

## **Sisevõrgu kasutamise kord**

### **1. Üldsätted**

- 1.1. Kord sätestab RIKi poolt hallatava sisevõrgu (edaspidi sisevõrk) kasutajate õigused ja kohustused, et kaitsta ning majandada otstarbekalt ministeeriumi riist- ja tarkvara ning viimaste abil töödeldavad andmeid.
- 1.2. Kord on täitmiseks kõikidele sisevõrgu ressurside kasutajatele ning kõikidele ministeeriumi seadmete ja tööjaamade kasutajatele (arvuti, sülearvuti, terminal jne).

### **2. Kasutaja õigused**

- 2.1. Kasutajaõigused saanud isikul on õigus omada juurdepääsu IT-teenusele teenustaseme leppes määratud tööajal.
- 2.2. Kasutajal on õigus saada IT-abist mõistliku aja jooksul eelnevat informatsiooni planeeritud muudatustest ja sündmustest RIKi hallatavate IT-teenuste töös, mis oluliselt mõjutavad nende kasutamist.
- 2.3. Kasutajal on õigus pöörduda infotehnoloogia alase abi saamiseks RIKi IT-abi poole.

### **3. Kasutaja üldised kohustused**

- 3.1. Kasutajal on kohustus töödelda (nt vaadata, muuta, väljastada, salvestada) AK-ks määratud informatsiooni ainult oma otseste töö- või ametiülesannete täitmiseks. Seda teavet ei ole lubatud edastada teistele isikutele juurdepääsupiirangu kehtestanud asutuse loata.
- 3.2. Kasutajal peavad olema oma teenistus- või tööülesannete täitmiseks vajalikud arvutikasutamise algteadmised. Vajadusel korraldab arvuti algteadmiste-alase koolituse kasutaja struktuuriüksus.
- 3.3. Kasutaja on kohustatud kahe nädala jooksul tööle või teenistusse asumisest arvates, ja edaspidi iga kahe aasta järel, läbima veebipõhise infoturbe koolituse ja sooritama eksami. Juhul, kui kasutaja seda kohustust ei täida, on infoturbejuhil õigus piirata kasutaja Interneti ja väliste digitaalsete andmekandjate kasutamise õigust ulatuses, mis ei takista otseste teenistustest või tööülesannete täitmist. Piirangu kohaldamise kavatsusest informeerib infoturbejuht kasutajat ja tema otsest juhti vähemalt kaks nädalat enne piirangute kehtestamist. Piirangud kasutaja Interneti kasutamisele eemaldatakse pärast kohustuse täitmist.
- 3.4. Kasutaja on kohustatud kasutama võrguressursse optimaalselt ning mitte koormama sisevõrku mittetööalaste failide ja tegevustega, regulaarselt korrastama endaga seotud elektronposti ja failiserveris asuvaid andmeid, kustutades ebaolulise sisuga kirjad ja failid.

### **4. IT-abi**

- 4.1. Kasutaja on kohustatud esimesel võimalusel teavitama IT-abi kõikidest ja infoturbeintsidentidest ja IT-teenuste kasutamist takistavatest või IT-teenuse kasutamist takistada võivatest juhtumitest, samuti sellesisulistest kahtlustest.
- 4.2. IT-abisse saab pöörduda:
  - 4.2.1. IT-abi lingi (iseteenindusportaali) kaudu;
  - 4.2.2. kasutades elektronposti aadressi itabi@just.ee või itabi@rik.ee;
  - 4.2.3. helistades IT-abi telefoninumbril 663 6464.
- 4.3. IT-abisse saabunud pöördumised registreeritakse, neile määratakse prioriteet ja suunatakse kindlaksmääratud lahendajatele.

## **5. IT riist- ja tarkvara tellimine või tagastamine**

- 5.1. Kui tööülesande täitmiseks on vaja uut tarkvara võib kasutaja selle paigaldada iseseisvalt IT-abi lehel olevalt tarkvara lisamise lingilt.
- 5.2. IT-riistvara tellimiseks tuleb IT-teenuste juhtimise tarkvara (iseteenindusportaal) kaudu teha riistvarataotlus.
- 5.3. Tarkvarade lisamise veebilehel mitteoleva standardtarkvara (valmistarkvara, mida ei pea spetsiaalselt arendama või kohandama) tellimiseks tuleb teha vastavasisuline pöördumine IT-abisse.
- 5.4. Taotlus vaadatakse RIKi poolt läbi viie tööpäeva jooksul ning kasutajale antakse tagasiside vara kasutamisse andmise tähtaegade, kasutusse mitteandmise põhjuste ja/või võimalike alternatiivide osas. Taotluse rahuldamisel lähtutakse vajaduse põhjendatusest ja eelarveliste ressursside olemasolust vastava taotleja asutuse poolt RIKi eraldatud eelarves. Ostud kooskõlastatakse taotleja asutuse selleks määratud esindajaga. Oste väärtusega kuni 100 eurot ei pea kooskõlastama.
- 5.5. Taotlus tuleb esitada ka juhul, kui riistvara/tarkvara soetatakse taotleja poolt finantseeritavast eelarvest. Sellisel juhul tuleb taotlusele teha vastav märge koos summaga, mis on antud ostu jaoks planeeritud ja millisest eelarvest raha kasutatakse. 14 tööpäeva jooksul lepib RIK riist- ja tarkvara ühtse ning ressursi säästlikuma haldamise tagamiseks tellijaga kokku nõuded, millele ostetav riistvara/tarkvara peab vastama ja kuidas hankeprotseduur läbi viia.
- 5.6. Kui vara kasutaja lahkub ametist või vahendi kasutamine pole enam teenistus- või tööülesannete täitmiseks vajalik võib RIK kokku leppida vabaks jäänud vara kasutamises mõnes teises struktuuriüksuses.
- 5.7. Vara tagastamise kohta teeb kasutaja struktuuriüksuse juht, personali teenistuja või asutuse juhi poolt selleks volitatud isik IT-abisse vastavasisulise pöördumise, mille järgselt lepitakse kokku detailsed vara tagastamise tingimused.

