KINNITATUD
Ravimiameti peadirektori
veebruari 2025
käskkirjaga nr 21

INFOVARA KASUTAMISE KORD

SISUKORD

1. Üldsätted

1.1. Käesolev kord sätestab Ravimiameti (edaspidi amet) infovara kasutaja õigused ja kohustused, et kaitsta ja hallata asutuse infotehnoloogilisi vahendeid, infosüsteeme ja nende abil töödeldavaid andmeid.
1.2. Käesolev kord kehtib kõikidele ameti infovarade 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. IT varade kord (TEHIK),
2.4. Hangitavate IT väikevarade loetelu ja arveldamise kord (TEHIK).

3. Mõisted

3.1. TEHIK – Tervise- ja Heaolu Infosüsteemide Keskus, ametile IT-teenuste pakkuja;
3.2. 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;

3.3. Infovara - informatsioon ja andmed ning nende töötlemiseks vajalikud infotehnoloogilised rakendused ja tehnilised vahendid;
3.4. IT-kasutajatugi – TEHIKu IT-teenuste kasutajatugi ja kõnekeskus;
3.5. IT-spetsialist – TEHIKu või tema koostööpartneri (nt Telia) IT-alaste teadmistega IT-teenindaja;
3.6. IT-teenus – TEHIKu poolt ametile 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) ameti teenuste kasutamist;
3.7. IKT vahend – info- ja kommunikatsioonitehnoloogia vahend ehk andmete töötlemise, salvestamise ja edastamise tehnilised vahendid, näiteks sülearvuti, monitor, printer jne;
3.8. Mobiilsideseade – teatud liiki IKT vahend, näiteks tahvelarvuti, mobiiltelefon jms;
3.9. 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);
3.10. 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;
3.11. Juurdepääsupiiranguga teave – teave, mis seaduse, lepingu või mõnel muul alusel on kuulutatud mitteavalikuks;
3.12. Intsident – ootamatu rike (mis ei ole normaalse/standardse teenuse osa), mis põhjustab või võib põhjustada IT-teenuse planeerimata katkestuse või teenuse kvaliteedi olulise languse;
3.13. 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 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 infovara töö ja teenuste ning infoturbe paremaks korraldamiseks.

5. Kasutaja kohustused

5.1. Kasutaja on kohustatud järgima ametis kehtivaid kordasid ja juhendeid ning infovara kasutamiseks kehtestatud alalisi ja ajutisi piiranguid.
5.2. Kasutaja on kohustatud kasutama TEHIKu pakutavaid IT-teenuseid ja infovara 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 ametile oma tegevusega või tegevusetusega kahju ega ohtu arvutivõrgu turvalisusele.
5.5. Kõik infovara 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 ja infoturbe eest vastutavat isikut.
5.7. Keelatud on omavoliline (ilma TEHIKu loata) IKT vahendite, sh tarkvara, lisamine (va mobiilsed andmekandjad, mille kohta kehtib käesoleva korra punkt 10), ümberpaigutamine, häälestamine, eemaldamine ja ameti ruumidest välja viimine (v.a mobiilsed andmekandjad, mille kohta kehtib käesoleva korra punkt 10, 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 ametile mittekuuluvat riistvara, tuleb lähtuda käesoleva korra punktist 13.
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 arvutitöökoha paigutama nii, et kõrvalisel isikul ei oleks võimalik näha ekraanil kuvatavaid andmeid. Arvutitöökohaga liikudes ja avalikus kohas töötades tuleb kasutada kogu ekraani katvat filtrit.
5.10. Keelatud on IKT vahendi kasutamine teise isiku poolt või IKT vahendi jätmine järelevalveta kohtadesse, kus on oht nende sattumiseks kõrvaliste isikute valdusesse.
5.11. 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 vastuvõetule, arvestades vara normaalset kulumist. Vara varguse, kahjustumise, hävimise või kaotamise korral tuleb esimesel võimalusel teavitada IT-kasutajatuge ja haldusspetsialisti.
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. Arvutil on ka parooliga kaitstud ekraanilukk, mis rakendub automaatselt, kui seadet ei ole 10 minuti jooksul kasutatud.
5.13. Töö lõpetamisel on kasutaja kohustatud sulgema kõik kasutusel olnud infosüsteemid ja rakendused, arvuti lukustama ja võtma kasutusele kõik meetmed välistamaks dokumentide ning mobiilsete andmekandjate sattumist võõrastesse kätesse.

