

IT-TEENUSTE KASUTAMISE EESKIRI

SISUKORD

1.	ÜLDSATTED	1
2.	MÕISTED	1
3.	TARK- JA RIISTVARA KASUTUS JA HALDUS	2
4.	PÄÄSUÕIGUSTE KASUTUS JA HALDUS	2
5.	SISEVÕRGU JA INTERNETI KASUTUS JA HALDUS	3
6.	MEILI- JA FAILISERVERI KASUTUS JA HALDUS	4
7.	KAUGTÖÖKOHT, SÜLEARVUTID, NUTISEADMED JA ANDMEKANDJAD	5
8.	VÄIKESEADMETE KASUTUS JA HALDUS	6
9.	RÜNDETÕRJETARKVARA KASUTUS JA HALDUS	6
10.	VARUNDAMINE	7
11.	SANKTSIOONID	7

1. ÜLDSATTED

- 1.1 Käesolev eeskiri kehtib kõikidele Ravimiameti (edaspidi „amet“) IT-teenindajatele, kasutajatele ja külalistele ning sätestab nende õigused ning kohustused. Kasutajad ja IT-teenindajad peavad täiendavalt arvestama infoturbepoliitikas ja muudes dokumentides sätestatud.
- 1.2 Kasutajad on kohustatud kasutama ameti IT-teenuseid ning tark- ja riistvaralisi süsteeme ainult teenistus- ja tööülesannete täitmiseks.
- 1.3 Kasutajad on kohustatud oma ülesannete täitmisel järgima kõiki ametis kehtestatud turvanõudeid ja IT-teenuste kasutamisel kinni pidama IT-teenindajate seatud ajutistest piirangutest.
- 1.4 Kasutajad on kohustatud võimalikest ja toimunud turvaintsidentidest viivitamatult teavitama e-posti teel ameti turbejuhti või IT-teenindajaid. Viimasel juhul teavitab IT-teenindaja turbejuhti pärast esmaste abinõude kasutuselevõttu.
- 1.5 Kasutajatel on õigus saada IT-teenindajatelt teavet muudatuste ja intsidentide kohta, mis oluliselt mõjutavad ameti tark- ja riistvara kasutamist või rikuvad kasutaja privaatsust.
- 1.6 Kasutajatel on õigus saada oma teenistus- ja tööülesannete täitmise piires igakülgset IT-teenuste alast abi ja infoturbe alast teavet IT-teenindajatelt.

2. MÕISTED

- 2.1 Kasutajad – ameti ametnikud ja töötajad (edaspidi koos nimetatud „teenistujad“), kes kasutavad IT-teenuseid tulenevalt oma teenistus- või tööülesannetest ja kes on registreeritud ameti IT-teenuste kasutajate registris.
- 2.2 IT-teenindajad – ameti teenistujad, kelle ametijuhendist tulenevate teenistus- või tööülesannete hulka kuulub IT-teenuste tööks vajalike tark- ja riistvaraliste süsteemide

arendamine ja haldamine. Kõik kasutajate kohustused ja õigused kehtivad ka IT-teenindajate kohta.

- 2.3 Külalised – isikud, kellel on ligipääs Internetti ameti kulul ning ameti võrguseadmete vahendusel ja kes ei ole registreeritud ameti IT-teenuste kasutajate registris.
- 2.4 Seadmed – ameti poolt kasutajale teenistus- või tööülesannete täitmiseks eraldatud sülearvuti, nutiseade vm IT seade.
- 2.5 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.

3. TARK- JA RIISTVARA KASUTUS JA HALDUS

- 3.1 Amet tagab kasutajale tark- ja riistvaralised vahendid vastavalt kasutaja teenistus- või tööülesannetele.
- 3.2 Kasutajad on kohustatud viivitamatult teavitama IT-teenindajaid võimalikest tark- või riistvaralistes süsteemides ilmnenud rikestest ja kirjeldama nende teket ning olemust võimalikult täpselt.
- 3.3 Kasutajatel on keelatud mittemobiilse riistvara väljaviimine ameti ruumidest.
- 3.4 Kasutajatel on keelatud jätta ameti vara järelevalveta, kui ei ole välistatud volitamata ligipääs.
- 3.5 Töö lõpetamisel tuleb sulgeda kõik rakendused, arvutivõrgust välja logida ning lülitada välja monitor. Tööjaam (lauaarvuti) jäetakse ööseks tööle automaatseteks uuendusteks, kui ei ole antud teistsugust korraldust.
- 3.6 Kasutajad on kohustatud tööajal töökohalt lühemaks või pikemaks ajaks lahkudes ennast kasutajakontolt välja logima või kasutajakonto lukustama (Windows-klahv + L) .
- 3.7 Teenistus- või töösuhte lõpetamisel on kasutaja kohustatud tagastama kõik tema kasutuses olnud ameti tark- ja riistvaralised süsteimid.

