormis, et tema töölt puudumise korral oleks tagatud töö probleemideta jätkamine tema asendaja poolt.
- 8.4 Ametis on kehtestatud õnnetusjuhtumite korral tegutsemise juhend, mis sätestab ennetavad tegevused õnnetusjuhtumite vältimiseks, tegutsemisjuhised õnnetusjuhtumite korral ja töö korraldamise põhimõtted õnnetusjuhtumite järgselt.
- 8.5 Kõigist ameti olulistest andmetest tehakse perioodiliselt varukoopiaid. Täpsemalt on varundamise põhimõtted sätestatud IT-teenindamise eeskirja lisas 1.
- 8.6 Turvaintsidente käsitletakse sellisel viisil, et minimiseerida ja/või piirata turvaintsidentidest tekkida võivaid kahjusid ning taastada rakenduste ja süsteemide töö aktsepteeritava aja jooksul. Täpsemalt on turvaintsidentide käsitlemine sätestatud IT-teenindamise eeskirjas.

## 9. INFOTURBE ALANE TEAVITUS

- 9.1 Kord kuus toimub IT-koosolek, millest võtavad osa arendusnõunik, üldosakonna juhataja, turbejuht ja teised ameti IT-teenindajad.
- 9.2 IT-koosolekul annab turbejuht ülevaate toimunud turvaintsidentidest, ilmnenu turvariskidest ja intsidentide ning riskide maandamise meetmete rakendamisest. Olulisematest teemadest tehakse ülevaade juhtkonna koosolekul.
- 9.3 Operatiivne teavitus toimub ameti sisemise meililisti ja/või siseveebi kaudu. Teatatakse olulistest turvaintsidentidest, turvasituatsiooni muudatustest, teenistujate teenistusse ja tööle võtmisest ja vabastamisest ning pikemaajalistest külastajatest ameti tööruumides.
- 9.4 Iga aasta 15. jaanuariks koostab turbejuht ameti peadirektorile ja Sotsiaalministeeriumile aruande ameti infoturbe kohta. Aruandes sisaldub:
- uuendatud turvameetmete rakenduskava,
  - ülevaade eelneval aastal toimunud infoturbealasest tegevusest,
  - ülevaade eelneval aastal toimunud turvaintsidentidest ja nende lahendusest,
  - ülevaade infoturbe dokumentatsiooni seisust ning tehtud ja planeeritavatest muudatustest.
- 9.5 Punktis 9.4 nimetatud aruande põhjal hinnatakse rakendamata ja osaliselt rakendatud meetmeid ning need aktsepteeritakse peadirektori poolt jääkriskidena või kommenteeritakse rakenduskavas. Nimetatud dokument edastatakse Sotsiaalministeeriumile iga aasta 15. veebruariks.

## **10. INFOTURBE DOKUMENTATSIOON**

10.1 Ameti infoturbe dokumentatsioon koosneb järgmistest dokumentidest:

- Infoturbepoliitika;
- IT-teenuste kasutamise eeskiri;
- IT-teenindamise eeskiri;
- Õnnetusjuhtumite korral tegutsemise juhend;
- Kvaliteedikäsiraamat;
- Sisekorraeeskiri;
- Asjaajamiskord;
- muud infoturbega seotud eeskirjad.

10.2 Lisaks koostatakse ja hoitakse pidevalt ajakohasena Ravimiametis järgnevaid infoturbega seotud materjale:

- andmekogude kaardistus;
- infovarade inventuuri aruanded;
- infoturbemeetmete rakenduskava (sh erandjuhtumid ja jääkriskid);
- infoturbeintsidentide dokumentatsioon;
- pääsuõiguste dokumentatsioon;
- eri andmekogude ja tööprotsesside kohta käiv spetsiifiline dokumentatsioon.