

Infovara kasutamise kord

SISUKORD

1. Üldsätted	1
2. Seotud dokumendid	1
3. Mõisted	2
4. Kasutaja õigused.....	2
5. Kasutaja kohustused	2
6. Paroolinõuded	3
7. <i>Onedrive, SharePoint, Teams</i>	4
8. E-post.....	4
9. Avaliku võrgu (interneti) kasutamine, sh sotsiaalmeedia ja tehisintellekt.....	5
10. Printimine.....	6
11. Mobiilsed andmekandjad	6
12. Mobiilsideseadmete kasutamine.....	6
13. Arvutitöökohateenuse juurde mittekuuluva IKT-vahendi kasutamine.....	7
14. Kaugtöö ehk töö väljaspool ameti kohtvõrku.....	8
15. Info- ja kommunikatsioonitehnoloogia vahendite tellimine ja tagastamine.....	8
16. Infovara väärkasutuse tagajärjed	9
Lisa 1 - Sülearvutite kasutamise kord	10

1. Üldsätted

- 1.1. Käesolev kord sätestab Ravimiameti (edaspidi amet) infovara kasutaja õigused ja kohustused, et kaitsta ja hallata asutuse infotehnoloogilisi vahendeid, infosüsteeme ja andmeid.
- 1.2. Käesolev kord kehtib kõikidele ameti infovara kasutajatele ning kõikidele arvutivõrku ühendatud seadmetele ja tööjaamadele (sülearvuti, dokk jne).

2. Seotud dokumendid

- 2.1. Infoturvapoliitika;
- 2.2. Infovara juurdepääsuõiguste haldamise kord;
- 2.3. Andmekaitse kord;
- 2.4. Riigi IT Keskuse (RIT) arvutitöökohateenuse kasutusjuhendid töölaua IT-abi keskkonnas;
- 2.5. Tervise ja Heaolu Infosüsteemide Keskuse (TEHIK): [infosüsteemide teenustingimused](#).

3. Mõisted

- 3.1. Kasutaja – isik, kellele on antud ameti infovara ja selle kasutusõigused, sh kõik ametiga töö- või teenistussuhtes olevad ametnikud, töötajad või muu lepingu (nt käsundusleping, töövõtuleping) alusel ameti huvides tegutsevad isikud;
- 3.2. Infovara - informatsioon ja andmed ning nende töötlemiseks vajalikud infotehnoloogilised rakendused ja tehnilised vahendid;
- 3.3. IKT vahend – info- ja kommunikatsioonitehnoloogia vahend ehk andmete töötlemise, salvestamise ja edastamise tehnilised vahendid, näiteks sülearvuti, monitor, printer jne;
- 3.4. Mobiilsideseade – teatud liiki IKT vahend, näiteks tahvelarvuti, mobiiltelefon jms;
- 3.5. Irdmeedia – USB-pordi või juhtmevaba ühenduse kaudu arvutiga ühendatav väline digitaalne andmekandja (telefon, fotokaamera, mälupulk, väline kõvaketas, diktofon, CD/DVD lugeja, kirjutaja) või seade (dokk, hiir, klaviatuur, kuvar, printer);
- 3.6. Digitaalne andmekandja – seade, millele saab salvestada või millelt lugeda digitaalset infot. Mobiilseteks loetakse andmekandjatest neid, mida saab kaasas kanda ning ilma arvuti korpust avamata arvuti küljest või arvutivõrgust eemaldada või sinna lisada;
- 3.7. Juurdepääsupiiranguga teave – teave, mis seaduse, lepingu või mõnel muul alusel on kuulutatud mitteavalikuks;
- 3.8. Intsidend – ootamatu rike (mis ei ole normaalse/standardse teenuse osa), mis põhjustab või võib põhjustada IT-teenuse planeerimata katkestuse või teenuse kvaliteedi olulise languse;
- 3.9. 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. Infovara kasutajal on õigus omada juurdepääsu talle tööks vajalikule teabele ja teenustele. Kasutamise õigused antakse kasutajale vastavalt kasutaja teenistus- või tööülesannetele lähtudes *Infovara juurdepääsuõiguste haldamise korrast*.
- 4.2. Kasutajal on õigus saada tööks vajalikke IKT vahendeid.
- 4.3. Kasutajal on õigus saada mõistliku aja jooksul ennetavalt infot planeeritud muudatustest ja sündmustest infosüsteemides ja arvutivõrgus, kui muutused mõjutavad oluliselt teenuste kvaliteeti.
- 4.4. Kasutajal on õigus pöörduda abi saamiseks RIT IT-kasutajatoe poole e-postiaadressil itabi@rit.ee või telefonil 663 6464 ja TEHIK IT-kasutajatoe poole e-postiaadressil itabi@tehi.ee või telefonil 794 3913. IT-kasutajatugi haldab pöördumisi vastavalt prioriteetsusele, mis määratakse mõju ja kasutajate arvu alusel.
- 4.5. Kasutajal on õigus esitada ettepanekuid infovara kasutamise ja infoturbe paremaks korraldamiseks.