4. PÄÄSUÕIGUSTE KASUTUS JA HALDUS

- 4.1 Kõigile kasutajatele antakse pääsuõigused ameti sisevõrgu, meilikonto ja dokumendihaldussüsteemi üldtasandi jaoks.
- 4.2 Infosüsteemide ja juurdepääsupiiranguga infot sisaldavate võrgu- ja dokumendihalduskataloogide pääsuõigused antakse vastavalt kasutaja teenistus- või tööülesannetest tulenevatele vajadustele.

- 4.3 Pääsuõiguste ulatuse ja nende uuendamise vajaduse otsustab kasutaja vahetu juht. Pääsuõiguste andmine on detailsemalt kirjeldatud IT-teenindamise eeskirjas.
- 4.4 Autentimine toimub kasutajanime ja parooliga või ID-kaardiga.
- 4.5 Kasutaja on kohustatud hoidma oma paroole saladuses ja mitte lubama teistel isikutel kasutada tema pääsuõigusi.
- 4.6 Kasutajad on kohustatud valima endale parooli, mis on vähemalt 7 märki pikk ja sisaldab keerulisuse nõuetele vastavalt suur- ja väiketähti ning numbreid. Parool ei tohi baseeruda kasutaja nime või initsiaalide modifitseerimisel, sõnastiku sõnadel või muudel isikliku tähendusega sõnadel (laste nimed, sünnikuupäevad, lemmikloomade nimed jne). Paroolis pole soovituslik kasutada täpitähti või erimärke, mille paigutus klaviatuuridel võib erineda. Nutiseadmete parooliks (lukukoodiks) peab kasutama vähemalt neljakohalist numbrit. Keelatud on kasutada musterkoodi, samasuguseid numbreid (näiteks 0000, 1111 jne.), järjestikuseid numbreid (näiteks 1234, 4567 jne.), kasutajaga seotud andmetest tulenevaid numbreid (näiteks sünniaasta, sünnikuupäev) ning teiste isiklike dokumentidega seotud koode (näiteks ID-kaart, pangakaart jne.).
- 4.7 Parool tuleb sisestada kõrvalistele isikutele märkamatuks. Kasutajad on kohustatud viivitamatult võtma kasutusele uue parooli, kui on tekkinud kahtlus, et see on saanud teatavaks kõrvalistele isikutele.
- 4.8 Kasutajad on kohustatud võrgukasutaja parooli muutma iga 90 päeva järel. Parooli vahetamise vajadust tuletatakse kasutajale meelde sisselogimisel vähemalt 5 päeva enne parooli aegumist. Süsteem ei luba parooli vahetamisel taaskasutada kuut viimast kasutaja parooli.
- 4.9 Kasutajad on kohustatud võrku või infosüsteemi esimest korda sisselogides ära muutma IT-teenindajate poolt antud ajutise parooli. See säte kehtib ka juhul, kui IT-teenindajad on ära muutnud parooli kasutaja nõudel.

5. SISEVÕRGU JA INTERNETI KASUTUS JA HALDUS

- 5.1 Ameti arvutivõrk on tulemüüri abil jagatud kolmeks segmendiks: a) sisevõrk (tööjaamad ja ameti sisemise kasutusega serverid), b) demilitariseeritud tsoon (tulemüüri kaudu kontrollitav ligipääs nii välis- kui ka sisevõrgust: veebiserverid jms), c) välisvõrk (EENET'i võrguühendus).
- 5.2 Kõik ameti kulul või ameti võrguseadmete vahendusel sisevõrku ühendatud tööjaamad kuuluvad registreerimisele ameti IT-teenuste kasutajate registris.
- 5.3 Tööjaamade ja teiste võrguseadmete (v.a ameti sülearvutid) sisevõrku ühendamine ja sisevõrgus ümberpaigutamine on lubatud ainult IT-teenindajatele.
- 5.4 Kasutajatel on keelatud ameti riistvara kasutades külastada teenistus- või tööülesannetega mitteseonduvaid veebilehekülgi ja laadida alla tööks mittevajalikke programme ja potentsiaalselt ohtlikke faile.
- 5.5 Avalikke traadita võrguga internetipunkte kasutades peab kasutaja arvestama, et reeglina on avalikud traadita internetipunktid ebatavalised.