6. Paroolinõuded

6.1. Arvutivõrgu ja arvutivõrgus asuvate infosüsteemide kasutamiseks saab iga kasutaja personaalse kasutajatunnuse, üldjuhul kujul eesnimi.perenimi, ja parooli. Arvutivõrgus asuvatele infosüsteemidele 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 kasutamisjuhend 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 ühesugususestest sümbolitest ega klaviatuurijärjestuses tähtedest või numbritest;
  6.9.3. 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;
  6.9.4. 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 IT-kasutajatoe poole.
6.12. Parooli ununemise või mittetöötamise korral teavitab kasutaja sellest koheselt IT-kasutajatuge, kes loob kasutajale uue ühekordse parooli. Parool edastatakse kasutajale viisil, mis võimaldab isikutuvastust, st IT-kasutajatugi peab veenduma, et kasutaja on tõepoolest see, kes ta väidab end olevat.
6.13. 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 ameti ja erinevate struktuuriüksuste ja teemadega seotud võrgukettaid.
7.2. Ameti, struktuuriüksuste ja erinevate teemadega seotud võrguketastele antakse juurdepääsuõigused vastavalt *Infovara juurdepääsuõiguste haldamise korrale*.
7.3. Iga kasutaja jaoks ette nähtud personaalsel võrgukettal olevad dokumendid on kättesaadavad vaid kasutajale endale. Personaalsele võrgukettale viitab ka kasutaja töölaual olev kodukataloog (Minu dokumendid/My Documents).
7.4. Arvutivõrgu ressursside säästliku kasutamise eesmärgil on iga kasutaja personaalsel võrgukettal limiit (vastavalt kehtivale amet-TEHIK teenuslepingule). 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 kõvakettale. Võrguketastel olevatest failidest tehakse regulaarselt varukoopiaid.
7.6. Failide salvestamisel võrguketastele tuleb jälgida, et failid oleksid kättesaadavad vaid isikutele, kes tohivad neile juurde pääseda.
7.7. Juurdepääsupiiranguga informatsiooni skaneerimisel, printimisel või paljundamisel tuleb skaneeritud, väljaprinditud 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.
7.8. Kasutajatel on keelatud hoida failiserveris faile, mille sisu on ebaseaduslik, ebaeetiline või kahjustab riigi või ameti 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 teenistus- või tööülesannete täitmiseks.
8.3. Arvutivõrgu ressursside säästliku kasutamise eesmärgil on igal elektronposti kasutajakontol limiit (vastavalt amet-TEHIK kehtivale teenuslepingule), 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 välistele elektronposti 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“, „hot.ee“ jne).
8.7. Andmed, mille avalikuks tulek võib põhjustada ametile olulist kahju, tuleb edastada krüpteeritult, kasutades selleks ameti sertifikaati, ID-kaardi, VeraCrypt vm Software Center-ist allalaaditavat rakendust.
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.
8.10. Kasutaja Outlooki põhipostkastist liigutatakse 365 päeva vanused e-kirjad arhiivpostkasti. Jagatud postkastide e-kirjad säilitatakse Outlooki põhipostkastis 3 aastat, seejärel liigutatakse need arhiivpostkasti. Arhiivpostkastis säilitatakse kirju kokku 7 aastat, mille möödumisel kustuvad kirjad automaatselt.
8.11. Ametiaja või töösuhte lõppemisel säilitatakse kasutaja isiklikku Outlooki postkasti 365 päeva pärast kasutaja viimast sisselogimist, misjärel kustutatakse nii peamine (põhipostkast) kui ka arhiivpostkast.

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

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 IT-kasutajatoe loata alla mistahes programme, programmiuuendusi, mänge jms. Kasutajal on keelatud luua ameti nimel kontosid või lisada ameti kontot veebiteenusele.
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.

10. Mobiilsed andmekandjad

10.1. Mobiilsete andmekandjate kasutamine on üldjuhul kasutajale piiratud ja lubatakse tööülesannete täitmise vajadusel eriõigusega vastavalt *Infovara juurdepääsuõiguste haldamise korrale.*
10.2. Ametis tohib kasutada vaid ameti poolt hangitud 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 IT-kasutajatoe poole.
10.3. 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.
10.4. Kui töökohustuste tõttu on vajalik kasutada andmekandjaid, mis ei ole ameti soetatud, tuleb see IT-kasutajatoega kokku leppida. Vajadusel tõstetakse sellise arvuti turvalisust või lepitakse kokku milliseid andmekandjaid usaldatakse.
10.5. Juurdepääsupiiranguga teavet sisaldava mobiilse andmekandja ühendamisel arvutiga või juurdepääsupiiranguga teabe kopeerimisel mobiilsele andmekandjale, tuleb võimalusel eelistada juhtmega ühendust juhtmevaba ühenduse (nt sinihammas, infrapuna) asemel.
10.6. 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 Software Center-ist alla laetavat rakendust.
10.7. Kui juurdepääsupiiranguga andmete hoidmine mobiilsel andmekandjal ei ole enam teenistus- või tööülesannete täitmiseks vajalik, tuleb andmed andmekandjalt koheselt kustutada ja võimalusel kasutada selleks programmi Eraser (Software Center-ist alla laetav), kustutades andmed 7 kordse ülekirjutamisega.
10.8. Mobiilse andmekandja andmisel teise isiku valdusesse tuleb eelnevalt veenduda, et andmekandja ei sisalda teavet, millele andmekandja saanud isik juurdepääsu omada ei tohi.
10.9. 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.