5. Kasutaja kohustused

- 5.1. Kasutaja on kohustatud järgima ametis kehtivaid kordasid ja teenuseosutaja (RIT, TEHIK) juhendeid ning infovara kasutamiseks kehtestatud alalisi ja ajutisi piiranguid.
- 5.2. Kasutaja on kohustatud kasutama infovara ainult teenistus- ja tööülesannete täitmiseks.
- 5.3. Kasutaja kohustub arvutivõrku ja infosüsteemidesse sisenema ainult oma personaalse kasutajatunnuse ja parooli, pin-koodi või kiipkaardiga ning ei tohi neid kellelegi (sh IT-kasutajatugi) avalikustada.
- 5.4. Kui parool või pin-kood on saanud teatavaks kõrvalistele isikutele või sellise kahtluse korral, on kasutaja kohustatud parooli või PIN koodi koheselt muutma või paluma seotud kasutajaõigused RIT või TEHIK IT-kasutajatoel tühistada.
- 5.5. Kõik infovara juurdepääsuõigused on isiklikud ning neid ei ole lubatud edasi anda.

- 5.6. Keelatud on infovara kasutamine teise isiku poolt või jätmine järelevalveta kohtadesse, kus on oht sattumiseks kõrvaliste isikute valdusesse.
- 5.7. Kasutaja on kohustatud kasutama võrguressursse optimaalselt ning mitte koormama arvutivõrku tööga mitteseotud andmete või tegevustega ega segama teiste arvutivõrgu kasutajate tööd.
- 5.8. Kasutaja peab järgima head tava ja ei tohi tekitada teistele kasutajatele või ametile oma tegevusega või tegevusetusega kahju ega ohtu arvutivõrgu turvalisusele.
- 5.9. Keelatud on omavoliline RIT *Company Portal* välise tarkvara lisamine, tule müüri, viirusetõrje või muude turvafunktsioonide omavoliline muutmine või välja lülitamine.
- 5.10. Sinihammas (*bluetooth*), NFC (*NearFieldCommunication*) avaliku võrgu teenust (*wifi*) ja infrapunaliideseid ei tohi tööalase vajaduseta aktiivsena hoida.
- 5.11. Kasutaja on kohustatud arvutitöökoha paigutama nii, et kõrvalisel isikul ei oleks võimalik näha ekraanil kuvatavaid andmeid. Arvutitöökohaga liikudes ja avalikus kohas töötades tuleb kasutada kogu ekraani katvat privaatsusfiltrit.
- 5.12. 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.
- 5.13. Kasutaja on kohustatud kasutama talle teenistus- ja tööülesannete täitmiseks antud infovara heaperemehelikult, et vältida selle kahjustumist, vargust või kaotamist, mitte andma infovara kasutamiseks kolmandale isikule ning pärast kasutamisperioodi lõppu tagastama infovara samas seisukorras vastuvõtule, arvestades vara normaalset kulumist. Vara varguse, kahjustumise, hävimise või kaotamise korral tuleb esimesel võimalusel teavitada RIT IT-kasutajatuge ja haldusspetsialisti.
- 5.14. Kasutaja on kohustatud võimalikest ja toimunud tõrgetest, rikestest ja turvaintsidentidest viivitamatult teavitama RIT või TEHIK IT-kasutajatuge ja infoturbe eest vastutavat isikut.
- 5.15. 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. Arvutisse sisselogimisel, taaskäivitamisel ja talveune režiimist ärkamisel käivitub *Bitlocker*, mille jaoks tuleb rakendada 8-20 numbriline pin-kood. Kui pin-kood ununeb või on seda üle 3 korra valesti sisestatud, tuleb ühendust võtta RIT IT-kasutajatoega.
- 6.2. Arvutitöökohateenuse kasutajakontole sisselogimine on esmakordselt ainuvõimalik ID-kaardi abil, seejärel kas ID-kaardi, sõrmejälje, iseseadistatud 8-20 numbrilise või *Windows Hello* pin-koodi abil.
- 6.3. Infosüsteemide kasutamiseks saab iga kasutaja personaalse kasutajatunnuse, üldjuhul kujul eesnimi.perenimi, ja parooli. Infosüsteemidele juurdepääs toimub kas kasutajatunnuse ja parooli, ID-kaardi või Mobiil-ID-ga.
- 6.4. Parool, mis kasutajale kasutajaõiguste saamisel antakse, on ühekordne (kui vastava infosüsteemi kasutamisejuhend ei sätesta teisiti) ning kasutaja kohustub selle vahetama esimesel sisse logimisel ainult temale teadaoleva parooli vastu.
- 6.5. Igas infosüsteemis ja rakenduses peab olema kasutusel erinev parool.
- 6.6. Parool peab olema valitud selliselt, et seda on võimalik meelde jätta, kuid pole lihtne ära arvata.
- 6.7. Parooli ei ole lubatud ühelegi andmekandjale krüpteerimata kujul jäädvustada või dokumenteerida ega teatavaks teha ühelegi kolmandale isikule.
- 6.8. Parool peab koosnema suur- ja väiketähtede ning numbrite ja kirjavahemärkide kombinatsioonist. Parooli pikkus peab olema vähemalt 16 sümbolit.