## **6. Juurdepääs kasutaja sisevõrgu kasutamisega seonduvatele andmetele**

- 6.1. RIKi poolt pakutavate IT-teenuste kasutamist logitakse (seal hulgas sisse- ja väljalogimine, andmete vaatamine, kustutamine, lisamine, muutmine, elektronposti saatmine ja vastuvõtmine, Interneti kasutamine, tööjaama/sisevõrku sisse- ja väljalogimine, tööjaama tarkvara installeerimine, arvuti viiruste tuvastamine). IT-teenuse omanikul on oma IT-teenuse kasutajakontode kontrollimise eesmärgil kasutaja nõusolekuta juurdepääsuõigus kasutaja IT-teenuste kasutamisega seonduvatele andmetele (v.a punktis 6.2 toodud andmed).
- 6.2. Kasutaja sisevõrgu kasutamisega seotud andmeid (sealhulgas logisid, personaalsel võrgukettal ja kasutajale RIKi poolt eraldatud tööjaama kõvakettal, nimelise elektronposti kasutajakontol olevaid andmeid, ning kasutaja Interneti kasutamisega seotud andmeid) tohib väljastada või neile juurdepääsu võimaldada üksnes kirjalikku taasesitamist võimaldava avalduse alusel IT-abisse alljärgnevatel tingimustel, mahus ja korras:
  - 6.2.1. kasutajale tema enda kohta;
  - 6.2.2. kolmandale isikule, kui kasutaja on sellega kirjalikus või kirjalikku taasesitamist võimaldavas vormis igakordselt nõustunud;
  - 6.2.3. seadusega ettenähtud tingimustel ja korras kriminaal- ja/või väärteomenetluses uurimist teostava asutuse või tsiviilkohtumenetluses kohtu kirjaliku või kirjalikku taasesitamist võimaldavas vormis järelepärimise alusel;
  - 6.2.4. vastava valdkonna asekantsleri või kantsleri kooskõlastusel kasutaja suhtes algatatud distsiplinaarmenetluses või töölepingu alusel tegutseva kasutaja poolt lepingu rikkumise korral ning juhul kui kasutaja sisevõrgu kasutamisega seotud andmed on rikkumise asjaolude väljaselgitamiseks hädavajalikud;

- 6.2.5.vastava valdkonna asekanstleri või kanstleri kooskõlastusel kui töö- või teenistussuhtest lahkuv kasutaja keeldub oluliste tööalaste dokumentide või e-kirjade üleandmisest või kui üleandmine pole võimalik ning nendega tutvumine on asutuse ülesannete täitmiseks vajalik;
- 6.2.6.infoturbejuhil või asutuse juhi poolt infoturbeintsidendi lahendamiseks määratud isikul infoturbeintsidendi lahendamiseks vajalikus ulatuses.
- 6.3. Punktides 6.2.4 ja 6.2.5. sätestatud alusel andmete väljastamine kooskõlastatakse infoturbe juhiga. Võimalusel ei väljastata ega võimaldata juurdepääsu tööga mitteseotud kirjavahetusele, dokumentidele ning kasutaja Interneti kasutamise seotud andmetele. Vajadusel konsulteerib infoturbejuht väljastatava teabe mahu osas vastava ministeeriumi isikuandmete kaitse eest vastutava isikuga.
- 6.4. Punktides 6.2.4, 6.2.5 ja 6.2.6 sätestatud andmete edastamise või neile juurdepääsu võimaldamise juhtudel, teavitab teavet taotlenud isik kasutajat kirjalikku taasesitamist võimaldavas vormis andmete saamisest või nendele juurdepääsu võimaldamisest, andmete väljastamise või neile juurdepääsu võimaldamise eesmärgist ning väljastatud andmete koosseisust. Kasutajat ei teavitata, kui teavitamine võib:
- kahjustada teise isiku õigusi ja vabadusi;
  - ohustada lapse põlvnemise saladuse kaitset;
  - takistada kuriteo tõkestamist või kurjategija tabamist;
  - raskendada kriminaalmenetluses tõe väljaselgitamist.

