

Arvutivõrgu ja IT varade kasutamise kord

SISUKORD

1. Üldsätted	1
2. Seotud dokumendid.....	1
3. Mõisted.....	2
4. Kasutaja õigused	2
5. Kasutaja kohustused.....	3
6. Paroolinõuded	3
7. Võrgukettad, failide hoidmine ja printimine	4
8. Elektronpost	5
9. Faks, skanner ja muud sarnased väikeseadmed	6
10. Avaliku võrgu (interneti) kasutamine	6
11. Digitaalsed andmekandjad	6
12. Kaugtöö ehk töö väljaspool asutuse arvutivõrku	7
13. RA arvutivõrgu mobiilsideseadmetega kasutamine.....	7
14. RA mittekuuluva IKT-vahendi kasutamine asutuse arvutivõrgus	8
15. Info- ja kommunikatsioonitehnoloogia vahendite tellimine ja tagastamine	8
16. IT-kasutajatugi	9
17. Arvutivõrgu ja IT varade väärkasutuse tagajärjed	9
Lisa 1 - Ravimiameti sülearvutite kasutamise kord	11

1. Üldsätted

- 1.1. Käesolev kord sätestab Ravimiameti (edaspidi RA) arvutivõrgu ja infotehnoloogiliste (IT) varade kasutaja õigused ja kohustused, et kaitsta ja hallata asutuse arvutivõrgu ühtseid ressursse, infosüsteeme ja nende abil töödeldavaid andmeid.
- 1.2. Käesolev kord kehtib kõikidele RA arvutivõrgu teenuste ja IT varade kasutajatele ning kõikidele arvutivõrku ühendatud seadmetele ja tööjaamadele (lauaarvuti, sülearvuti, terminal, nende tarkvara jne).
- 1.3. RA arvutivõrk koosneb ühiseid ressursse ja teenuseid kasutavatest infotehnoloogilistest vahenditest (riist- ja tarkvara) ning nende abil töödeldavatest andmetest.
- 1.4. RA arvutivõrguks ei loeta asutuse poolt külalistele pakutavat avaliku võrgu teenust ehk WIFI-t.

2. Seotud dokumendid

- 2.1. Ravimiameti infoturbepoliitika,
- 2.2. Arvutivõrgu ja infosüsteemide juurdepääsuõiguste haldamise kord (RA),
- 2.3. IT varade kord (TEHIK),
- 2.4. Hangitavate IT väikevarade loetelu ja arveldamise kord (TEHIK).

3. Mõisted

- 3.1. TEHIK – Tervise- ja Heaolu Infosüsteemide Keskus, RAle IT-teenuse pakkuja;
- 3.2. kasutaja – isik, kellele on antud RA arvutivõrgu kasutusõigused ja IT varad, sh kõik RAga töö- või teenistussuhtes olevad ametnikud, töötajad või muu lepingu (nt käsundusleping, töövõtuleping) alusel asutuse huvides tegutsevad isikud;
- 3.3. IT-kasutajatugi – TEHIKu IT-teenuste kasutajatugi ja kõnekeskus;
- 3.4. IT-spetsialist – TEHIKu või tema koostööpartneri (nt Telia) IT-alaste teadmistega IT-teenindaja;
- 3.5. IT-teenus – TEHIKu poolt RAle pakutav lahendus, mis võib baseeruda mingil riist- või tarkvaral ja selle juurde osutatavatel tegevustel (sh vajadusel IT-teenuse osutamisega seotud informatsiooni andmine/konsultatsioon) ning mis toetab (võimaldab) RA teenuste kasutamist;
- 3.6. IKT vahend – info- ja kommunikatsioonitehnoloogia vahend ehk andmete töötlemise, salvestamise ja edastamise tehnilised vahendid, näiteks tööjaam, lauarvuti, sülearvuti, monitor, printer, skanner jne;
- 3.7. IT-vara – kõik IKT vahendid ning muud sellega seotud seadmed ja komponendid, abimaterjalid ja tarvikud;
- 3.8. mobiilsideseade – teatud liiki IKT vahend, näiteks tahvelarvuti, mobiiltelefon, nutikell jms;
- 3.9. digitaalne andmekandja – seade, millele saab salvestada digitaalset infot (nt kõvaketas). Mobiilseteks loetakse andmekandjatest neid, mida saab kaasas kanda ning ilma arvuti korpust avamata arvuti küljest või arvutivõrgust eemaldada või sinna lisada (nt USB pulgad, mälukaardid, CD/DVD plaadid, telefonide ja fotoaparaatide mälukaardid, väline kõvaketas jne)
- 3.10. juurdepääsupiiranguga teave – teave, mis seaduse, lepingu või mõnel muul alusel on kuulutatud mitteavalikuks;
- 3.11. intsident – ootamatu rike (mis ei ole normaalse/standardse teenuse osa), mis põhjustab või võib põhjustada IT-teenuse planeerimata katkestuse või teenuse kvaliteedi olulise languse;
- 3.12. teenindussoov – kasutaja pöördumine IT-kasutajatoe poole info või nõuande saamiseks, taotlus juurdepääsu saamiseks või muutmiseks, andmete parandamise tellimus, statistika või väljavõtte koostamise tellimus, tarkvara või riistvara tellimus jmt.