6.9. Parool ei tohi olla:

- 6.9.1. suvaline nimi, sõnaraamatus leiduv sõna või kuupäev;
 - 6.9.2. koostatud vaid ühesugusustest sümbolitest ega klaviatuurijärjestuses tähtedest või numbritest;
 - 6.9.3. tuletatud kasutaja isiklikust informatsioonist, mida keegi võib lihtsa vaevaga ära arvata, näiteks kasutaja nimi, pereleht või lemmiklooma nimi, oma telefoni- või autonumber, enda või perekonnaliikmete sünnipäev või aadress jne;
 - 6.9.4. lihtsasti tuletatav eelnevalt kasutatud paroolidest, näiteks muutes paroolis ühte tähte või numbrit.
 - 6.9.5. eelnevalt juba kasutusel olnud (sama parooli ei tohi kasutada rohkem kui üks kord).
- 6.10. Parooli tuleb vahetada regulaarselt, parooli kehtivusaeg on kuni 365 päeva. Parooli vahetamise vajadust tuletatakse kasutajale meelde sisse logimisel vähemalt 5 päeva enne parooli aegumist.
 - 6.11. Parooli kolmekordsel valesti sisestamisel arvuti kasutajakonto lukustub. Kasutajakonto taasavamiseks tuleb pöörduda TEHIK IT-kasutajatoe poole.
 - 6.12. Parooli ununemise või mittetöötamise korral teavitab kasutaja sellest koheselt TEHIK IT-kasutajad, kes loob kasutajale uue ühekordse parooli. Parool edastatakse kasutajale viisil, mis võimaldab isikutuvastust, st TEHIK IT-kasutajadugi veendub, et kasutaja on tõepoolest see, kes ta väidab end olevat.
 - 6.13. Paroolide haldamiseks on soovitatav kasutada *Passwordstate*'i paroolihoidlat.

7. *Onedrive, SharePoint, Teams*

- 7.1. Arvutitöökohateenuse kasutajakonto annab igale kasutajale õiguse kasutada *Onedrive*'i, *Teams*i ning vastavalt temale antud juurdepääsuõigustele ameti ja erinevate struktuuriüksuste ja teemadega seotud *SharePoint*i saite ja teekes, millele antakse juurdepääsuõigused vastavalt *Infovara juurdepääsuõiguste haldamise korrale*.
- 7.2. *Onedrive*'is olevad dokumendid on kättesaadavad vaid kasutajale endale. Andmete salvestamisel ja jagamisel *SharePoint*is ja *Teams*is tuleb jälgida, et need oleksid kättesaadavad vaid isikutele, kellel on selleks tööülesannetest tulenev vajadus. Seejuures *Teams*is ei ole lubatud jagada eriliigilisi isikuandmeid, muud juurdepääsupiiranguga või konfidentsiaalset teavet võib *Teams*is jagada ainult asutusesiseselt, minimaalses mahus ja volitatud isikutele.
- 7.3. Ressursside säästliku kasutamise eesmärgil on iga kasutaja *Onedrive*'is ja asutuse *Sharepoint*i saitidel ja teekides mahu limiit. Üleliigsed failid tuleb kustutada või pöörduda arhiveerimiseks dokumendihalduse spetsialisti poole.
- 7.4. Kasutaja peab hoidma töödeldavaid andmeid *Onedrive*'is, *SharePoint*is või infosüsteemides ning vältima salvestamist *Teams*i või arvuti kõvakettale.
- 7.5. Varukoopiad on kättesaadavad järgmiselt: *Onedrive* failide versioneerimine 30 päeva, prügikastist taastamise võimalus 93 päeva; *SharePoint* failide versioneerimine 30 päeva, RIT tehtud varukoopiad 1 aasta.
- 7.6. Kasutajatel on keelatud kasutada ja säilitada andmeid ja materjale, mille sisu on ebaseaduslik, ebaeetiline või kahjustab riigi või ameti mainet.
- 7.7. Kasutaja on kohustatud regulaarselt korrastama endaga seotud andmeid, kustutades ebaolulised failid.