## **7. Arvutivõrgu kasutajakonto**

- 7.1. Sisevõrgu kasutajaõiguste andmise eelduseks on isiku kohta kirje olemasolu Riigi Tugiteenuste Keskuse (RTK) personaliprogrammis SAP. Töötaja andmed peavad SAPis olema vähemalt kaks tööpäeva enne uue töötaja tööle asumist.
- 7.2. Kasutaja personali andmekogusse registreerimise tulemusena moodustub isikule automaatselt sisevõrgu personaalne kasutajakonto millele omistatakse õigused vastavalt määratud struktuuriüksusele. Kasutajakontot ei aktiveerita.
- 7.3. Kasutajakonto aktiveerimiseks peab kasutaja struktuuriüksuse juht, personali teenistuja või asutuse juhi poolt selleks volitatud isik vähemalt kaks tööpäeva enne kasutaja esimest tööpäeva saatma IT-abisse elektrooniliselt avalduse, kus on ära toodud uue kasutaja täpne esimene tööpäev.
- 7.3.1.Pöördumises edastada järgnev info:
- 7.3.1.1. töötaja nimi;
  - 7.3.1.2. isikukood;
  - 7.3.1.3. tööle asumise üksus;
  - 7.3.1.4. tööle asumise kuupäev (praktikandi, käsunduslepingu või muu tähtajalise lepinguga töötaja puhul ka töö lõppemise kuupäev);
  - 7.3.1.5. märkida tööks vajaminevad ligipääsud (meililistid, grupid);
  - 7.3.1.6. praktikantide, käsunduslepingu või muu tähtajalise lepingu alusel tööle asuva töötaja puhul märkida pöördumisse, et SAPi andmeid ei kanta.
- 7.4. Hiljemalt üks tööpäev enne uue kasutaja esimest tööpäeva annab IT-abi kasutajakonto aktiveerimise avalduse esitanule teada uue kasutaja kasutajanime ja esmase parooli. Kasutajakonto avatakse kasutaja esimesel tööpäeval hiljemalt kell 10.00.
- 7.5. Sisevõrgu kasutajakonto annab kasutajale õiguse kasutada isiklikku võrguketast, tema struktuuriüksuse võrgukettaid, Interneti, oma asutuse siseveebi, vastavalt asutusele dokumendihaldust ja elektronposti (kuju: „eesnimi.perenimi@rik.ee“ või vastavalt asutuste domeenile „@fin.ee“, „@aki.ee“, „@ekei.ee“ jne).

- 7.6. Iga kasutaja saab sisevõrgu kasutamiseks personaalse kasutajanime ja parooli. Alternatiivselt võib tööjaama sisenemiseks kasutada personaalset kiipkaarti (näiteks ID-kaart) ja selle juurde kuuluvat PIN-koodi.
- 7.7. Kasutajakonto lukustub parooli kolmekordsel valesti sisestamisel 10 minutiks. Kui konto pärast nimetatud perioodi ei avane või on kasutaja parooli unustanud, tuleb kasutajal konto lahti lukustamiseks pöörduda IT-abi poole.

## **8. Kasutajaõigused**

- 8.1. Juurdepääsuõiguste ja -piirangute jagamisel tuleb järgida põhjendatud teadmisi- ja juurdepääsuvajaduse olemasolu põhimõtet.
- 8.2. Kõik IT-teenuste kasutamisega kaasnevad kasutamissoigused- ja piirangud on personaalsed (kui konkreetse õiguse kohta pole öeldud teisiti) ning neid ei ole lubatud ühelt isikult teisele edasi anda.
- 8.3. Kui mõni õigusakt või vastava IT-teenusega seotud õiguste andmise kord ei sätesta teisiti, tellib IT-teenuste õiguse avamise ja sulgemise kasutaja struktuuriüksuse juht IT-abi kaudu.
- 8.4. Vastutus kasutajale õiguste andmise, muutmise või kustutamise osas lasub õiguste tellijal. Õiguste tellija peab veenduma, et õiguste saajal on õigus vastavaid õiguseid saada ja ta on tutvunud kõigi asjakohaste õigusaktide, juhendite ning kordadega, mis kaasnevad konkreetse juurdepääsuõiguse realiseerimisega.
- 8.5. Juurdepääsu saamiseks mõne teise struktuuriüksuse võrgukettale peab struktuuriüksuse juht, kelle kettale ligipääsu soovitakse, esitama vastava avalduse IT-abisse. Õigused antakse hiljemalt viie tööpäeva jooksul.
- 8.6. Kasutajagrupid, mille alusel vastavale IT-teenusele õiguseid antakse, peavad olema omaniku poolt defineeritud vastava IT-teenuse põhimääruses või muus IT-teenuse kasutamist reguleerivas korras. Kasutajagrupid peavad olema koostatud alljärgnevalt:
  - 8.6.1. gruppide arv peab olema väike, kuid arvestama teadmisi vajaduse olemasolu põhimõtteid;
  - 8.6.2. peab olema tagatud, et kasutajad saaksid oma õigused läbi gruppide.
- 8.7. Eriõiguste taotlemiseks peab kasutaja struktuuriüksuse juht, personali teenistuja või asutuse juhi poolt selleks volitatud isik esitama põhjendatud taotluse IT-abisse.
- 8.8. Kui kasutajal pole eriõiguseid enam otseste teenistus- või tööülesannete täitmiseks vaja, peab tema struktuuriüksuse juht, personali teenistuja või asutuse juhi poolt selleks volitatud isik sellest viivitamatult teatama IT-abisse.