6. MEILI- JA FAILISERVERI KASUTUS JA HALDUS

6.1 Põhimõtted

- 6.1.1 Kõigile kasutajatele võimaldatakse isiklik kettaruum failiserveris (U ketas) ja isiklik meiliaadress kujul eesnimi.perekonnanimi@ravimiamet.ee, kusjuures tähed õ, ä, ö, ü, š ja ž asendatakse nimes vastavalt tähtedega o, a, o, u, s ja z.
- 6.1.2 Kõik e-kirjad on allutatud viirusetõrjele ja rämpsposti filtrile, mistõttu ei ole soovitatav kirjadele lisada faile viiruste levitamist võimaldavas vormingus (exe, com, mpg, avi, eml, zip jms).
- 6.1.3 Kasutaja meilikonto maht ei ole piiratud, failiserveris eraldatakse kasutajatele isiklik kettaruum arvestusega ca 2 GB kasutaja kohta.
- 6.1.4 Maksimaalne e-kirja suurus, mida e-posti server vastu võtab, on 20 MB. Väljasaadetava e-kirja puhul tuleb arvestada, et vastuvõtval serveril võib piirang olla madalam ja e-kirja suurus peaks soovituslikult jääma alla 8 MB.
- 6.1.5 Ameti meilikontole ligipääs on võimalik ameti arvutist ja sülearvutist Microsoft Outlook tarkvaraga, ameti nutiseadmest e-posti rakendusega, Microsoft Exchange serveri veebimeili täisversiooni (<https://mail.ravimiamet.ee/exchange>) või tekstiversiooni (<https://mail.ravimiamet.ee/oma>) abil.
- 6.1.6 Teenistus- või töösuhte lõppemisel või peatumisel üle 3 kuu eemaldatakse e-posti aadress postiloenditest ja kasutajakonto blokeeritakse.
- 6.1.7 Failinimedes ei soovitata kasutada õ, ä, ö ja ü tähte ning koma, tühikut või punkti.

6.2 Kasutajate kohustused

- 6.2.1 Kasutajad on kohustatud talle eraldatud meiliaadressi ja failiserveri kettaruumi kasutama ainult tööalastel eesmärkidel.
- 6.2.2 Kasutaja peab arvestama, et teenistus- või töösuhte pikaajalisel peatumisel või lõppemisel võetakse kasutajalt ära pääsuõigused meilikontole ja kettaruumile, kasutaja kirjavahetus säilitatakse ning kasutaja asendajale võimaldatakse lugemisõigus kasutaja meilikonto ja erijuhtudel ka isikliku kettaruumi andmetele.
- 6.2.3 Kasutajatel on keelatud ameti meili- ja failiserveri ressursside tahtlik raiskamine või muu selline tegevus, mis häirib süsteemi kasutamist määratud otstarbel.
- 6.2.4 Kasutajatel on keelatud edastada e-kirju ja hoida failiserveri kettapinnal faile, mille sisu on illegaalne, ebaetiline, solvav või kahjustab riigi või asutuse mainet. Seda põhimõtet tuleb järgida ka kollegiaalses kirjavahetuses.
- 6.2.5 Kasutajad on kohustatud regulaarselt korrastama endaga seotud meili- ja failiserveris asuvaid andmeid, kustutades ebaolulised kirjad ja failid.
- 6.2.6 Kasutajad on kohustatud pikemaajalise eemalviibimise, teenistus- või töösuhte peatumise või lõppemise puhul aktiveerima enda meilikonto automaatvastuse funktsiooni, kus märgib ära

enda eemaloleku perioodi ning enda asendaja või selle puudumisel ameti üldised kontaktandmed.