8. E-post

- 8.1. Iga kasutaja jaoks on ettenähtud isiklik e-posti kasutajakonto, mille juurde kuulub ka kalendri ja tööülesannete haldamise võimalus.
- 8.2. E-posti aadressi kasutamine on lubatud üksnes teenistus- või tööülesannete täitmiseks. E-postkastis isiklike kirjade säilitamine on keelatud.

- 8.3. Ressursside säästliku kasutamise eesmärgil on igal e-posti kasutajakontol mahu limiit 100GB ja ühispostkastidel 50GB, mille ületamisel on kasutaja kohustatud liigsed e-kirjad kustutama või arhiveerima. Kasutajat teavitatakse limiidi lähenemisest ning kasutaja peab üleliigsed kirjad kontolt kustutama või pöörduma limiidi suurendamiseks RIT 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. Juhul, kui saatja usaldusväärsuses on veendunud, võib faile ja veebilinke kontrollida: <https://kontrolli.tehik.sise/>.
- 8.5. Kasutaja ei tohi suunata e-kirju automaatselt edasi välistele aadressidele. Kirjade manuaalsel edasisaatmisel tuleb alati jälgida, et tahtmatult ei saadetaks välja juurdepääsupiiranguga teavet kõrvalistele isikutele.
- 8.6. Kasutajal on keelatud eriliigiliste isikuandmete, asutusesiseseks kasutamiseks tunnistatud info või muu konfidentsiaalse sisuga teabe saatmine või vastuvõtmine, kasutades selleks isiklikku välist elektronposti („gmail.com“, „hotmail.com“, jne).
- 8.7. Eriliigilised isikuandmed jm *Andmekaitse korras* kirjeldatud tundlik info tuleb edastada krüpteeritult, kasutades selleks ameti sertifikaati, ID-kaardi vm RIT *Company Portal*ist allalaaditavat rakendust.
- 8.8. Kasutaja on kohustatud regulaarselt korrastama postkasti, kustutades ebaolulised kirjad ja failid, vajadusel salvestades olulised kirjad või manused infosüsteemidesse.
- 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.
- 8.10. *Outlooki* postkastist liigutatakse 180 päeva vanused e-kirjad automaatselt arhiivpostkasti. Prügikastist on võimalik kustutatud kirju ise taastada 90 päeva jooksul.
- 8.11. Ametiaja või töösuhte lõppemisel säilitatakse kasutaja isiklikku *Outlooki* postkasti 30 päeva pärast kasutaja viimast sisselogimist, misjärel kustutatakse nii peamine (põhipostkast) kui ka arhiivpostkast.

9. Avaliku võrgu (interneti) kasutamine, sh sotsiaalmeedia ja tehisintellekt

- 9.1. Avalikke traadita võrguga internetipunkte kasutades peab kasutaja arvestama, et reeglina on need ebaturvalised.
- 9.2. Kasutajal on keelatud edastada läbi sõnumivahetusprogrammide, foorumite, blogide, kommentaaride jne krüpteerimata teavet, mis ei ole mõeldud avalikuks kasutamiseks. Postituste, blogide jne avaldamine ameti võrgust on lubatud vaid juhul, kui need ei kajasta poliitikat, ameti töökorraldust, ei õhuta vaenu, ei ole solvavad, laimavad, diskrimineerivad vms.
- 9.3. Kasutajal on keelatud laadida internetist ilma RIT IT-kasutajatoe loata alla mistahes programme, programmiuendusi, mänge jms. Kasutajal on keelatud luua ameti nimel kontosid või lisada ameti kontot veebiteenustele (avalikud tehisintellekti rakendused jm).
- 9.4. Kasutajal on keelatud internetis, v.a otseste teenistus- või tööülesannete täitmiseks, külastada veebilehti, mille kasutamise avalikuks tulemine võib tuua kaasa ameti või riigi maine kahjustumise (näiteks piraatlusega tegelevad lehed).
- 9.5. Kasutajal on keelatud esineda võrgus kellegi teisena või püüda varjata oma identiteeti.
- 9.6. Pilveteenuste ja tehisintellekti rakenduste kasutamisel tuleb järgida *Andmekaitse korda*.