## **9. Teenistus- või töösuhte peatumised pikaajalise töövõimetuse, pikaajalise puhkuse (sh lapsehoolduspuhkuse) ja pikaajalise lähetuse korral**

- 9.1. Teenistuja või töötaja lahkumisel pikemale kui 90-päevasele puhkusele, lapsehoolduspuhkusele või rasedus- ja sünnituspuhkusele, lähetusse, eemal viibimisel seoses töövõimetusega või muul põhjusel töö- või teenistussuhte peatumisel, peab tellija poolt selleks volitatud isik sellest IT-abisse teada andma, misjärel lukustatakse kõik kasutaja kasutajaõigused.
- 9.2. Tellija poolt volitatud isikul on õigus taotleda IT-abilt kasutaja kasutajaõiguste avatuks jätmist.
- 9.3. Töö- või teenistussuhte peatumise lõppemisest peab tellija poolt selleks määratud isik teavitama IT-abi vähemalt kaks tööpäeva ette, et oleks võimalik õigeaegselt lukustatud kasutajakonto avada.
- 9.4. Töö- või teenistussuhte peatumise lõppemisel taastatakse kasutaja õigused ja failid endisel kujul, kui tellija poolt selleks volitatud isik pole oma avalduses märkinud teisiti.
- 9.5. RIKil on õigus lukustada kontod (kaasa arvatud elektronpost), mida ei ole kasutatud üle 100 päeva.
- 9.6. Pärast töö- või teenistussuhte peatumise pöördumise saamist peatab IT-abi ligipääsu kasutaja postkastile. Postkastile pannakse kolmeks kuuks automaatteavitus, mis sedastab, et kasutaja

töö- või teenistussuhe on peatunud ja palub edastada pöördumine asutuse üldaadressile. Kasutaja võib enne teenistus- või töösuhte peatumist panna oma postkastile isikliku kontorist väljasoleku teavituse. Postkasti saabunud elektronposti edasisuunamine on keelatud.

## **10. Struktuuriüksuse muutumine ja kasutajaõiguste sulgemine**

- 10.1. Kui kasutaja vahetab teenistukohta struktuuriüksust, peab kasutaja struktuuriüksuse juht, personali teenistuja või tellija poolt selleks volitatud isik taotlema kasutajale IT-abist kõik tööks vajalikud õigused vähemalt kaks tööpäeva enne struktuuriüksuse muutumist. Teavituse peab sisaldama kasutaja uuel töökohal töötamise alustamise täpset kuupäeva. IT-abi muudab uuel teenistuskohal tööle asumise päeval hiljemalt kell 10.00 kasutaja sisevõrgu õigused selliselt, et need vastaksid uue struktuuriüksuse õigustele.
- 10.2. Kasutaja lahkumisel korraldab IT-abi kasutaja õiguste kustutamise kõigis RIKi hallatavates teenustes hiljemalt kasutaja viimasele tööpäevale järgneval tööpäeval. Samuti organiseerib IT-abi kasutaja kasutatavate RIKi väliste IT-teenuse pakkuja teavitamise vastavalt kokkulepetele nende teenuste pakkujatega.
- 10.3. Töötaja viimase tööpäeva tähtaja märkimisest SAPis järgmisel päeval kell 7.00 sulgetakse arvutikasutaja konto ligipääs automaatselt.
- 10.4. Praktikantide, käsunduslepingu või muu tähtajalise lepingu alusel töötanud töötaja arvutikasutaja ligipääsude sulgemine toimub automaatselt vastavalt töö lõppemise kuupäevale.
- 10.5. Kasutaja peab enne töö- või teenistussuhte lõppemist kustutama oma elektronpostkastist, võrgukettalt ja tööjaama kõvakettalt isiklikud ja ebaolulise sisuga e-kirjad ja failid.
- 10.6. Olulise sisuga tööalased failid (dokumendid, e-kirjad jms) ja vastamist vajavad e-kirjad peab lahkuv kasutaja üle andma otsese juhi poolt määratud ajaks, salvestades need oma struktuuriüksuse kettal asuvasse kausta „lahkunud teenistujate kaustad“ omanimelisse alamkausta. Struktuuriüksuse juht või tema poolt määratud isik kontrollib eelmainitud kohustuse täitmist ning märgib vajadusel lahkuva kasutaja üle antavate tööalaste failide loetelu ning andmed tööalaste failide üleandmise kohustuse täitmise kohta asutuse asjaajamiskorra kohasesse asjaajamise üleandmis-vastuvõtmisakti.
- 10.7. Pärast töö- või teenistussuhte lõppemist ligipääs kasutaja postkastile suletakse. Postkastile pannakse kolmeks kuuks automaatteavitus, mis sedastab, et kasutaja postkast on suletud ja palub edastada pöördumine asutuse üldaadressile. Kasutaja võib enne lahkumist panna oma postkastile isikliku kontorist eemaloleku teavituse. Postkasti saabunud elektronposti edasisuunamine on keelatud.
- 10.8. Kõik kasutajate varukoopiatele salvestatud personaalses postkastis olevad kirjad ja personaalsel võrgukettal olevad failid on varukoopiatelt taastatavad ühe aasta jooksul alates kasutaja lahkumisest. Pärast seda need kustutatakse jäädavalt.