10.10. Kui edasiantavad andmed asuvad üksnes andmekandjal ning andmeid ei saa taastada muudest andmeallikatest, tuleb teha andmekandjal olevatest andmetest varukoopia.

10.11. Juurdepääsupiiranguga andmeid sisaldava mobiilse andmekandja kadumisest või vargusest tuleb koheselt teavitada sekretäri ja infoturbe eest vastutavat isikut.

11. Kaugtöö ehk töö väljaspool ameti arvutivõrku

11.1. 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*).

11.2. Kaugtöö on võimalik ainult ameti sülearvutist, et tagada ja kontrollida selle turvalisust.

11.3. Kaugtöö tegemise eelduseks on kiire ja stabiilse internetiühenduse olemasolu. Kasutada tuleb usaldusväärseid nõuetekohase parooliga kaitstud ja ajakohastatud tarkvaraga kohtvõrku (nt. kodune Wi-Fi). Avalike võrkudega (nt kohvikute, hotellide jms) ühenduse loomisele tuleb eelistada mobiilset andmeside kasutamist (nt turvalise parooliga kaitstud kuumkoht).

11.4. Kaugtöö tegemiseks kasutatakse VPN ühendust.

11.5. Kaugtöö tegemiseks vajalikud infovarad väljastab TEHIK ameti aadressile ning ei taga infovarade paigaldamist ja seadistamist kasutaja kodukontoris.

11.6. Kaugtöö tegemisel ameti sülearvutist tuleb järgida ka käesoleva korra Lisas 1 toodud sülearvutite kasutamise nõudeid.

11.7. 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. Juhul, kui seadme ekraanifiltrit ei kasutata või ekraani ei saa muul viisil kõrvaliste isikute eest varjata, on töötamine keelatud.

11.8. Paberkandjal ja ka teistel välistel andmekandjatel teabe kaasavõtmisel väljaspoole ameti ruume tuleb lähtuda minimaalsuse printsiibist.

12. Mobiilsideseadmete kasutamine

12.1. Mobiilsideseadmetega (tahvelarvuti, mobiiltelefon, nutikell) arvutivõrgu kasutaja peab arvestama, et seadet kasutatakse väljaspool ameti 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 ameti andmetele antakse põhjendatud tööalase vajaduse korral ning ajaks, millal andmete kasutamine on tööalaselt vajalik.

12.2. Mobiilsideseadmega on võimalik juurdepääs ametielektronpostile ja kalendrile. Juurdepääs on lubatud tootja poolt tagatud tarkvara uuendustega Android ja iOS seadmetele. Ameti võrguketastele ja infosüsteemidele mobiilsideseadmetega juurdepääs ei ole võimalik.

12.3. Mobiilsideseadmega arvutivõrgu kasutamiseks saab kasutada nii ametile kuuluvaid mobiilsideseadmeid kui kasutajale isiklikult kuuluvaid seadmeid. TEHIK ei garanteeri ameti arvutivõrgu juurdepääsu ametile mittekuuluva mobiilsideseadmega. Samuti ei vastuta TEHIK sellise seadme riknemise või seadmes olevate andmete kaotsi mineku eest.

