Lisa 1
KINNITATUD
Terviseameti peadirektori 18.07.2024
käskkirjaga nr 1.1-1/24/47

1 Üldsätted

1.1. Käskkirjas kehtestatakse Terviseameti (edaspidi amet) infoturbe üldalused, vastutus ning põhimõtted infoturbe tagamiseks.
1.2. Infoturbena mõistetakse käesolevas käskkirjas Vabariigi Valitsuse 15.03.2012 määruse nr 26 „Infoturbe juhtimise süsteem“ sätestatut tähenduses, mille kohaselt on infoturve turvameetmete loomise, valimise ja rakendamise protsesside kogum.
1.3. Infoturbe põhimõtete eesmärk on käskkirjas kirjeldatud põhimõtete, tegevuste ja meetmete abil saavutada olukord, kus ameti teenistujad mõistavad infoturbe valdkonnaga tegelemise vajalikkust ametis, on teadlikud, miks ja kuidas infoturvet luua ja rakendada ning seeläbi ennetada ja minimeerida võimalikud riskid, tagada tegevuste jätkusuutlikkus ning- kaitsta vara parimal viisil.
1.4. Ameti infoturbe põhimõtted kehtivad kõikidele ameti vara kasutajatele.
1.5. Käskkirjas toodud põhimõtteid tuleb arvestada ameti muude töökorraldust ja tegevusi reguleerivate dokumentide koostamisel.

2 Mõisted

2.1 **Andmekogu** - infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.
2.2 **Infoturbeintsident** - mis tahes sündmus, mis põhjustas või võib põhjustada infovara tervikluse, käideldavuse või konfidentsiaalsuse kao.
2.3 **Infoturve** - turvameetmete loomise, valimise ja rakendamise protsesside kogum, vara (sh. infovara) käideldavuse, tervikluse ja konfidentsiaalsuse tagamiseks.
2.4 **Vara kasutaja** - ameti teenistuja või ametiga mõnes muus lepingulises suhtes olev ameti vara kasutav füüsiline või juriidiline isik.
2.5 **Vara** – informatsiooni ja andmete töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid ja infovara.
2.6 **Infovara** – mis tahes viisil kogutud, jäädvustatud ja töödeldud andmete kogum mistahes andmekandjal, sh paberkandjal.
2.7 **Infosüsteem** – andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega.
2.8 **Infoturbe haldus** – tegevusriski kaalutlemisel põhinev organisatsiooni üldise haldussüsteemi osa, mis tegeleb infoturbe rajamise, juurutamise, rakendamise, seire, hoolduse ja täiustamisega, suunates ja juhtides infoturvet põhimõtete, protseduuride ja muude vahendite kaudu.
2.9 **Isikuandmed** - igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta.
2.10 **Konfidentsiaalsus** - andmete kättesaadavus ainult selleks volitatud isikutele.
2.11 **Käideldavus** - andmete kasutuskõlblikkus, õigeaegne kättesaadavus ja töödeldavus.
2.12 **Küberintsident** - süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust.
2.13 **Kaitseala** – turbekontseptsiooni koostamise ja rakendamise käsitlusala, millesse amet liigitab kogumi sihtobjekte, mida turbeprotsess hakkab edaspidi kaitsma. Infoturbe

juhtimissüsteemi kontekstis on organisatsiooni poolt kaitstavad elemendid: taristu, korraldus, personal, tehnilised komponendid jmt.

2.14 **Kaitsetarve** – äriprotsessi kriitilisusest ja vara väärtusest tulenev vajadus vara kaitsta. Andmete ja teabe omadus, väljendab vajadust kaitsta teda kahju eest, mille võib tekitada konfidentsiaalsuse, tervikluse ja/või käideldavuse rikkumine. E-ITSi kontekstis laieneb kaitsetarve ka teenusele. Kaitsetarvet väljendatakse kolmeastmelises skaalas: „**normaalne**“, „**suur**“ või „**väga suur**“.