## **11. Ministeeriumivälised kasutajad**

- 11.1. Ministeeriumiväliste kasutajate (kasutajad, kes ei ole personali andmebaasi järgi ministeeriumi töötajad) lubamiseks sisemistele kasutajatele mõeldud IT-teenuste kasutajateks, peab struktuuriüksuse juht või asutuse juhi poolt selleks volitatud isik, kelle vastutusel väline kasutaja RIKi hallatavatele teenuseis kasutama lubatakse, esitama elektrooniliselt taotluse IT-abisse.
- 11.2. Taotlus peab sisaldama isiku, kellele õiguseid soovitakse, kontaktandmeid, juurdepääsu vajaduse põhjendust, kirjeldust, milliseid ministeeriumi IT-teenuseid on vaja kasutada ja juurdepääsu algus- ning lõpptähtaega. Taotlusele peab olema lisatud kasutaja poolt täidetud ja digitaalselt allkirjastatud konfidentsiaalsuskinnitus.
- 11.3. Juurdepääsu tähtaja pikkus on maksimaalselt üks aasta juurdepääsu andmise hetkest. Kasutajakonto lukustatakse automaatselt, kui saabub juurdepääsu lõpptähtaeg või kui juurdepääsu ei ole kasutatud 90 päeva jooksul.

- 11.4. Kui esialgselt esitatud tähtajast ei piisa, tuleb vähemalt viis tööpäeva enne tähtaja saabumist esitada uus taotlus.
- 11.5. Kui välise kasutaja juurdepääs sisevõrku või mõnele ministeeriumi IT-teenusele ei ole enam vajalik, peab sellest viivitamatult teavitama IT-abi.

## **12. IT riist – ja tarkvara haldamine**

- 12.1. IT-riistvara (nt tööjaamad, printerid, skännerid) paigutamise planeerimisel peab konsulteerima RIKi IT-spetsialistidega ja paigutama need nii, et vastavat õigust mitteomavad inimesed ei omaks juurdepääsu AK informatsioonile ning IT-vahendid oleks kaitstud varguse eest.
- 12.2. Keelatud on ilma RIKi loata IT-riistvara ja tarkvara lisamine (v.a mobiilsed andmekandjad ja käesoleva korra punkti 5.1 alusel), ümberpaigutamine, häälestamine, eemaldamine, konfigureerimine ja ministeeriumi haldusala territooriumilt välja viimine (v.a eemaldatavad andmekandjad ning nutiseadmed ja sülearvutid). Siia hulka kuuluvad ka tulemüüri, viirusetõrje või muude turvafunktsioonide omandamine või muutmise või välja lülitamine.
- 12.3. IT-riistvara kolimisest tuleb IT-abi ette teavitada vähemalt kaks nädalat.
- 12.4. Kasutajal on keelatud sisevõrgu ja operatsioonisüsteemide turvaaukude, ründekoodi, paroolihakkimise tarkvara, võrguskannerite, ründetarkvara või muu sarnase kasutamine.
- 12.5. Kui kasutaja soovib kasutada sisevõrgus ministeeriumile mittekuuluvat seadet, peab ta tegema põhjendatud taotluse IT-abisse. Taotluse rahuldamiseks peavad olema täidetud järgmised tingimused:
  - 12.5.1. otsese juhi kooskõlastus;
  - 12.5.2. infoturbejuhi kooskõlastus;
  - 12.5.3. infoturbejuhi hinnangul ei põhjusta seadme kasutamine sisevõrgus lisariske. Näiteks tööjaamade, nutiseadmete turvaseaded ja konfiguratsioon peab olema sama turvaline või turvalisem kui vastavatel RIKi hallata olevatel seadmetel.
- 12.6. Tööjaamade sisevõrku lisamise eelduseks on tööjaama lisamine ministeeriumi Windows domeeni, millega kaasneb domeeni reeglite laienemine isiklikule seadmele. Samuti võib RIK nõuda tööjaama viiruse/nuhkvara tõrje väljavahetamist ministeeriumis kasutuses oleva viirusetõrje lahenduse vastu.
- 12.7. Riistvara tohib ministeeriumi sisevõrku või tööjaama külge ühendada alles pärast kinnituse saamist, et avaldus on rahuldatud ning tööjaama üle vaatamist ja konfigureerimist IT-spetsialisti poolt.
- 12.8. Kõigist avalduses toodud riistvara andmete muudatustest või riistvara kasutamise lõpetamisest ministeeriumi võrgus või tööjaamas peab tööjaama kasutaja koheselt teavitama IT-abi.