4. Kasutaja õigused

- 4.1. Arvutivõrgu kasutajal on õigus omada juurdepääsu talle tööks vajalikule teabele ja teenustele. Arvutivõrgu teenuste kasutamise õigused antakse kasutajale vastavalt kasutaja teenistus- või tööülesannetele lähtudes *Arvutivõrgu ja infosüsteemide juurdepääsuõiguste haldamise korrast*.
- 4.2. Kasutajal on õigus saada tööks vajalikke IKT vahendeid.
- 4.3. Kasutajal on õigus saada IT-kasutajatoelt mõistliku aja jooksul ennetavalt infot planeeritud muudatustest ja sündmustest infosüsteemides ja arvutivõrgus, kui muutused mõjutavad oluliselt teenuste kvaliteeti.
- 4.4. Kasutajal on õigus pöörduda infotehnoloogiaalase abi saamiseks IT-kasutajatoe poole e-postiaadressil itabi@tehik.ee või telefonil 794 3913.
- 4.5. Kasutajal on õigus esitada TEHIKule ettepanekuid arvutivõrgu töö ja teenuste ning infoturbe paremaks korraldamiseks.

5. Kasutaja kohustused

- 5.1. Kasutaja on kohustatud järgima asutuses kehtivaid kordasid ja juhendeid ning arvutivõrgu või infosüsteemi kasutamiseks kehtestatud alalisi ja ajutisi piiranguid.
- 5.2. Kasutaja on kohustatud kasutama TEHIKu poolt pakutavaid IT-teenuseid, tark- ja riistvaralisi süsteeme ja IT varasid ainult teenistus- ja tööülesannete täitmiseks.
- 5.3. Kasutaja on kohustatud kasutama võrguressursse optimaalselt ning mitte koormama arvutivõrku tööga mitteseotud andmete või tegevustega ega segama teiste arvutivõrgu kasutajate tööd.
- 5.4. Kasutaja peab järgima head tava ja ei tohi tekitada teistele kasutajatele või asutusele oma tegevusega või tegevusetusega kahju ega ohtu arvutivõrgu turvalisusele.
- 5.5. Kõik arvutivõrgu ja infosüsteemide juurdepääsuõigused on isiklikud ning neid ei ole lubatud edasi anda.
- 5.6. Kasutaja on kohustatud võimalikest ja toimunud tarkvara tõrgetest või riistvaralistest riketest ja turvaintsidentidest viivitamatult teavitama IT-kasutajatuge.
- 5.7. Keelatud on omavoliline (ilma TEHIKu loata) IKT vahendite, sh tarkvara, lisamine (va mobiilsed andmekandjad, mille kohta kehtib käesoleva korra punkt 11), ümberpaigutamine, häälestamine, eemaldamine ja asutuse territooriumilt välja viimine (v.a mobiilsed andmekandjad, mille kohta kehtib käesoleva korra punkt 11, ja sülearvutid, mille kohta kehtib käesoleva korra Lisa 1). Siia hulka kuuluvad ka tulemüüri, viirusetõrje või muude turvafunktsioonide omavoliline muutmine või välja lülitamine. Kui kasutaja soovib kasutada arvutivõrgus RA-le mittekuuluvat riistvara, peab ta seda tegema vastavalt käesoleva korra punktile 14.
- 5.8. Sinihammas (*bluetooth*), NFC (*NearFieldCommunication*) ja avaliku võrgu teenus (*wifi*) ja infrapunaliidesed peavad olema välja lülitatud, kui neid parasjagu ei kasutata.
- 5.9. Kasutaja on kohustatud arvutitöökohta paigutama nii, et kõrvalisel isikul ei oleks võimalik näha ekraanil kuvatavaid andmeid, samuti välistama arvuti kasutamise teise isiku poolt. Keelatud on jätta järelevalveta IKT vahendeid kohtadesse, kus on oht nende sattumiseks kõrvaliste isikute valdusesse.
- 5.10. Kasutaja on kohustatud kasutama talle teenistus- ja tööülesannete täitmiseks antud IT vara heaperemehelikult, et vältida selle kahjustumist, vargust või kaotamist, mitte andma IT vara kasutamiseks kolmandale isikule ning pärast kasutamisperioodi lõppu tagastama IT vara samas seisukorras vastuvõetule, arvestades vara normaalset kulumist. Vara varguse, kahjustumise, hävimise või kaotamise korral tuleb esimesel võimalusel teavitada IT-kasutajatuge ja üldosakonda.
- 5.11. Arvuti juurest lahkudes peab kasutaja sulgema arvuti või lühema pausi korral selle lukustama (näiteks Windows logo klahv + L). Kui arvutivõrku kasutatakse isikliku kiipkaardiga (nt ID-kaart), tuleb arvuti juurest lahkudes kiipkaart kaasa võtta. Arvutil on ka parooliga kaitstud ekraanilukk, mis rakendub automaatselt, kui seadet ei ole 10 minuti jooksul kasutatud.
- 5.12. Töö lõpetamisel on kasutaja kohustatud sulgema kõik kasutusel olnud infosüsteemid ja rakendused, arvuti lukustama ja võtma kasutusele kõik meetmed välistamiseks dokumentide ning mobiilsete andmekandjate sattumist võõrastesse kätte.