7. KAUGTÖÖKOHT, SÜLEARVUTID, NUTISEADMED JA ANDMEKANDJAD

7.1 Põhimõtted

- 7.1.1 Kasutajatel on õigus kasutada teenistus- või tööülesannete täitmiseks kaugtöökohta, kui see on tööandja ja vahetu juhi poolt lubatud, ei halvenda töötulemusi ja ei põhjusta juurdepääsupiiranguga teabe lekkimist.
- 7.1.2 Sülearvuti ja/või nutiseade eraldatakse kasutajale vahetu juhi ettepanekul, kui see on põhjendatud teenistus- või tööülesannete iseloomuga ja kaugtöö tegemise vajadusega. Isiklike ameti tehnilistele nõuetele vastavate (kirjeldatud IT-teenindamise eeskirjas) nutiseadmete tööalane kasutamine lepitakse kokku töötaja osakonna juhatajaga.
- 7.1.3 Sülearvuti ja/või nutiseade valmistatakse kasutajale ette IT-teenindajate poolt ja antakse üle vara kasutamise kokkuleppe alusel. Isiklikud nutiseadmed häälestatakse IT-teenindajate poolt.
- 7.1.4 Sülearvuti kõvaketas ja nutiseadme sisemälu koos mälukaardiga on krüpteeritud, kaitsmaks andmete väärkasutust seadme varguse või volitamata kasutamise puhul.
- 7.1.5 Nutiseadmed lukustuvad automaatselt 5 minuti jooksul.
- 7.1.6 Juhul kui parooli või lukukoodi on sisestatud korduvalt valesti, rakendatakse seadmetes täiendavaid võimalikke turvameetmeid, mis tõkestavad teatud aja jooksul uuesti parooli või lukukoodi sisestamise.
- 7.1.7 Väljastpoolt ametit saab sülearvutitega ameti sisevõrku ühenduda VPN ühenduse abil, mis seadistatakse IT-teenindajate poolt.
- 7.1.8 Ameti üldisi ja osakonnasiseseid ühisligipääsuga dokumente tohib sülearvutisse salvestada ja töötlemise järel tagasi võrgukettale salvestada vaid teiste kasutajatega kokkuleppel, kui muudatuste tegemine on jälgitav ja erinevate versioonide haldus on võimalik.

7.2 Kasutajate kohustused

- 7.2.1 Kasutajad on kohustatud tagama kaugtöökoha turvalisuse samaväärselt ameti tööruumide tingimustele. Avalikus kohas tuleb seadmeid kasutada turvaliselt, kaitstes neid varguse, rikkumise, ekraanil oleva info liigse avalikkuse ja teiste ohtude eest.
- 7.2.2 Kasutajatel on keelatud kaugtöökohas teostada teenistus- või tööülesannetest tulenevat delikaatsete isikuandmete (v.a inspeksiooni käigus kogutud materjalid) töötlust, sh talletada ja transportida neid andmeid andmekandjatel ja seadmetes. Ärisaladust sisaldavaid andmeid võib kaugtöökohas töödelda vaid ameti poolt selleks ettevalmistatud seadmetega.
- 7.2.3 Kasutajad on kohustatud kasutama juurdepääsupiiranguga teabe transportimisel andmete krüpteerimist, kasutades selleks näiteks ameti IT-teenindajate poolt ette valmistatud ja krüpteeritud mälu pulki või ID-kaarti ja DigiDoc tarkvara krüpteerimisvahendeid.
- 7.2.4 Kasutajad ei tohi seadmetes välja lülitada ega deinstalleerida viirusetõrjetarkvara, viiruste andmebaasi ning süsteemiuuenduste tegemist.

- 7.2.5 Kasutajatel on keelatud salvestada ja installeerida seadmetesse programme ja faile (arvutimängud, filmid), mis ei ole seotud teenistus- või tööülesannete täitmisega ning koormavad süsteemi või on potentsiaalselt nakatatud ründetarkvaraga.
- 7.2.6 Andmete üleandmiseks kasutataval andmekandjal (nt CD-ROMil, mälupulgal jne) ei tohi olla mingeid muid materjale ega peitandmeid. Andmekandja peab olema märgistatud korrektselt (saaja ja saatja andmed, saadetise nimetus ja formaat), kuid nii, et kõrvalisel isikul ei oleks võimalik märgistusest välja lugeda liigset infot selle sisu kohta.
- 7.2.7 Defektsed ja kasutusest väljunud andmekandjad tuleb anda turvaliseks kustutamiseks ja hävitamiseks IT-teenindajatele.
- 7.2.8 Kasutaja on kohustatud tooma vähemalt korra kvartalis seadme(d) IT-teenindajatele korrastamiseks ja hooldamiseks.
- 7.2.9 Kasutajatel on keelatud anda seadmeid või andmekandjaid kasutamiseks teistele isikutele.