10. Printimine

- 10.1. Lubatud printerid saab seadistada läbi RIT *Company Portal*i.
- 10.2. Juurdepääsupiiranguga informatsiooni skaneerimisel, printimisel või paljundamisel tuleb skaneeritud, väljaprintitud või paljundatud materjal toimingujärgselt koheselt seadmest

eemaldada. Leides seadmesse unustatud juurdepääsupiiranguga materjali, tuleb see kas omanikule koheselt ära viia (kui on teada) või panna andmekandjate hävitamiseks ettenähtud kasti.

11. Mobiilsed andmekandjad

- 11.1. Mobiilsete andmekandjate kasutamine on vaikinisi kasutajale piiratud ja tööülesannete täitmise vajadusel tuleb taotleda RIT IT-kasutajatoelt erioigus vastavalt *Infovara juurdepääsuõiguste haldamise korrale*.
- 11.2. Ametis tohib kasutada vaid ameti poolt hangitud ja/või RIT IT-kasutajatoe poolt heaks kiidetud andmekandjaid, sh krüpteeritud mälupulki, mida väljastab ja mille üle peab arvestust sekretär. Enne mälupulga kasutamist tuleb veenduda selle turvalisuses (<https://kontrolli.tehik.ee/>) või pöörduda kontrollimiseks RIT IT-kasutajatoe poole.
- 11.3. Mobiilsete andmekandjate kasutamisel tuleb arvestada, et nende kasutamine on kõrgendatud ohu allikas, kuna neid on lihtne kaotada, varastada ja neid võidakse kasutada arvuti viirustega nakatamiseks.
- 11.4. Kui tökohustuste tõttu on vajalik kasutada andmekandjaid, mis ei ole ameti soetatud, tuleb see RIT IT-kasutajatoega kokku leppida.
- 11.5. Juurdepääsupiiranguga teavet sisaldava mobiilse andmekandja ühendamisel arvutiga või juurdepääsupiiranguga teabe kopeerimisel mobiilsele andmekandjale, tuleb võimalusel eelistada juhtmega ühendust juhtmevaba ühenduse (nt sinihammas, infrapuna) asemel.
- 11.6. Andmete salvestamine mobiilsele andmekandjale on lubatud vaid otseste teenistus- või tööülesannete täitmiseks ning selliste andmete salvestamisel mobiilsele andmekandjale tuleb andmed krüpteerida, kasutades selleks ameti sertifikaati, ID-kaardi vm RIT *Company Portal*ist alla laetavat rakendust.
- 11.7. Kui juurdepääsupiiranguga andmete hoidmine mobiilsel andmekandjal ei ole enam teenistus- või tööülesannete täitmiseks vajalik, tuleb andmed sellelt koheselt kustutada.
- 11.8. Mobiilse andmekandja andmisel teise isiku valdusesse tuleb eelnevalt veenduda, et andmekandja ei sisalda teavet, millele selle saanud isik juurdepääsu omada ei tohi.
- 11.9. Juurdepääsupiiranguga andmeid sisaldava andmekandja saatmisel postiga, kulleriga vm üleandmisel tuleb vormistada sellekohane üleandmise akt või saatekiri, mis registreeritakse dokumendihaldussüsteemis. Dokument peab sisaldama saatjat, vastuvõtjat, andmekandja liiki, identifitseerimistunnuseid, saatmise/üleandmise kuupäeva ja osapoolte allkirju.
- 11.10. Kui edasiantavad andmed asuvad üksnes andmekandjal ning andmeid ei saa taastada muudest andmeallikatest, tuleb teha andmekandjal olevatest andmetest varukoopia.
- 11.11. Juurdepääsupiiranguga andmeid sisaldava mobiilse andmekandja kadumisest või vargusest tuleb koheselt teavitada sekretäri ja infoturbe eest vastutavat isikut.

12. Mobiilsideseadmete kasutamine

- 12.1. Mobiilsideseadmega (mobiiltelefon, tahvelarvuti) on võimalik juurdepääs MS365 rakendustele, e-postile ja kalendrile. Juurdepääs on lubatud tootja poolt tagatud tarkvara uuendustega *Android*, *iOS* ja *iPadOS* seadmetele. Ameti infosüsteemidele mobiilsideseadmetega juurdepääs ei ole võimalik.
- 12.2. Mobiilsideseadmega arvutitöökohateenust saab kasutada nii ametile kuuluvate mobiilsideseadmete kui kasutajale isiklikult kuuluvate seadmetega, tehes vajalikud seadistused RIT kasutusjuhendi alusel.
- 12.3. Mobiilsideseadme kasutamisel dokumentide ja andmete salvestamiseks või transportimiseks loetakse mobiilsideseadet ühtlasi mobiilseks andmekandjaks ja sellele kehtivad samad reeglid, mis on kehtestatud mobiilsetele andmekandjatele käesoleva korra punktis 11.