## **13. Paroolinõuded**

- 13.1. Kasutaja vastutab temale antud paroolide saladuses hoidmise eest. Kui parooli või kiipkaardi PIN-kood on saanud teatavaks kõrvalistele isikutele või on kahtlus, et see on võinud juhtuda, on kasutaja kohustatud parooli/PIN-koodi koheselt muutma või laskma parooli/kiipkaardiga seotud kasutajaõigused läbi IT-abi tühistada.
- 13.2. Kasutaja kohustub sisevõrku sisenema ja IT-teenuseid kasutama ainult oma personaalse kasutajatunnuse ja parooli või kiipkaardiga ning tagama, et tema kasutajatunnuse või kiipkaardi abil ei pääse sisevõrku keegi teine.
- 13.3. Parool, mis kasutajale esmastel kasutajaõiguste saamisel antakse, on ühekordne (kui vastava IT-teenuse kasutusjuhendis ei ole märgitud teisiti) ning kasutaja kohustub selle vahetama esimesel sisselogimisel ainult temale teadaoleva parooli vastu.
- 13.4. Parooli ei ole lubatud ühelegi andmekandjale krüpteerimata kujul jäädvustada või dokumenteerida ega teatavaks teha ühelegi teisele isikule (ka mitte IT-abi töötajatele).
- 13.5. Kasutaja ei tohi kasutada oma tööalaseid paroole töövälistes süsteemides.

- 13.6. Parool peab koosnema numbrite, väike- ja suurtähtede kombinatsioonist. Soovitav on lisaks kasutada kirjavahemärke. Parooli pikkus peab olema vähemalt 9 sümbolit.
- 13.7. Parool ei tohi olla:
  - 13.7.1. lihtsasti ära arvatav, näiteks tuletatud enda või pereliikmete isikuandmetest, sõiduki registreerimisnumbrist, lemmiklooma nimest, sõnaraamatus leiduv sõna või kuupäev vms;
  - 13.7.2. koostatud klaviatuurijärjestuses tähtedest või numbritest;
  - 13.7.3. lihtsasti tuletatav eelnevalt kasutatud paroolidest.
- 13.8. Parooli tuleb vahetada regulaarselt. Maksimaalne parooli kehtivusaeg on 90 päeva.
- 13.9. Parooli ununemise või parooli mittetöötamise korral peab kasutaja sellest teavitama IT-abi. IT-abis luuakse kasutajale uus ühekordne parool. Parool edastamisel kasutajale peab IT-abi peab veenduma, et kasutaja on see, kes ta väidab end olevat.
- 13.10. Tööjaama juurest lahkudes peab kasutaja sulgema või lukustama tööjaama (näiteks Windows logo klahv + L) ning eemaldama kiipkaardi.

#### **14. Võrgukettad, failide hoidmine ja printimine**

- 14.1. Iga kasutaja jaoks on ette nähtud personaalne ja struktuuriüksuse võrguketas või -kettad. Personaalsele võrguketale viitab ka kasutaja kodukataloog (Minu dokumendid/My Documents) töölaua.
- 14.2. Personaalsel võrguketlale on olemas dokumendid on kättesaadavad vaid kasutajale endale.
- 14.3. Failide salvestamisel võrguketastele tuleb jälgida, et failid salvestatakse asukohta kuhu saavad ligi vaid isikud/grupid, kes tohivad juurdepääsu omada.
- 14.4. Säästlikuks sisevõrgu ressursside kasutamiseks on iga kasutaja personaalsel võrguketlale ja struktuuriüksuse võrguketlale limiit, mille kvoodid on leitavad IT-abi siseveebi lehelt (<https://rik.just.sise/itabi>).
- 14.5. Kasutajat teavitatakse personaalse võrguketta ja struktuuriüksuse juhti struktuuriüksuse võrguketta mahulimiidi lähenemisest. Limiidi lähenemise teate saanud kasutaja peab ebavajalikud failid võrgukettalt kustutama või pöörduma failide arhiveerimiseks või limiidi suurendamiseks IT-abi poole.
- 14.6. Statsionaarsete tööjaamade kasutaja peab hoidma oma faile vaid võrguketastel. Sülearvuti kasutaja peab tööalaste failide salvestamisel tööjaama kettale arvestama, et varukopeerimine tagatakse vaid võrguketastel olevatele failidele.
- 14.7. Varukopeeritud faile saab varukoopiatelt taastada ühe aasta jooksul nende salvestamisest alates. Pärast seda varukoopiad kustutatakse.
- 14.8. AK informatsiooni printimisel või paljundamisel tuleb väljaprintitud/paljundatud materjal koheselt pärast printimist printerist eemaldada.
- 14.9. Leides printerisse või koopiamasinasse unustatud AK materjali tuleb see omanikule koheselt ära viia (kui isik on teada) või hävitada.

#### **15. Elektronpost**

- 15.1. Iga kasutaja jaoks on ette nähtud isiklik elektronposti kasutajakonto, mille juurde kuulub ka kalendri kasutamise võimalus.
- 15.2. Kasutaja peab kasutama tööalaste mailide saatmiseks ja vastuvõtmiseks vaid temale ministeeriumi poolt eraldatud ametlikku elektronposti aadressi.
- 15.3. Igal elektronposti kasutajakontol mahupiirang, mille ületamisel on kasutaja kohustatud kustutama või arhiveerima vanad elektronkirjad. Samuti on saadetavale või vastuvõetavale elektronposti manusele kehtestatud mahupiirang. Piirangute kohta saab infot IT-abi siseveebi lehelt (<https://rik.just.sise/itabi>).