2.15 **Turvaintsident** – sündmus(ed), millega kaasneb andmete või muu vara käideldavuse, tervikluse või konfidentsiaalsuse kadu või tekib oht andmete käideldavuse, tervikluse või konfidentsiaalsuse kao tekkeks. Turvaintsidendiks loetakse kõiki reaalse või potentsiaalse kahju juhtumeid, mis võivad ohustada või halvata vara turvalisust.

2.16 **Turvameetmed** – erinevad organisatsioonilised toimingud ja vahendid, tehnilised protsessid ja vahendid mida rakendatakse andmete ja infosüsteemide turvalisuse saavutamiseks ja säilitamiseks. Turvameetmeks nimetatakse kõiki tegevusi, mille eesmärgiks on turvariskide vähendamine ja nende ennetamine.

2.17 **Teenus** – tegevuste kogum, mis koostöös teiste osapooltega loob kliendile terviklikku väärtust. Teenustel on selged ja mõõdetavad eesmärgid kliendist lähtudes.

2.18 **Teenuse juht** - juhib teenust, mh haldab ka igapäevaselt teenuse osutamisega seotud riske, sh infoturbe riske.

2.19 **Teenuse omanik** – osakonnajuhataja ehk teenuste portfelli juht. E-ITS mõistes on teenuste portfell võrdsustatud teenuste äriprotsesside portfelliga. Kaitsetarbe protokollid on loodud teenuste portfellide tasanditele, mille vastutajaks on teenuse omanikud.

2.20 **Turbeviis** – meetod E-ITS standardil põhineva infoturbe halduse süsteemi rajamiseks. Turbeviisi valikul lähtutakse regulatsioonidest ja kaitsetarbest, aga ka organisatsiooni infoturbe küpsusest.

2.21 **Teenistuja** - kõik ameti ametnikud ja töötajad.

2.22 **Terviklus** – andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

2.23 **E-ITS** – Eesti infoturbestandard.

3 Infoturbe eesmärk

3.1 Ameti infoturbe eesmärkideks on tagada:

3.1.1 ameti igapäevane ülesannete täitmine, teenuste osutamine, infovahetus ja asjaajamine, kus põhieesmärgiks on ootustele vastav, stabiilselt toimiv, turvaline ja töökindel töökeskkond;

3.1.2 ametis töödeldavate andmete konfidentsiaalsus ja terviklus;

3.1.3 ameti infosüsteemide ja andmekogude nõuetekohane pidamine ning arendamine, lähtudes kehtivatest õigusaktidest.

3.2 Infoturbe eesmärkide saavutamine toimub eeskätt vara käideldavuse, tervikluse ja konfidentsiaalsuse tagamise kaudu.

4 Põhimõtted, mida järgitakse infoturbe tagamisel

4.1 Infoturbe juhtimise süsteemi rakendamise eest vastutab peadirektor.

4.2 Infoturbe nõuete järgimine on ameti teenistujatele kohustuslik. Nõuete mittetäitmisel vastutavad ameti teenistujad vastavalt kehtivatele õigusaktidele.

4.3 Asjakohaste infoturbemeetmete valimisel, halduse ja kontrolli korraldamisel ning infoturbe alaste riskide, ohtude ja nõrkuste analüüsil ametis on aluseks küberturvalisuse seaduses kehtestatud turvameetmete süsteem, mis seisneb infoturbe eesmärkidele

vastavate kaitsetarvete määramises ja nendele vastavate turvameetmete valimises, rakendamises ja kontrollis vastavalt E-ITS-le.

4.4 Turvameetmete valikul arvestatakse, et need oleksid majanduslikult õigustatud ja proportsioonis võimaliku kahjuga, mis võib tekkida meetmete puudulikkuse tõttu ning nende häiriv toime ameti tegevusele ja ameti teenistujate tööle peab olema võimalikult väike.

4.5 Infoturbe meetmed tagatakse erinevate tegevuste abil, sh õigusaktide ja muude regulatsioonide järgimine, millega on kehtestatud hoonete läbipääsupõhimõtted, sisekorraeeskirjad, teabehalduse korraldus, IT vara kasutamise ja infoturbeintsidentide haldamise korraldus.