- 12.4. Mobiilsideseade peab olema kaitstud automaatse ekraanilukuga, kui seadet pole enam kui ühe minuti jooksul kasutatud. Ekraanilukuks tuleb kasutada minimaalselt 6-kohalist PIN-koodi või biomeetriat. Keelatud on kasutada lihtsasti arvatavaid või järjestikuseid kombinatsioone (nt 1234, 1111, 0000 jne) ja nn näpuga lohistatavat mustri lukku, samuti parooli või PIN-koodi muutmisel viimati kasutatud kombinatsioone.
- 12.5. Mobiilsideseadme kasutamisel on keelatud:
- 12.5.1. juurdepääsupiiranguga teabe salvestamine seadmesse;
 - 12.5.2. seadmed, millelt on eemaldatud kasutuspiirangud (*jailbreaking, rooting*) või puudub ametliku tootja operatsioonisüsteem (*flashing*);
 - 12.5.3. seadet ühendada ebausaldusväärse või võõra arvuti, seadme külge, sh aku laadimiseks;
 - 12.5.4. varundada töö postkasti ja kalendri sisu mujale, kui RIT hallatavasse tööjaama;
 - 12.5.5. paigaldada rakendusi mujalt, kui usaldusväärsete tootja varamust (*Google Play, Apple App Store*);
 - 12.5.6. kasutada lõpetatud tootja toega rakendusi;
 - 12.5.7. avaldada seadme lukukoodi kolmandatele isikutele, seda dokumenteerida ega krüpteerimata kujul jäädvustada ühelegi andmekandjale;
 - 12.5.8. anda seadet kasutamiseks volitamata isikutele ja sellega võimaldada kolmandate isikute juurdepääsu ameti e-postile ja kalendrile.
- 12.6. Kasutaja on kohustatud:
- 12.6.1. veenduma, et mobiilsideseadme, *wifi*, infrapuna-, sinihamba ning NFC liidesed on välja lülitatud, kui neid ei kasutata;
 - 12.6.2. andmevahetuseks kasutama eelistatult mobiilsidoperaatori andmeside teenust, avalikke *wifi* võrke kasutama ainult äärmise vajaduse korral;
 - 12.6.3. mobiilsideseadme ühendamisel väliste seadmetega sinihamba-, infrapunaliidese või NFC kaudu kasutama turvalist ühendamist (nt turvalise paaritamiskoodiga, krüpteeritud ühendus);
 - 12.6.4. tagama, et määratud seadmenimi ei sisalda viidet ametile ega kasutajale;
 - 12.6.5. paigaldama esimesel võimalusel seadme- või operatsioonisüsteemi tootja poolt väljastatud tarkvara turvauuendused;
 - 12.6.6. enne mobiilsideseadme väljavahetamist, parandusse või garantiisse viimist teavitama RIT IT-kasutajatuge või kustutama seadmest ligipääsu tööalasele e-postkastile ja kalendrile;
 - 12.6.7. mobiilseadme tagastamisel kustutama kõik andmed ja lähtestama tehaseseaded (vt ka kiirjuhend siseveebis: IT-abi, IT-seadmete kasutusjuhendid);
 - 12.6.8. mobiilsideseadme, sh isikliku seadme, kui sellega kasutatakse töö tegemiseks vajalikke teenuseid, kaotusest koheselt teavitama haldusspetsialisti (blokeerib SIM-kaardi), RIT IT-kasutajatuge (sulgeb teenustele juurdepääsu) ja infoturbe eest vastutavat isikut.
- 12.7. Mobiilseadme vastuvõtmisel kasutajalt kontrollib haldusspetsialist, et sellel olevad andmed on kustutatud ja tehaseseaded lähtestatud.

13. Arvutitöökohateenuse juurde mittekuuluva IKT-vahendi kasutamine

- 13.1. Ameti arvutiga ja arvutivõrku ühendada on lubatud ainult RIT IT-kasutajatoe poolt heaks kiidetud IKT vahendeid. Selleks tuleb saata pöördumine RIT IT-kasutajatoele, kus on kirjas IKT vahendi täpne mark ja mudel. Heaks kiitmata IKT vahendid ei pruugi arvutitöökohateenusel toimida.
- 13.2. Isikliku printeri kasutamine ei ole lubatud.