6. Paroolinõuded

- 6.1. Arvutivõrgu ja arvutivõrgus asuvate infosüsteemide kasutamiseks saab iga kasutaja personaalse kasutajatunnuse, üldjuhul kujul eesnimi.perenimi, ja parooli. Samuti saab arvutisse sisenemiseks kasutada personaalset kiipkaarti (nt ID-kaart) ja selle juurde

- kuuluvat PIN koodi. Arvutivõrgus asuvate infosüsteemide juurdepääs toimub kas kasutajatunnuse ja parooli, ID-kaardi või Mobiil-ID-ga.
- 6.2. Kasutaja kohustub arvutivõrku ja infosüsteemidesse sisenema ainult oma personaalse kasutajatunnuse ja parooli või kiipkaardiga ning vastutab temale antud paroolide saladuses hoidmise eest. Kui tegemist on kaugtööga, ei tohi kasutaja kasutajatunnuse või kiipkaardi abil arvutivõrgu ressursse kasutada teised isikud.
 - 6.3. Kui parool või kiipkaardi PIN kood on saanud teatavaks kõrvalistele isikutele või sellise kahtluse korral, on kasutaja kohustatud parooli või PIN koodi koheselt muutma või paluma parooli/kiipkaardiga seotud kasutajaõigused IT-kasutajatoel tühistada.
 - 6.4. Parool, mis kasutajale kasutajaõiguste saamisel antakse, on ühekordne (kui vastava infosüsteemi kasutamishuud ei sätesta teisiti) ning kasutaja kohustub selle vahetama esimesel sisse logimisel ainult temale teadaoleva parooli vastu.
 - 6.5. Parool peab olema valitud selliselt, et seda on võimalik meelde jätta, kuid pole lihtne ära arvata.
 - 6.6. Parooli ei ole lubatud ühelegi andmekandjale krüpteerimata kujul jäädvustada või dokumenteerida ega teatavaks teha ühelegi kolmandale isikule.
 - 6.7. Parool peab koosnema suur- ja väiketähtede ning numbrite ja kirjavahemärkide kombinatsioonist. Parooli pikkus peab olema vähemalt 12 sümbolit.
 - 6.8. Parool ei tohi olla:
 - 6.8.1. suvaline nimi, sõnaraamatus leiduv sõna või kuupäev;
 - 6.8.2. koostatud vaid ühesugusustest sümbolitest ega klaviatuurijärjestuses tähtedest või numbritest;
 - 6.8.3. tuletatud kasutaja isiklikust informatsioonist, mida keegi võib lihtsa vaevaga ära arvata, näiteks kasutaja nimi, pereliikme või lemmiklooma nimi, oma telefoni- või autonumber, enda või perekonnaliikmete sünnipäev või aadress jne;
 - 6.8.4. lihtsasti tuletatav eelnevalt kasutatud paroolidest, näiteks muutes paroolis ühte tähte või numbrit.
 - 6.9. Parooli tuleb vahetada regulaarselt, parooli kehtivusaeg on kuni 90 päeva. Parooli vahetamise vajadust tuletatakse kasutajale meelde sisse logimisel vähemalt 5 päeva enne parooli aegumist.
 - 6.10. Parooli kolmekordsel valesti sisestamisel arvuti kasutajakonto lukustub. Kasutajakonto taasavamiseks tuleb pöörduda IT-kasutajatoe poole.
 - 6.11. Parooli ununemise või mittetöötamise korral teavitab kasutaja sellest koheselt IT-kasutajatoe, kes loob kasutajale uue ühekordse parooli. Parool edastatakse kasutajale viisil, mis võimaldab isikutuvastust, st IT-kasutajatoe peab veenduma, et kasutaja on tõepoolest see, kes ta väidab end olevat.
 - 6.12. Oma isiklikku parooli ega PIN koodi ei tohi kasutaja kellelegi avalikustada. IT-kasutajatoel on olemas eraldi juurdepääsuõigused kasutaja probleemide lahendamiseks ning ta ei pea teadma kasutaja parooli.

7. Võrgukettad, failide hoidmine ja printimine

- 7.1. Arvutivõrgu kasutajakonto annab igale kasutajale õiguse kasutada personaalset võrguketast ning vastavalt temale antud juurdepääsuõigustele asutuse ja erinevate struktuuriüksuste ja teemadega seotud võrgukettaid.
- 7.2. Asutuse, struktuuriüksuste ja erinevate teemadega seotud võrguketastele antakse juurdepääsuõigused vastavalt *Arvutivõrgu ja infosüsteemide juurdepääsuõiguste haldamise korrale*.

- 7.3. Iga kasutaja jaoks ette nähtud personaalsel võrgukettal olevad dokumendid on kättesaadavad vaid kasutajale endale. Personaalsele võrguketale viitab ka kasutaja töölaual olev kodukataloog (Minu dokumendid/My Documents).
- 7.4. Arvutivõrgu ressursside säästliku kasutamise eesmärgil on iga kasutaja personaalsel võrgukettal limiit (RA võrguketaste limiidid on sätestatud 6.02.2019 RA ja TEHIKu vahel sõlmitud teenuslepingu nr 1-10/1702-1 lisas 2 Arvutitöökoha käideldavusnõuded – alates 2019.aasta juulist tööle asunud töötajate võrguketaste mahupiirang on 10GB). Kasutajat teavitatakse limiidi lähenemisest. Teate saanud kasutaja peab üleliigsed failid võrgukettalt kustutama või pöörduma failide arhiveerimiseks või limiidi suurendamiseks IT-kasutajatoe poole.
- 7.5. Kasutaja peab hoidma töödeldavaid faile võrguketastel ning vältima failide salvestamisest arvuti kõvaketale. Võrguketastel olevatest failidest tehakse regulaarselt varukoopiaid.
- 7.6. Failide salvestamisel võrguketastele tuleb võimalusel jälgida, et failid oleksid kättesaadavad vaid isikutele, kes tohivad neile juurde pääseda.
- 7.7. Juurdepääsupiiranguga informatsiooni printimisel või paljundamisel tuleb väljaprintitud või paljundatud materjal koheselt pärast printimist printerist või paljundamist koopiaimasinast eemaldada. Leides printerisse või koopiaimasinasse unustatud juurdepääsupiiranguga materjali, tuleb see kas omanikule koheselt ära viia (kui on teada) või panna andmekandjate hävitamise suletud kasti.
- 7.8. Kasutajatel on keelatud hoida failiserveris faile, mille sisu on ebaseaduslik, ebaeetiline või kahjustab riigi või asutuse mainet.
- 7.9. Kasutaja on kohustatud regulaarselt korrastama endaga seotud failiserveris asuvaid andmeid, kustutades ebaolulised failid.