12.4. 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 10.
12.5. 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 tegema IT-kasutajatoele vastavasisulise pöördumise, kus on ära toodud mobiilsideseadme tootja ja mudel ning põhjendus elektronposti ja kalendri sünkroniseerimise vajaduse kohta.
12.6. 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 peab seadme kasutamisel järgima kõiki seatud turvanõudeid (vt täpsemalt *EASi kasutamise juhendist*).
12.7. 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 mustrilukku, samuti parooli või PIN-koodi muutmisel viimati kasutatud kombinatsioone.
12.8. Mobiilsideseadme kasutamisel on keelatud:
12.8.1. Exchange ActiveSync'i krüpteerimata HTTP protokoll, kasutada tuleb turvalise šifrikomplektiga HTTPS protokolli;
12.8.2. juurdepääsupiiranguga teabe salvestamine seadmesse;
12.8.3. seadmed, millelt on eemaldatud kasutuspiirangud (jailbreaking, rooting) või puudub ametliku tootja operatsioonisüsteem (flashing);
12.8.4. seadet ühendada ebausaldusväärse või võõra arvuti, seadme külge, sh aku laadimiseks;
12.8.5. varundada töö postkasti ja kalendri sisu mujale, kui TEHIKu hallatavasse tööjaama;
12.8.6. paigaldada rakendusi mujalt, kui usaldusväärsete tootja varamust (Google Play, Apple App Store);
12.8.7. kasutada lõpetatud tootja toega rakendusi;
12.8.8. avaldada seadme lukukoodi kolmandatele isikutele, seda dokumenteerida ega krüpteerimata kujul jäädvustada ühelegi andmekandjale;
12.8.9. anda seadet kasutamiseks volitamata isikutele ja sellega võimaldada kolmandate isikute juurdepääsu ameti elektronpostile ja kalendrile.
12.9. Kasutaja on kohustatud:
12.9.1. veenduma, et mobiilsideseadme, Wi-Fi, infrapuna-, sinihamba ning NFC liidesed on välja lülitatud, kui neid ei kasutata;
12.9.2. andmevahetuseks kasutama eelistatult mobiilsideoperaatori andmeside teenust, avalikke Wi-Fi võrke kasutama ainult äärmise vajaduse korral;
12.9.3. mobiilsideseadme ühendamisel väliste seadmetega sinihamba-, infrapunaliidese või NFC kaudu kasutama turvalist ühendamist (nt turvalise paaritamiskoodiga, krüpteeritud ühendus);
12.9.4. tagama, et määratud seadmenimi ei sisalda viidet ametile ega kasutajale;
12.9.5. paigaldama esimesel võimalusel seadme- või operatsioonisüsteemi tootja poolt väljastatud tarkvara turvauuendused;
12.9.6. enne mobiilsideseadme väljavahetamist, parandusse või garantiisse viimist teavitama IT-abi ja kustutama seadmest ligipääsu tööalasele e-postkastile ja kalendrile;

12.9.7. mobiilseadme tagastamisel kustutama kõik andmed ja lähtestama tehaseseaded (vt ka kiirjuhend siseveebis: IT-abi, IT-seadmete kasutusjuhendid);
12.9.8. mobiilsideseadme, sh isikliku seadme, kui sellega kasutatakse töö tegemiseks vajalikke teenuseid, kaotusest koheselt teavitama haldusspetsialisti (blokeerib SIM-kaardi), IT-abi (sulgeb teenustele juurdepääsu) ja infoturbe eest vastutavat isikut.
12.10. Mobiilseadme vastuvõtmisel kasutajalt kontrollib haldusspetsialist, et sellel olevad andmed on kustutatud ja tehaseseaded lähtestatud.

13. Ametile mittekuuluva IKT-vahendi kasutamine ameti arvutivõrgus

13.1. Üldjuhul on lubatud ameti arvutiga ja arvutivõrku ühendada ainult ametile kuuluvaid IKT vahendeid. Isikliku printeri kasutamine ei ole lubatud.
13.2. Kui otseste tööülesannete täitmiseks on vajalik, et ameti arvutivõrku või arvuti külge ühendataks ametile 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.
13.3. IT-kasutajatugi võib pakkuda välja alternatiivi ametile mittekuuluva IKT vahendi kasutamiseks ameti arvutivõrgus. Kui alternatiivi ei leita ja IKT vahend ei kujuta TEHIKu arvates ohtu ameti arvutivõrgu ja süsteemide turvalisusele või käideldavusele, lubatakse IKT vahendi kasutamine vastavalt TEHIKu nõuetele.
13.4. Kõigist ametile mittekuuluvatest IKT vahendite kasutamise lõpetamisest ameti võrgus või arvutis peab kasutaja koheselt teavitama IT-kasutajatuge.