4.6 Infosüsteemidega seonduvate muudatuste kavandamisel analüüsitakse muudatuste sisu vastavust infoturbe nõuetele ning vajadusel teostatakse infosüsteemile uus kaitsetarbe hindamine.

5 Infoturbe põhimõtete rakendamine

5.1 Infoturbeprotsessi parandatakse ja täiustatakse vastavalt ameti eesmärkidele ja ohumaastiku muutumisele. Infoturbeprotsessi täiustamise ja muutmise ettepanekud teeb infoturbe eest vastutav isik ameti juhtkonnale vastavalt vajadusele, kuid vähemalt üks kord aastas.

5.2 Infoturbe põhimõtteid rakendatakse kõigile vara käitlemisega seotud protsessidele (sh protsesside kavandamisele) ning see seisneb asjakohaste turvameetmete kavandamises, planeerimises, loomises, rakendamises, haldamises.

5.3 Kõigile ameti andmetele, ruumidele ja infosüsteemidele kehtestatakse juurdepääsuõiguste alused, sh järelevalve teostamise kord. Juurdepääsuõiguste aluste kehtestamise ja jälgimise eest vastutab teenuse omanik.

5.4 Ameti poolt teenistujale tööülesannete täitmiseks antud seadmed ja süsteemid (sh e-postiaadress) on tööalaseks kasutamiseks.

5.5 Tööülesannete täitmiseks tohib teenistuja kasutada ainult ameti antud seadmeid. Igakordselt põhjendatud juhul, mis on kooskõlastatud infoturbe eest vastutava isikuga, võib tööülesannete täitmiseks kasutada isiklikku mobiiltelefoni.

5.6 Teenistuja arvutis, mobiiltelefonis või muus teenistuja kasutusse antud seadmes olev teave, mis on loodud ametiülesannete täitmiseks, kuulub ametile ning sellest ei ole lubatud teha koopiaid teenistuja isiklikesse seadmetesse ja süsteemidesse.

5.7 Teenistuja kohustub hoidma konfidentsiaalsena talle antud kasutajatunnused, paroolid, ligipääsukoodid jms ning välistama nende sattumise kolmandate isikute kätte.

5.8 Infoturbe põhimõtete rakendamiseks vajalikud tegevused kajastatakse tööplaanis vastavalt rakendusplaanile, mis sisaldab konkreetseid (kalendriaasta jooksul) teostamisele kuuluvaid koordineerituid tegevusi.

6 Infoturbe organisatsioon ja juhtimine

6.1 Infoturvet käsitlevad dokumendid, millega kindlustatakse juhtkonna kohustumus ja ameti infoturbe koguvastutus juhtkonna tasemel, kinnitab peadirektor. Infoturvet käsitlevad dokumendid on kättesaadavad ameti dokumendihaldussüsteemis ja siseveebis.

6.2 <u>Peadirektori infoturbealased ülesanded:</u>

6.2.1 teeb infoturbealased otsuseid talle esitatud ettepanekute alusel ja osaleb infoturbe olulisusest teavitamisel;

6.2.2 vastutab infoturbe juhtimise süsteemi toimimise eest;

6.2.3 vastutab infoturbe halduse käigus hoidmise eest ning tagab regulaarselt toimiva infoturbealase riskihalduse;

6.2.4 kehtestab valdkonda puudutavad regulatsioonid, korrad ja põhimõtted;
6.2.5 määrab infoturbe eest vastutava isiku või üksuse;
6.2.6 kinnitab infoturbe valdkonna eesmärgid;
6.2.7 osaleb infoturbe peamiste riskide hindamise ja jääkriskide aktsepteerimise protsessis;
6.2.8 kinnitab teenustele määratud kaitsetarbed;
6.2.9 osaleb infoturbe olulisuse teavitamises;
6.2.10 vastutab infoturbe põhimõtete rakendamise eest.