14. Kaugtöö ehk töö väljaspool ameti kohtvõrku

- 14.1. 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*).
- 14.2. Kaugtöö on lubatud ainult ameti sülearvutist või p 11.1 vastavast mobiilsest seadmest.
- 14.3. Kaugtöö tegemise eelduseks on kiire ja stabiilse internetiühenduse olemasolu. Kasutada tohib usaldusväärseid nõuetekohase parooliga kaitstud ja ajakohastatud tarkvaraga kohtvõrku (nt. kodune *wifi*). Avalike võrkudega (nt kohvikute, hotellide jms) ühenduse loomisele tuleb eelistada mobiilse andmeside kasutamist (nt turvalise parooliga kaitstud kuumkoht).
- 14.4. Kaugtöö tegemiseks vajalikud infovarad väljastab RIT ameti aadressile ning ei taga infovarade paigaldamist ja seadistamist kasutaja kodukontoris.
- 14.5. Kaugtöö tegemisel ameti sülearvutist tuleb järgida ka käesoleva korra Lisas 1 toodud sülearvutite kasutamise nõudeid.
- 14.6. 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. Juhul, kui seadme privaatsusfiltrit ei kasutata või ekraani ei saa muul viisil kõrvaliste isikute eest varjata, on töötamine keelatud.
- 14.7. Paberkandjal ja ka teistel välistel andmekandjatel teabe kaasavõtmisel väljaspoole ameti ruume tuleb lähtuda minimaalsuse printsiibist.

15. Info- ja kommunikatsioonitehnoloogia vahendite tellimine ja tagastamine

- 15.1. Kõigile kasutajatele on standardtöökohaseadmetena ette nähtud sülearvuti ja dokk, monitor, klaviatuur, hiir ja vajalikud ühenduskaablid ning standardtarkvarana MS365, *Outlook*, dokumendihaldussüsteem ja tööks vajalikud infosüsteemid.
- 15.2. Standardtöökoha seadmete või standardtarkvara tellimiseks uuele kasutajale teeb RIT IT-kasutajatoele pöördumise ameti personalispetsialist *vastavalt Infovara juurdepääsuõiguste haldamise korrale*.
- 15.3. Infovara (sh ka väikevahendid, tarkvarad, litsentsid jm) asendamiseks või täiendamiseks esitab kasutaja esmalt kirjaliku taotluse haldusspetsialistile, kes kaasab kooskõlastusringi vahetu juhi ning sõltuvalt maksumusest ka finantsjuhi ja/või peadirektori. Haldusspetsialistilt saadud heakskiidu (maksumus kuni 50eur) ja vajadusel finantsjuhi (50-500 eur) ja/või peadirektori (üle 500 eur) kinnituse alusel võib kasutaja teha tellimuse RIT iseteeninduses või saata pöördumise RIT IT-kasutajatoele.
- 15.4. Infovarasid ei pea eraldi taotlema, kui olemasolev infovara ei ole töökorras, sellisel juhul teeb kasutaja ise pöördumise RIT IT-kasutajatoele kirjeldades mittetöötamise põhjuseid ja RIT IT-kasutajatugi tellib vara hoolduse, remondi või väljavahetamise.
- 15.5. Infovara vahetatakse välja infovara rendiperioodi lõppedes. Sellisest vahetusest teavitab RIT IT-kasutajatugi ette vähemalt kümme tööpäeva ning lepib kasutajaga kokku vahetamise aja.
- 15.6. Infovara kasutamise kohta sõlmitakse kasutajaga kokkulepe Riigitöötaja Iseteenindusportaalil. Infovara vahetuse korral peab kasutaja veenduma infovara ja RTIPi üleandmise akti andmete vastavuses.
- 15.7. Kui infovara kasutaja lahkub ametist või vahendi kasutamine pole enam töö- või teenistusülesannete täitmiseks vajalik, teavitab haldusspetsialist RIT IT-kasutajatuge vabaks jäänud IT vahendist ning kasutaja peab tagastama kõik tema kasutuses olnud ameti tark- ja riistvaralised süsteemid.

- 15.8. Defektsed ja kasutuskõlbmatud andmekandjad tuleb anda hävitamiseks arendus- ja haldusosakonnale.

16. Infovara väärkasutuse tagajärjed

- 16.1. Kahtluse tekkimisel infovara kasutamise reeglite rikkumise või väärkasutuse osas on RIT või TEHIK IT-kasutajatoel õigus peatada või piirata kasutusõigust kuni asjaolude selgitamiseni.
- 16.2. Infovara kasutamist reguleerivate õigusaktide mittetäitmine võib tuua kaasa kriminaal-, väärteo- või distsiplinaarkaristuse.
- 16.3. Infovara süüalise rikkumise korral on vara soetanud ametil õigus nõuda kahju hüvitamist. Kahju tekkimisel hinnatakse infovara kahjustamise ajaolusid koostöös RIT või TEHIK IT-kasutajatoe ja ameti haldusspetsialistiga.
- 16.4. Kui infovara 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.
- 16.5. 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.