8. Elektronpost

- 8.1. Iga kasutaja jaoks on ettenähtud isiklik elektronposti kasutajakonto, mille juurde kuulub ka kalendri ja tööülesannete haldamise võimalus.
- 8.2. Elektronposti aadressi kasutamine on lubatud üksnes asutuse teenistus- või tööülesannete täitmiseks.
- 8.3. Arvutivõrgu ressursside säästliku kasutamise eesmärgil on igal elektronposti kasutajakontol limiit (RA elektronpostkastide limiit uutele kasutajatele alates 2019. aasta juulist on 5 GB), mille ületamisel on kasutaja kohustatud kustutama või arhiveerima vanad elektronkirjad. Kasutajat teavitatakse limiidi lähenemisest ning kasutaja peab üleliigsed kirjad kontolt kustutama või pöörduma limiidi suurendamiseks IT-kasutajatoe poole.
- 8.4. Kasutajal on keelatud avada kahtlust tekitava pealkirjaga või kahtlustäratavalt elektronposti aadressilt saabuvat elektronkirja ning käivitada elektronkirjade manuses olevaid programme või skripte.
- 8.5. Kasutaja ei tohi suunata elektronkirju automaatselt edasi asutusevälistele elektronposti aadressidele. Kirjade manuaalsel edasisaatmisel tuleb alati jälgida, et tahtmatult ei saadetakse välja juurdepääsupiiranguga teavet kõrvalistele isikutele.
- 8.6. Kasutajal on keelatud tööalaste juurdepääsupiiranguga andmete saatmine või vastuvõtmine, kasutades selleks isiklikku asutusevälist elektronposti („gmail.com“, „hotmail.com“, „hot.ee“ jne).
- 8.7. Andmed, mille avalikuks tulek võib põhjustada asutusele olulist kahju, tuleb edastada krüpteeritult kasutades selleks asutuse sertifikaati, ID-kaardi rakendust või programmi VeraCrypt, mille saab vajadusel kasutaja arvutisse paigaldada IT-kasutajatugi.

- 8.8. Kasutaja on kohustatud regulaarselt korrastama postkasti kustutades ebaolulised kirjad ja failid, vajadusel salvestades olulised kirjad või manused võrgukettale jms.
- 8.9. Kasutaja on kohustatud teenistusest või töölt eemal viibimisel, nt puhkuse, puhul aktiveerima enda meilikonto automaatvastuse, kus märgib ära enda eemaloleku perioodi või naasmise kuupäeva ning enda asendaja või selle puudumisel ameti üldised kontaktid.

9. Faks, skänner ja muud sarnased väikeseadmed

- 9.1. Fakside, skännerite ja muude sarnaste infotehnoloogiliste väikeseadmete toimimise eest vastutab RA üldosakond.
- 9.2. Asutuse põhifaksiaparaadi sihipärase kasutamise ja hoolduse korraldamise eest vastutab üldosakonna dokumendihalduse spetsialist. Järelevalveosakonna ruumide juures oleva faksiaparaadi sihipärase kasutamise ja hoolduse korraldamise eest vastutab järelevalveosakonna spetsialist (dokumendihalduse alal).
- 9.3. Väikeseadmete kasutamisel peab iga kasutaja tegema kõik endast oleneva, et tagada juurdepääsupiiranguga teabe adekvaatne kaitse.
- 9.4. Sissetulevad faksid edastatakse määratud meiliaadressile, et vältida tarbetut väljaprintimist.

10. Avaliku võrgu (interneti) kasutamine

- 10.1. Avalikke traadita võrguga internetipunkte kasutades peab kasutaja arvestama, et reeglina on need ebaturvalised.
- 10.2. Kasutajal on keelatud edastada läbi sõnumivahetusprogrammide, foorumite, blogide, kommentaaride jne krüpteerimata teavet, mis ei ole mõeldud avalikuks kasutamiseks.
- 10.3. Kasutajal on keelatud laadida internetist ilma IT-kasutajatoe loata alla mistahes programme, programmiuendusi, mänge jms.
- 10.4. Kasutajal on keelatud internetis, v.a otseste teenistus- või tööülesannete täitmiseks, külastada veebilehti, mille kasutamise avalikuks tulemine võib tuua kaasa asutuse või riigi maine kahjustumise (näiteks piraatlusega tegelevad lehed).