- 15.4. Kasutaja elektronpostkasti sisu (kirja mustandid, saadetud ja saadud kirjad, manused, kalendri kanded) on varukoopiatelt taastatav ühe aasta jooksul alates salvestamisest/saatmisest/saamisest. Pärast seda varukoopiad kustutatakse jäädavalt.
- 15.5. Lahkunud kasutaja postkasti säilitatakse kolm kuud.
- 15.6. Kasutajal on keelatud avada kahtlusi tekitava pealkirjaga või kahtlustäratavalt elektronposti aadressilt saabuvat elektronkirja ning käivitada elektronkirjade manuses olevaid programme või skripte siseveebi lehelt.
- 15.7. Keelatud on töölase elektronposti aadressi kasutamine tarbijamängude mängimiseks, isiklike kommertsteadete tellimiseks, foorumite kasutamiseks ning muudeks tegevusteks, mis võivad põhjustada hulgalise kommertsteadete ja spämmi saatmise mõnele tellija elektronposti aadressile.
- 15.8. Kirjade manuaalsel edasisaatmisel tuleb jälgida, et ei saadetaks välja AK informatsiooni selleks mitte volitatud isikutele.
- 15.9. Dokumentide saatmisel on soovitatav kasutada PDF vormingut.
- 15.10. Informatsiooni, mille avalikuks tulek võib kahjustada oluliselt tellija mainet või põhjustada tellijale olulist kahju, saatmisel väljapoole ministeeriumi, tuleb see krüpteerida ID-kaardi või muud RIKi poolt aktsepteeritud krüptolahendust kasutades. Infot aktsepteeritavate krüptolahenduste kohta saab IT-abi siseveebi lehelt (<https://rik.just.sise/itabi>).

## **16. Avaliku võrgu (Interneti) kasutamine**

- 16.1. Kasutajal on keelatud edastada Interneti kaudu (ka läbi sõnumivahetus-programmide, faili jagamisteenuste, pilveteenuste, foorumite, blogide, kommentaaride või muu sarnase) AK teavet krüpteerimata kujul.
- 16.2. Kasutajal on keelatud laadida Internetist omavoliliselt (ilma IT-abi kirjalikku taasesitamist võimaldava loata) alla mistahes programme, programmiuuendusi, mänge, ebaseaduslikult omandatud autoriõigusega kaitstud elektroonses vormis andmeid jms.
- 16.3. Kasutajal on keelatud külastada ilma otsese tööalase vajaduseta veebilehekülgi, mille külastamine kasutaja poolt võib tuua kaasa tellija või RIKi maine kahjustumise. Näiteks pornograafilisi materjale või illegaalset autoriõiguse all olevaid materjale sisaldavad lehed.
- 16.4. Turvaohu vältimiseks piiratakse võrgus potentsiaalselt viiruseid või muud ründetarkvara sisaldavate veebilehtede külastamine. Kui kasutaja leiab, et mõni vajaliku lehe külastamine on piiratud ebaõigelt, tuleb sellest teada anda IT-abisse, kes organiseerib lehe taasavamise juhul, kui see pole ohtlik.

## **17. Digitaalsed andmekandjad**

- 17.1. Töölase teabe käitlemisel tohib kasutada vaid RIKi poolt heaks kiidetud ja üle kontrollitud digitaalseid andmekandjaid. Andmekandjad antakse üle tellija poolt volitatud isikule, kes peab vajadusel nende üle arvestust ja korraldab seiret.
- 17.2. AK informatsiooni salvestamine eemaldatavale digitaalsele andmekandjale on lubatud vaid otseste teenistus- või tööülesannete täitmiseks.
- 17.3. AK informatsiooni sisaldava andmekandja viimisel väljapoole tellija administratiivala, saatmisel posti või kulleriga tuleb andmekandja krüpteerida ID-kaarti kasutades või mõne muu RIKi poolt heaks kiidetud krüptolahendusega (näiteks kasutada krüptopulka). Krüptolahenduste kohta saab infot IT-abi siseveebi lehelt (<https://rik.just.sise/itabi>). Posti või kulleriga saates tuleb andmekandja lisaks pakkida kinnisesse pakendisse. Pakendi välisküljelt ei tohi olla võimalik tuvastada andmekandja sisu ega selle kirjeldust. Andmekandja kohalejõudmist tuleb saatja poolt kontrollida.



- 17.4. Kui AK informatsiooni hoidmine andmekandjatel ei ole enam otseste teenistus- või tööülesannete täitmiseks vajalik, tuleb informatsioon andmekandjalt koheselt kustutada või anda andmekandja hävitamiseks RIKi IT spetsialisti kätte.
- 17.5. AK informatsiooni sisaldava andmekandja kadumisest või vargusest tuleb koheselt teavitada IT-abi.
- 17.6. Kui töökohustuste tõttu on mõnes tööjaamas vajalik sage võõraste andmekandjate kasutamine, tuleb see kooskõlastada IT-abiga. Vajadusel tõstetakse sellise tööjaama turvalisust või lepitakse kokku asutused, kelle andmekandjaid usaldatakse.