Lisa 1 - Sülearvutite kasutamise kord

1. Sülearvuti mobiilsus ja võimalus sülearvutit kasutada väljaspool ameti turvatud arvutivõrku teeb sülearvutist kõrgendatud ohu allika ning paneb kasutajale lisavastutuse.
2. Kasutajal on keelatud sülearvutit edasi anda kasutamiseks kolmandale isikule. Võõrastes ruumides viibides tuleb võtta sülearvuti endaga kaasa ka siis, kui ruumist lahkutakse vaid korraks. Kui seda teha ei saa, tuleb sülearvuti sulgeda ja lukustada.
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 kahjustumist või hävinemist;
 - 3.5. reisimisel kandma sülearvutit käsipagasis.
4. Sülearvuti vargusest, kaotamisest või hävimisest on kasutaja kohustatud viivitamatult teavitama haldusspetsialisti, infoturbe eest vastutavat isikut ja RIT 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 ameti sisevõrku (eriti avalikes *wifi* võrkudes) võidakse krüpteerimata ühendusi pealt kuulata;
 - 5.2. sisestama paroolid või PIN koodi nii, et kõrvalised isikud ei näeks, milline parool/PIN kood sisestati;
 - 5.3. sülearvuti juurest lahkumisel sulgema sülearvuti ja eemaldama kiipkaardi;
 - 5.4. juhtmeta ühenduste (*wifi*, infrapunaliides, sinihammas) kasutamisel vältima nende tarbetut aktiveerimist ning konfidentsiaalsete andmete töötlemisel eelistama kaabelühendust;
 - 5.5. lülitama välja kõik sülearvuti juhtmeta (*wifi*, infrapunaliides, sinihammas) ühendused, kui sülearvuti on ameti arvutivõrgus võrgukaabliga;
 - 5.6. 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 RIT IT-kasutajatuge, kes korraldab arvuti ülevaatamise;
 - 5.7. kahtluse või teadmise korral, et sülearvutis on pahavara, mitte ühendama sülearvutit ameti ega avalikku arvutivõrku, vaid teatama juhtunust RIT 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. hoidma andmeid *Onedrive'is*, *SharePointis* või infosüsteemides;
 - 6.2. ühendades sülearvuti ameti arvutivõrku, tegema koheselt kõvakettal olevatest andmetest varukoopia p 6.1 toodud asukohtadesse;
 - 6.3. sülearvuti pikemal mobiilsel kasutamisel kaasas kandma laadijat, aku kasutusea pikendamiseks laadima sülearvutit tootja heakskiidetud laadijaga ja kasutusjuhendis näidatud viisil. Toiteallika (aku) tühjenemisega kaasneva võimaliku andmekao vältimiseks tuleb toite hoiatussignaali või märguande korral koheselt salvestada pooleliolev töö.
7. Kasutaja peab paigaldama võimalikult koheselt saadaolevad tarkvarauuendused.
8. Põhjendatud juhtudel väljastatakse sülearvuti ameti struktuuriüksusele ühiskasutuseks, sellisel juhul kehtivad järgmised reeglid:

- 8.1. ühiskasutuses oleva sülearvuti puhul määratakse väljastamise hetkel sülearvuti kasutamise eest üks vastutav isik (edaspidi *vastutaja*);
- 8.2. vastutaja on kohustatud pidama vabas vormis kirjalikku arvestust kogu oma vastutusaja jooksul, kellele on sülearvuti millisel ajahetkel kasutusse antud ning millises seisukorras see on tagastatud;
- 8.3. kui vastutaja annab sülearvuti teisele kasutajale, siirdub vastutus sülearvuti eest vastutajalt kasutajale ja tagastamisel jälle kasutajalt vastutajale;
- 8.4. vastutaja peab veenduma, et kõik kasutajad, kellele vastutaja sülearvuti kasutada annab, on tutvunud sülearvutite kasutamise nõuetega;
- 8.5. iga kasutaja kasutab sülearvutit oma personaalse kasutajakontoga, mis peab olema enne sülearvuti kasutusse andmist nõuetekohaselt seadistatud IT-spetsialisti poolt;
- 8.6. juhul, kui sülearvuti vastutaja ei suuda tõestada, kelle kasutuses sülearvuti süüalise kahju tekkimise hetkel oli, nõutakse kahjuhüvitist sülearvuti eest vastutajalt.