11. Digitaalsed andmekandjad

- 11.1. RA-s tohib kasutada vaid asutuse poolt hangitud andmekandjaid. Kui on vajadus kasutada isiklikku või asutuseväliselt isikult saadud andmekandjat, siis peab olema veendunud selle turvalisuses ning vajadusel pöörduma andmekandja kontrollimiseks IT-kasutajatoe poole.
- 11.2. Mobiilsete andmekandjate kasutamisel tuleb arvestada, et nende kasutamine on kõrgendatud ohu allikas. Mobiilseid andmekandjaid on lihtne kaotada, varastada ja neid võidakse kasutada arvuti viirustega nakatamiseks.
- 11.3. Kui tökohustuste tõttu on mõnes arvutis vajalik sagedasti mobiilsete andmekandjate kasutamine, mis ei ole IT-teenuse osutaja poolt soetatud, tuleb see IT-kasutajatoega kokku leppida. Vajadusel tõstetakse sellise arvuti turvalisust või lepitakse kokku milliseid andmekandjaid usaldatakse.
- 11.4. Juurdepääsupiiranguga teavet sisaldava mobiilse andmekandja ühendamisel arvutiga või juurdepääsupiiranguga teabe kopeerimisel mobiilsele andmekandjale, tuleb võimalusel eelistada juhtmega ühendust juhtmevaba ühenduse (nt sinihammas, infrapuna) asemel.

- 11.5. Andmete salvestamine mobiilsele andmekandjale on lubatud vaid otseste teenistus- või tööülesannete täitmiseks ning selliste andmete salvestamisel mobiilsele andmekandjale tuleb andmed krüpteerida kasutades selleks asutuse sertifikaati, ID-kaardi rakendust või programmi VeraCrypt, viimase saab vajadusel kasutaja arvutisse paigaldada IT-kasutajatugi.
- 11.6. Kui juurdepääsupiiranguga andmete hoidmine mobiilsel andmekandjal ei ole enam teenistus- või tööülesannete täitmiseks vajalik, tuleb andmed andmekandjalt kohekselt kustutada või andmekandja hävitada.
- 11.7. Mobiilse andmekandja andmisel teise isiku valdusesse tuleb eelnevalt veenduda, et andmekandja ei sisalda teavet, millele andmekandja saanud isik juurdepääsu omada ei tohi.
- 11.8. Juurdepääsupiiranguga andmeid sisaldava mobiilse andmekandja kadumisest või vargusest tuleb kohekselt teavitada IT-kasutajatuge.

12. Kaugtöö ehk töö väljaspool asutuse arvutivõrku

- 12.1. 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 (vt lisaks *Sisekorraeeskirja Lisa 1 Kaugtöö juhend Ravimiametis*).
- 12.2. Kaugtöö on võimalik ainult RA sülearvutist, et tagada ja kontrollida selle turvalisust.
- 12.3. Kaugtöö tegemise eelduseks on kiire ja stabiilse internetiühenduse olemasolu. Kaugtöö tegemiseks kasutatakse VPN ühendust.
- 12.4. Kaugtöö tegemiseks vajalikud IT varad väljastab TEHIK asutuse aadressile ning ei taga IT varade paigaldamist ja seadistamist kasutaja kodukontoris.
- 12.5. Kaugtöö tegemisel asutuse sülearvutist tuleb järgida ka käesoleva korra Lisas 1 toodud sülearvutite kasutamise nõudeid.
- 12.6. Kasutajad on kohustatud tagama kaugtöökohta turvalisuse samaväärselt ameti tööruumide tingimustele. Avalikus kohas tuleb seadmeid kasutada turvaliselt, kaitstes neid varguse, rikkumise, ekraanil oleva info liigse avalikkuse ja teiste ohtude eest.

13. RA arvutivõrgu mobiilsideseadmetega kasutamine

- 13.1. Mobiilsideseadmetega (tahvelarvuti, mobiiltelefon, nutikell) arvutivõrgu kasutaja peab arvestama, et seadet kasutatakse väljaspool asutuse turvatud arvutivõrku mistõttu see teeb seadmest kõrgendatud ohu allika ning paneb selle kasutajale lisavastutuse. Kuivõrd mobiilsideseade hävimise, kaotamise või varastamise tõenäosus on suur, siis juurdepääs mobiilsideseadmete kaudu RA andmetele antakse põhjendatud tööalase vajaduse korral ning ajaks, millal andmete kasutamine on tööalaselt vajalik.
- 13.2. Mobiilsideseadmega arvutivõrgu kasutamiseks saab kasutada nii asutusele kuuluvaid mobiilsideseadmeid kui kasutajale isiklikult kuuluvaid seadmeid. TEHIK ei garanteeri RA arvutivõrgu juurdepääsu RA-le mittekuuluva mobiilsideseadmega. Samuti ei vastuta TEHIK sellise seadme riknemise või seadmes olevate andmete kaotsi mineku eest.
- 13.3. Mobiilsideseadmega on juurdepääs asutuse elektronpostile ja kalendritele. Asutuse võrguketastele ja infosüsteemidele mobiilsideseadmetega juurdepääs ei ole võimalik.
- 13.4. Mobiilsideseadme kasutamisel dokumentide salvestamiseks või transportimiseks loetakse mobiilsideseadet ühtlasi mobiilseks andmekandjaks ja sellele kehtivad samad reeglid, mis on kehtestatud mobiilsetele andmekandjatele käesoleva korra punktis 11.
- 13.5. Mobiilsideseadmega on lubatud elektronpostile ja kalendritele juurde pääseda Exchange Activesync (EAS) abil, mis kujutab endast mobiilsideseadmele mõeldud teenust

seadmega elektronposti, kalendri ja kontaktide sünkroniseerimiseks. EASi kasutamine mobiilsideseadmes toimub vastavalt EASi kasutamise juhendile (vt siseveeb – IT-abi - Kasutusjuhendid). EASi lubamiseks peab kasutaja vahetu juht või RA üldosakond tegema IT-kasutajatoele vastavasisulise pöördumise, kus on ära toodud mobiilsideseadme tootja ja mudel ning põhjendus elektronposti ja kalendri sünkroniseerimise vajaduse kohta.