8. VÄIKESEADMETE KASUTUS JA HALDUS

- 8.1 Lauatelefonide, fakside, skännerite ja teiste infotehnoloogiliste väikeseadmete (edaspidi väikeseadmed) toimimise eest vastutab üldosakond.
- 8.2 Ameti põhifaksiaparaadi sihipärase kasutamise ja hoolduse korraldamise eest vastutab üldosakonna spetsialist (dokumendihalduse alal). Inspektsiooniosakonna ruumide juures asuva faksiaparaadi sihipärase kasutamise ja hoolduse korraldamise eest vastutab inspektsiooniosakonna sekretär-asjaajaja.
- 8.3 Väikeseadmete kasutamisel peab iga kasutaja tegema kõik endastoleneva, et tagada juurdepääsupiiranguga teabe adekvaatne kaitse.
- 8.4 Delikaatsete isikuandmete edastamine telefoni või faksi teel on keelatud. Juurdepääsupiiranguga andmete telefoni või faksi teel edastamine tööalases asjaajamises on lubatud vaid juhul, kui vastuvõtja poole isik on üheselt tuvastatav.
- 8.5 Nutiseadmete ühendamine ameti sisevõrku on keelatud.
- 8.6 Nutiseadmetes on keelatud hoida töölaseid konfidentsiaalseid andmeid.
- 8.7 Skänneri, faksi ja printeri kasutamisel peab iga kasutaja jälgima, et ei unustataks dokumente jm materjale pikemaks ajaks seadmesse või seadme vahetusse lähedusse.
- 8.8 Sissetulevad faksid edastatakse määratud meiliaadressile, et vältida tarbetut väljaprintimist.

9. RÜNDETÕRJETARKVARA KASUTUS JA HALDUS

- 9.1 Kasutajatel on keelatud nakatada teadlikult ründetarkvaraga ameti arvuteid, servereid ja muid andmekandjaid, avada ründetarkvara kahtlusega meililisanदेid ja veebilehti, välja lülitada failide automaatset taustkontrolli, muuta viirusetõrjeprogrammi määranguid ja iseseisvalt teostada aktiveerunud ründetarkvara eemaldamist.

- 9.2 Kasutajatel on keelatud ühendada ameti arvutite külge ebaturvalisi väliseid andmekandjaid. Vähimagi kahtluse korral tuleb andmekandjaga eelnevalt pöörduda IT-teenindajate poole.
- 9.3 Ründetarkvara puudutava hoiatuse ekraanile ilmudes on kasutajad kohustatud viivitamatult teavitama IT-teenindajaid ning enne edasiste juhiste saamist seiskama oma töö tööjaamas.

10. VARUNDAMINE

- 10.1 Vältimaks varundussüsteemide liigset koormamist, on kasutajatel keelatud hoida ameti tööga mitte seotud andmeid ameti andmekandjatel.
- 10.2 Kasutajad on kohustatud enda poolt salvestatud ja ebavajalikuks muutunud andmed regulaarselt ameti kettaruumilt ja andmekandjalt eemaldama.
- 10.3 Hävinenud andmete taastamist teostavad IT-teenindajad, eeldusel et see on tehniliselt võimalik, andmed on tööks vajalikud ja neid ei ole kustutatud teadlikult.
- 10.4 Sülearvutis töödeldavate ameti andmete piisava ja regulaarse varundamise eest vastutab selle kasutaja. Sülearvuti andmete varundamiseks peab kasutaja kasutama isiklikku kettapinda ameti sisevõrgus (U ketas).
- 10.5 Nutiseadmetes töödeldavate ameti andmete piisava ja regulaarse varundamise aitavad organiseerida IT-teenindajad.

11. SANKTSIOONID

- 11.1 Turvanõuete olulise rikkumise kahtluse korral võivad IT-teenindajad ajutiselt peatada kasutaja pääsuõigused ameti IT-teenustele asjaolude selgumiseni.
- 11.2 Turvanõuete järgimine on kõigile teenistujatele kohustuslik. Turvanõuete rikkumisel vastutab isik vastavalt õigusaktidele.