6.3 Infoturbealast tegevust ametis korraldab analüüsi- ja arendusosakond.

6.4 Infoturbe eest vastutava isiku ülesanded:
6.4.1 täidab oma infoturbealaseid kohustusi lähtuvalt E-ITS-st, käesolevast käskkirjast, valdkonda reguleerivatest õigusaktidest ja ametijuhendist;
6.4.2 rakendab ameti infoturbe juhtimise süsteemi, koordineerib E-ITS rakendamist ja ameti vara piisava taseme turvalisuse tagamist vastavalt infoturvet ning andmekaitset reguleerivatele õigusaktidele;
6.4.3 vastutab infoturbega seotud ülesannete täitmise eest ning tagab infoturvet reguleerivate juhiste olemasolu, elluviimise ja ajakohastamise;
6.4.4 haldab ameti turvaintsidente ning teavitab viivitamatult ameti peadirektorit. Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo või distsiplinaarsüüteo tunnused, antakse juhtum edasi menetlemiseks vastava menetluse läbiviimise õigust omavale organile;
6.4.5 kontrollib teenistujate infoturbenõuete tundmist ja järgimist. Nõuete rikkumise tuvastamise korral teavitab infoturbe eest vastutav isik tekkinud olukorrast teenistuja vahetut juhti ja peadirektorit ning annab soovitusi esile kerkinud probleemide ja riskide lahendamiseks või leevendamiseks;
6.4.6 teavitab teenistujaid turvareeglitest, nõustab neid infoturbealaselt ja korraldab teenistujatele koolitusi üldise turvateadlikkuse tõstmiseks.

6.5 Teenuse juhi ülesanded:
6.5.1 arvestab oma teenust juhtides infoturbe nõuetega;
6.5.2 tagab vara käideldavuse, tervikluse ja konfidentsiaalsuse ning varade kaitset reguleerivate õigusaktide täitmise;
6.5.3 jälgib oma teenuse infosüsteemide kasutamise ja toimimise õiguspärasust;
6.5.4 teeb ettepanekuid ja annab tagasisidet oma teenuse vaates infoturbealase dokumentatsiooni ja kordade toimimise kohta.

7 Vara ja kaitsetarve

7.1 Ameti vara on kaardistatud ning varana käsitletakse seda vara, mis on arvele võetud Riigitöötaja Iseteenindusportaali (edaspidi RTIP) varade moodulis. Uue vara lisandumisel või vara kasutuse lõpetamisel tehakse vara nimekirjas täiendused. Vara eest vastutaja on kohustatud hoidma varade ülevaadet ajakohasena.
7.2 Vara eest vastutab RTIPi varade moodulis vara kaardile määratud teenistuja, kes vastutab konkreetse vara olemasolu, säilimise ja sihipärase kasutamise eest.
7.3 Ametis kasutusel olevate infosüsteemide nimekiri ning neile määratud kaitsetarbed on sätestatud Terviseameti peadirektori 01.02.2021 käskkirja nr 1.1-1/21/1 „Terviseameti teabehalduse kord“ lisas 1.
7.4 Vara turvalisuse klass tuleneb ameti teenusele määratud kaitsetarbest.

7.5 Teenuste kaitsetarbeid hinnatakse iga-aastaselt ja muudatused kinnitatakse peadirektori poolt.

8 Infoturbe protsess ja infoturbeintsidentide haldus

8.1 Vara kasutajatele korraldatakse regulaarselt turvateadlikkuse koolitusi.

8.2 Vara kasutajatel on kohustus kord aastas läbida infoturbekoolitus ja test.

8.3 Vara kasutaja, kes avastab infoturbeintsidendi või selle ohu, peab viivitamatult, kuid mitte hiljem kui 24 tunni jooksul teavitama sellest IT-abi ning infoturbe eest vastutavat isikut. Kui infoturbeintsident puudutab isikuandmetega seotud rikkumist, tuleb lisaks teavitada ka andmekaitsespetsialisti.

8.4 Sisekontrolli juht teostab infoturbe protsessi sõltumatu läbivaatuse vastavalt vajadusele, kuid mitte harvem kui üks kord aastas vahetult enne EITS-i auditit ja koostab läbivaatuse tulemuste kohta raporti, mis esitatakse peadirektorile.

8.5 Infoturbe standardi E-ITS rakendamise audit hangitakse vastavalt EITS kehtivale auditeerimisjuhendile iga 3 aasta järel.