- 13.6. EASi kasutamisel hoitakse mobiilsideseadmes kasutaja elektronposti ja kalendri sisu ning avatud mobiilsideseadmega on võimalik reaalajas, ilma parooli küsimata, juurdepääs kasutaja elektronposti kontole ja elektronkirjadele. Seetõttu rakendatakse EASi kasutamisel mobiilsideseadmele mitmeid piiranguid ning kasutaja seadme kasutamisel järgima kõiki seatud turvanõudeid (vt täpsemalt *EASi kasutamise juhendist*).

14. RA mittekuuluva IKT-vahendi kasutamine asutuse arvutivõrgus

- 14.1. Kui otseste tööülesannete täitmiseks on vajalik, et RA arvutivõrku või arvuti külge ühendataks asutusele mittekuuluv IKT vahend, tuleb see kooskõlastada TEHIKuga. Selleks tuleb saata pöördumine IT-kasutajatoele, kus on kirjas IKT vahendi täpne mark ja mudel, kasutamise eesmärk ning kas vahend ühendub arvutivõrgu või arvuti külge.
- 14.2. IT-kasutajatugi võib pakkuda välja alternatiivi asutusele mittekuuluva IKT vahendi kasutamiseks asutuse arvutivõrgus. Kui alternatiivi ei leita ja IKT vahend ei kujuta TEHIKu arvates ohtu asutuse arvutivõrgu ja süsteemide turvalisusele või käideldavusele, lubatakse IKT vahendi kasutamine vastavalt TEHIKu nõuetele.
- 14.3. Kõigist asutusele mittekuuluvatest IKT vahendite kasutamise lõpetamisest RA võrgus või arvutis peab kasutaja koheselt teavitama IT-kasutajatuge.

15. Info- ja kommunikatsioonitehnoloogia vahendite tellimine ja tagastamine

- 15.1. Kõigile kasutajatele on IKT standardtöökohaseadmetena ette nähtud lauaarvuti või sülearvuti ja dokk, monitor, klaviatuur, juhtmega hiir ja vajalikud ühenduskaablid ning standardtarkvarana MS Office, Outlook, dokumendihaldussüsteem ja tööks vajalikud infosüsteemid.
- 15.2. Standardtöökoha seadmete või standardtarkvara tellimiseks uuele kasutajale teeb IT-kasutajatoele pöördumise RA personalispetsialist (vajadusel ka üldosakonna juhataja või haldusspetsialist) kümme tööpäeva enne vara kasutama hakkamist. Pöördumises tuleb tuua välja vara kasutaja ees- ja perekonnanimi, isikukood, töökoha asukoht, töö alustamise kuupäev, vajalike IT-varade kirjeldus ja selgitus vara vajaduse kohta, kui tegemist ei ole standardtöökoha seadmega (vt lisaks *TEHIKu IT varade kord*).
- 15.3. IT vara asendamiseks teistsuguse seadme vastu või täiendamiseks esitab kasutaja osakonna juht või RA üldosakonna juhataja või haldusspetsialist IT-kasutajatoele vabas vormis taotluse, mis sisaldab vähemalt vara kasutaja ees- ja perekonnanime, töökoha asukohta, IT vara nimetust/kirjeldust ja selgitust vara asendamise või täiendamise vajaduse kohta ning vajadusel olemasolevate IT varade koode. TEHIKu IT varahaldur hindab taotlust, vajadusel täpsustab ning kui vara asendamine või täiendamine on põhjendatud kooskõlastab vara taotluse, misjärel kasutaja varad asendatakse või täiendatakse vastavalt taotlusele.
- 15.4. IT varasid ei pea eraldi taotlema, kui olemasolev IT vara ei ole töökorras, sellisel juhul teeb kasutaja ise pöördumise IT-kasutajatoele kirjeldades mittetöötamise põhjuseid ja IT-kasutajatugi tellib vara väljavahetamise.

- 15.5. TEHIK võib IT varasid välja vahetada IT vara rendiperioodi lõppedes ja/või vastavalt vajadusele (amortiseerunud, vananenud). Sellisest vahetusest teavitab IT varahaldur ette vähemalt kümme tööpäeva ning IT-spetsialist lepib kasutajaga kokku IT varade vahetamise aja.
- 15.6. IT-vara kasutamise kohta sõlmitakse kasutajaga IT-vara kasutamise kokkulepe Riigitöötaja Iseteenindusportaalil.
- 15.7. Mittestandardseid IT-väikevarasid (nt kõlarid, kõrvaklapid, USB kettaseadmed, mälupulgad, toonerid, juhtmeta hiired jne) hangib RA üldosakond (vt ka *TEHIKu hangitavate IT väikevarade loetelu ja arveldamise korda*). Selliste varade saamiseks tuleb kasutajal pöörduda üldosakonna poole.
- 15.8. Kui IT vara kasutaja lahkub asutusest või vahendi kasutamine pole enam töö- või teenistusülesannete täitmiseks vajalik, teavitab RA üldosakond IT-kasutajatuge vabaks jäänud IT vahendist ning kasutaja peab tagastama kõik tema kasutuses olnud ameti tark- ja riistvaralised süsteemid. Mittestandardseid IT-väikevarad tuleb tagastada RA üldosakonda.
- 15.9. Defektsed ja kasutuskõlbatud andmekandjad tuleb anda hävitamiseks RA üldosakonnale.