14. Info- ja kommunikatsioonitehnoloogia vahendite tellimine ja tagastamine

14.1. Kõigile kasutajatele on standardtöökohaseadmetena ette nähtud sülearvuti ja dokk, monitor, klaviatuur, juhtmega hiir ja vajalikud ühenduskaablid ning standardtarkvarana MS Office, Outlook, dokumendihaldussüsteem ja tööks vajalikud infosüsteemid.
14.2. Standardtöökoha seadmete või standardtarkvara tellimiseks uuele kasutajale teeb IT-kasutajatoele pöördumise ameti personalispetsialist kümme tööpäeva enne vara kasutama hakkamist. Pöördumises tuleb tuua välja vara kasutaja ees- ja perekonnanimi, isikukood, töökoha asukoht, töö alustamise kuupäev, vajalike infovarade kirjeldus ja selgitus vara vajaduse kohta, kui tegemist ei ole standardtöökoha seadmega (vt lisaks *TEHIKu IT varade kord*).
14.3. Infovara asendamiseks teistsuguse seadme vastu või täiendamiseks esitab kasutaja osakonna juht või arendus- ja haldusosakonna 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.
14.4. Infovarasid ei pea eraldi taotlema, kui olemasolev infovara ei ole töökorras, sellisel juhul teeb kasutaja ise pöördumise IT-kasutajatoele kirjeldades mittetöötamise põhjuseid ja IT-kasutajatugi tellib vara väljavahetamise.
14.5. TEHIK võib infovarasid välja vahetada infovara rendiperioodi lõppedes ja/või vastavalt vajadusele (amortiseerunud, vananenud). Sellisest vahetusest teavitab IT varahaldur ette vähemalt kümme tööpäeva ning IT-spetsialist lepib kasutajaga kokku infovarade vahetamise aja.

14.6. Infovara kasutamise kohta sõlmitakse kasutajaga kokkulepe Riigitöötaja Iseteenindusportaalis.
14.7. Mittestandardseid väikevarasid (nt kõlarid, kõrvaklapid, USB kettaseadmed, mälupulgad, toonerid, juhtmeta hiired jne) hangib arendus- ja haldusosakond (vt ka *TEHIKu hangitavate IT väikevarade loetelu ja arveldamise korda*). Selliste varade saamiseks tuleb kasutajal pöörduda arendus- ja haldusosakonna poole.
14.8. Kui infovara kasutaja lahkub ametist või vahendi kasutamine pole enam töö- või teenistusülesannete täitmiseks vajalik, teavitab arendus- ja haldusosakond IT-kasutajatuge vabaks jäänud IT vahendist ning kasutaja peab tagastama kõik tema kasutuses olnud ameti tark- ja riistvaralised süsteemid. Mittestandardsed väikevarad tuleb tagastada arendus- ja haldusosakonda.
14.9. Defektsed ja kasutuskõlbmatud andmekandjad tuleb anda hävitamiseks arendus- ja haldusosakonnale.

15. IT-kasutajatugi

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

16. Infovara väärkasutuse tagajärjed

16.1. Kahtluse tekkimisel arvutivõrgu kasutamise reeglite rikkumise või infovara 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.
16.2. Infovara kasutamist reguleerivate õigusaktide mittetäitmine võib tuua kaasa kriminaal-, väärteo- või distsiplinaarkaristuse.
16.3. Infovara süülise rikkumise korral on vara soetanud ametil õigus nõuda kahju hüvitamist. Kahju tekkimisel esitab kasutaja TEHIKule seletuskirja kahju tekkimise asjaolude kohta, kes hindab infovara kahjustamise ajaolusid.
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.

16.6. Vääramatust jõust tingitud infovara rikkumisest või hävimisest tulenevad taastamiskulud katab TEHIK.

Lisa 1 - Ravimiameti 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 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 kiipkaardi 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 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 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 ameti arvutivõrgus hoidma andmeid selleks määratud võrgukettal;

6.2. ühendades sülearvuti ameti arvutivõrku, tegema koheselt kõvakettal olevatest andmetest varukoopia selleks määratud võrgukettale, kasutaja kodukataloog varundatakse arvutivõrku automaatselt;
6.3. töötades pikemaajaliselt ameti arvutivõrgu ühenduseta, tegema olulistest andmetest krüpteeritud koopia mobiilsele andmekandjale. Varukoopia salvestamisel mobiilsele andmekandjale peab viimast adekvaatselt kaitsma varguse, hävimise ja kaotamise eest;
6.4. 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 sülearvutiga käima ameti (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 kasutaja tooma sülearvuti IT-spetsialisti kätte korraliseks hoolduseks. Enne sülearvuti hooldusesse andmist peab kasutaja veenduma, et kõikidest vajalikest andmetest, mis on salvestatud sülearvuti kõvakettale, on tagavarakoopiad andmete hoidmiseks ettenähtud võrgukettal.
9. Põhjendatud juhtudel väljastatakse sülearvuti ameti 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 vastutusaja 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 ameti eelarvelistest vahenditest, ei anta seda IT-kasutajatoe poolt uude kasutusse teise haldusala kasutajale, v.a juhul kui selleks avaldab soovi sülearvuti soetanud ameti juht või tema poolt määratud isik.