16. IT-kasutajatugi

- 16.1. Kasutaja on kohustatud esimesel võimalusel teavitama IT-kasutajatuge IT-teenuste kasutamist takistavatest või potentsiaalselt teenuse kasutamist takistavatest juhtumitest ja turvaintsidentidest.
- 16.2. IT-kasutajatoes registreeritud juhtumeid nimetatakse kasutaja pöördumiseks.
- 16.3. IT-kasutajatoesse saab kasutaja pöörduda:
 - 16.3.1. läbi arvuti töölaual asuva IT-abi lingi;
 - 16.3.2. kasutades elektronposti aadressi itabi@tehik.ee;
 - 16.3.3. helistades telefoninumbril 794 3913.
- 16.4. IT-kasutajatoesse laekunud pöördumised registreeritakse, neile määratakse prioriteet lähtudes TEHIKU teenindussoovide ja intsidentide prioriseerimise maatriksile ning suunatakse kindlaksmääratud lahendaja(te)le.
- 16.5. Pöördumise kiire lahendamise tagamiseks peab kasutaja edastama juhtumi teatamisel IT-kasutajatoele järgneva informatsiooni:
 - 16.5.1. oma ees- ja perekonnanime, kui probleem edastatakse telefoni teel;
 - 16.5.2. tõrke tekkimise kuupäeva (sh võimalusel kellaaja) ja arvuti koodi (00VV00...), kus tõrge tekkis;
 - 16.5.3. infosüsteemi nimetuse, kus tõrge tekkis;
 - 16.5.4. veateade ekraanilt, saates IT-kasutajatoele võimalusel ekraanipildi failina;
 - 16.5.5. kui tegemist on vea kahtlusega, lisada teatele kirjeldus õigeks peetavast lahendusest.

17. Arvutivõrgu ja IT varade väärkasutuse tagajärjed

- 17.1. Kahtluse tekkimisel arvutivõrgu kasutamise reeglite rikkumise või võrgu väärkasutuse osas on TEHIKu IT-spetsialistidel õigus peatada või piirata kasutusõigust kuni asjaolude selgitamiseni. Kasutaja õiguste peatamisest või piiramisest peab IT-spetsialist viivitamatult teavitama kasutajat ja tema vahetut juhti.
- 17.2. Arvutivõrgu või infosüsteemi kasutamist reguleerivate õigusaktide mittetäitmine võib tuua kaasa kriminaal-, väärteo- või distsiplinaarkaristuse.

- 17.3. IT vahendi süülise rikkumise korral on vara soetanud asutusel õigus nõuda kahju hüvitamist. Kahju tekkimisel esitab kasutaja TEHIKule seletuskirja kahju tekkimise asjaolude kohta, kes hindab IT vara kahjustamise ajaolusid.
- 17.4. Kui IT vara kasutaja on tahtlikult vara kahjustanud, vastutab ta kogu tekitatud kahju eest isiklikult. Kui kasutaja on tekitanud varale kahju hooletuse või raske hooletuse tõttu, vastutab ta tekitatud kahju eest ulatuses, mille määrab tööandja iga juhtumi puhul individuaalselt.
- 17.5. Hüvitamiskohustuse määramisel arvestatakse süü vormi ja selle tagajärgede raskust, kasutajale antud juhiseid vara kasutamiseks, töötingimusi, töö iseloomust tulenevat riski, senist käitumist ning mõistlikult rakendatud võimalusi kahjude vältimiseks ja kindlustamiseks.
- 17.6. Vääramatust jõust tingitud IT varade rikkumisest või hävimisest tulenevad taastamiskulud katab TEHIK.

Lisa 1 - Ravimiameti sülearvutite kasutamise kord

1. Sülearvuti mobiilsus ja võimalus sülearvutit kasutada väljaspool asutuse turvatud arvutivõrku teeb sülearvutist kõrgendatud ohu allika ning paneb kasutajale lisavastutuse.
2. Kasutajal on keelatud sülearvutit edasi anda kasutamiseks kolmandale isikule.
3. Vältimaks sülearvuti varastamist, kaotamist või riknemist peab kasutaja:
 - 3.1. hoidma sülearvutit avalikes kohtades alati isikliku järelevalve all;
 - 3.2. mitte jätma sülearvutit valveta kohtadesse, kus on oht selle varastamiseks (auto salong, avalikku kohta järelevalveta, lahtise akna alla jne);
 - 3.3. mitte jätma sülearvutit magnetvälja, otsese päikesekiirguse või kõrge temperatuuri kätte, samuti tolmusesse või niiskesse keskkonda;
 - 3.4. transportima sülearvutit turvaliselt, et vältida selle hävinemist,
 - 3.5. reisimisel kandma sülearvutit käsipagasis.
4. Sülearvuti vargusest, kaotamisest või hävimisest on kasutaja kohustatud viivitamatult teavitama IT-kasutajatuge. Sülearvuti varguse korral on kasutaja kohustatud koheselt teavitama ka politseid.
5. Tagamaks sülearvutis olevate andmete turvalisust ja piiramaks pahavara levikut peab kasutaja:
 - 5.1. arvestama, et väljaspool asutuse sisevõrku (eriti avalikes *wifi* võrkudes) võidakse krüpteerimata ühendusi pealt kuulata;
 - 5.2. eelistama sülearvutisse logimiseks parooli asemel kiipkaardi ja PIN koodi kombinatsiooni;
 - 5.3. sisestama paroolid või kiipkaardi PIN koodi nii, et kõrvalised isikud ei näeks, milline parool/PIN kood sisestati;
 - 5.4. sülearvuti juurest lahkumisel sulgema sülearvuti ja eemaldama kiipkaardi (kui seda kasutati sülearvutisse logimiseks);
 - 5.5. juhtmeta ühenduste (*wifi*, infrapunaliides, sinihammas) kasutamisel vältima nende tarbetut aktiveerimist ning konfidentsiaalsete andmete töötlemisel eelistama kaabelühendust;
 - 5.6. lülitama välja kõik sülearvuti juhtmeta (*wifi*, infrapunaliides, sinihammas) ühendused, kui sülearvuti on asutuse arvutivõrgus võrgukaabliga;
 - 5.7. kahtluse või teadmise korral, et sülearvuti tulemüür ja/või viirusetõrjetarkvara ei ole töökorras või on välja lülitatud, mitte ühendama sülearvutit avalikku arvutivõrku, vaid teavitama sellest võimalikult kiiresti IT-kasutajatuge, kes korraldab arvuti ülevaatamise;
 - 5.8. kahtluse või teadmise korral, et sülearvutis on pahavara, mitte ühendama sülearvutit RA ega avalikku arvutivõrku, vaid teatama juhtunust IT-kasutajatuge, kes korraldab arvuti üle vaatamise.
6. Kasutaja peab arvestama, et sülearvuti kõvaketta rikke korral võivad hävida sülearvutis olevad varundamata andmed. Et tagada andmete säilimine peab kasutaja:
 - 6.1. töötades asutuse arvutivõrgus hoidma andmeid selleks määratud võrgukettal;
 - 6.2. ühendades sülearvuti RA arvutivõrku, tegema koheselt kõvakettal olevatest andmetest varukoopia selleks määratud võrgukettale, kasutaja kodukataloog varundatakse arvutivõrku automaatselt;
 - 6.3. töötades pikemaajaliselt RA arvutivõrgu ühenduseta, tegema olulistest failidest koopia mobiilsele andmekandjale. Varukoopia salvestamisel mobiilsele andmekandjale peab viimast adekvaatselt kaitsma varguse, hävimise ja kaotamise eest.

- 6.4. sülearvuti toiteallika (ehk aku) tühjenemisega kaasneva võimaliku andmekao vältimiseks peab kasutaja toite hoiatussignaali või märguande korral kohe salvestama poolelioleva töö.
7. Kasutaja peab sülearvutiga käima Ravimiameti (kaabli)arvutivõrgus vähemalt üks kord kvartalis, et arvuti saaks vajalikud uuendused ning arvuti probleemide korral tuleb kohe pöörduda IT-kasutajatoe poole.
8. IT-kasutajatoe nõudmisel peab kasutama tooma sülearvuti IT-spetsialisti kätte korraliseks hoolduseks. Enne sülearvuti hooldusesse andmist peab kasutaja veenduma, et kõikidest vajalikest andmetest, mis on salvestatud sülearvuti kõvakettale, on tagavarakoopiaid andmete hoidmiseks ettenähtud võrgukettal.
9. Põhjendatud juhtudel väljastatakse sülearvuti asutuse struktuuriüksusele ühiskasutuseks, sellisel juhul kehtivad järgmised reeglid:
 - 9.1. ühiskasutuses oleva sülearvuti puhul määratakse väljastamise hetkel sülearvuti kasutamise eest üks vastutav isik (edaspidi *vastutaja*);
 - 9.2. vastutaja on kohustatud pidama vabas vormis kirjalikku arvestust kogu oma vastutust aja jooksul, kellele on sülearvuti millisel ajahetkel kasutusse antud ning millises seisukorras see on tagastatud;
 - 9.3. kui vastutaja annab sülearvuti teisele kasutajale, siirdub vastutus sülearvuti eest vastutajalt kasutajale ja tagastamisel jälle kasutajalt vastutajale;
 - 9.4. vastutaja peab veenduma, et kõik kasutajad, kellele vastutaja sülearvuti kasutada annab, on tutvunud sülearvutite kasutamise nõuetega;
 - 9.5. iga kasutaja kasutab sülearvutit oma personaalse kasutajakontoga, mis peab olema enne sülearvuti kasutusse andmist nõuetekohaselt seadistatud IT-spetsialisti poolt;
 - 9.6. juhul, kui sülearvuti vastutaja ei suuda tõestada, kelle kasutuses sülearvuti süülise kahju tekkimise hetkel oli, nõutakse kahjuhüvitist sülearvuti eest vastutajalt.
10. Kui sülearvuti on soetatud Ravimiameti eelarvelistest vahenditest, ei anta seda IT-kasutajatoe poolt uude kasutusse teise haldusala kasutajale, v.a juhul kui selleks avaldab soovi sülearvuti soetanud asutuse juht või tema poolt määratud isik.