## **18. RIKi poolt väljastatud sülearvuti ja nutiseadme (nutitelefon, tahvelarvuti) kasutamine ja hoidmine**

- 18.1. Vältimaks seadme varastamist, kaotamist või kahjustamist peab kasutaja:
  - 18.1.1. hoidma seadet avalikes kohtades isikliku järelevalve all, st mitte jätma seadet valveta kohtadesse, kus on oht selle varastamiseks (nt auto salongi, lahtise akna alla);
  - 18.1.2. mitte jätma seadet otsese päikesekiirguse või kõrge/madala temperatuuri kätte, samuti tolmusesse või niiskesse keskkonda;
  - 18.1.3. transportima süle- ja tahvelarvutit vaid selleks ettenähtud kotis;
  - 18.1.4. reisimisel kandma seadet käsipagasina.
- 18.2. Tagamaks nutiseadmes olevate andmete turvalisust ja piiramaks viiruste levikut peab kasutaja:
  - 18.2.1. AK informatsiooni, parooli või PIN-koodi sisestamisel ja/või töötlemisel veenduma, et seade on paigutatud nii, et kuvaril toimuv ei ole kolmandatele isikutele nähtav;
  - 18.2.2. seadme juurest lahkumisel seadme sulgema või lukustama ning kiipkaardi kasutamisel selle eemaldama;
  - 18.2.3. seadme kaudu WiFi jagamisel (*hotspot*) kasutama vaid autenditud krüpteeritud ühendust ja mitte kasutama WiFi võrgu nimeks nime, mis võimaldab kasutajat või kasutaja ametit identifitseerida.
  - 18.2.4. kahtluse või teadmise korral, et seadme tulemüür ja/või viirusetõrjetarkvara ei ole töökorras või, et seadmes on viirus, mitte ühendama seadet sisevõrku, vaid andma seadme võimalikult kiiresti RIKi IT-spetsialistile kontrollimiseks.
- 18.3. Seadme lokaalsel kettal/mälus olevate andmete varundamise eest vastutab kasutaja. Andmete säilimise tagamiseks peab kasutaja:
  - 18.3.1. töötades ministeeriumi sisevõrgus hoidma andmeid selleks määratud võrgukettal;
  - 18.3.2. ühendades seadme sisevõrku, tegema lokaalsel kettal olevatest tööks vajalikest andmetest varukoopia võrgukettale.
- 18.4. Kasutaja peab RIKi nõudmisel esitama seadme RIKi IT-spetsialisti kätte korraliseks hoolduseks.
- 18.5. Seadme vargusest, kaotamisest või hävimisest on kasutaja kohustatud viivitamatult teavitama IT-abi ning kustutama esimesel võimalusel oma varastatud või kaotatud nutitelefoni või tahvelarvuti sisu läbi OWA (juhul kui seade on seadistatud sünkroniseerima andmeid tööandja e-posti serveriga). Seadme varguse korral on kasutaja kohustatud koheselt teavitama ka politseid.

## **19. Kaugtöö**

- 19.1. RIK tagab VPN kanali RIKi hallatavatele sülearvutitele. VPN kasutamise juhendi leiab IT-abi lehelt.
- 19.2. RIKi poolt mittehalltavate seademega on võimalik kaugtöö üle terminal-lahenduse (vaid ID-kaardi põhine autentimine) või läbi veebipõhise elektronposti (OWA). Juhised nende lahenduste kasutamiseks leiab IT-abi lehelt.
- 19.3. Kaugtöö tegemisel RIKi poolt mittehalltatavast seadmest ei tohi väljapoole kaugtöö keskkonda (nt seadme kõvakettale või mälukaardile) salvestada krüpteerimata AK informatsiooni.

- 19.4. Tagamaks turvalisuse, peab kasutaja kaugtöö tegemisel RIKi poolt mittehallatavast seadmest veenduma, et:
- 19.4.1. kaugtööks valitud asukoht ja seade on usaldusväärsed. Usaldusväärsete asukohtade hulka ei loeta avalikke seadmeid (nt kohvikute, lennujaamade, hotellide üldkasutatavad arvutid), kus on suur oht, et seade on nakatunud pahavaraga;
  - 19.4.2. seadme operatsioonisüsteemile ja seadmes kasutatavale tarkvarale on paigaldatud viimased turvauuendused ning paigaldatud viirusetõrje;
  - 19.4.3. seadmes ei ole pahavara, mis võiks sisestatud kasutajanime, parooli või andmeid salvestada ja kellelegi teisele edasi saata või ministeeriumi sisevõrku nakatada;
  - 19.4.4. seadme juurest lahkudes väljutakse kaugtöö keskkonnast ja suletakse kõik kaugtöö tegemiseks mõeldud rakendused ja veebiaknad ning kui kaugtöö toimus läbi veebibrauseri, kustutatakse veebibrauseri vahemälu, ajalugu ja võimalikud salvestatud paroolid;
  - 19.4.5. tööjaam on paigutatud selliselt, et AK informatsiooni töötlemise ajal ei ole ekraanile kuvatav info volitamata isikutele nähtav.

## **20. Nutisedmega kalendri ja elektronposti sünkroniseerimine ning mobiilne dokumendihaldus**

- 20.1. Lähtudes tööalasest vajadusest võimaldatakse RIKi poolt nutiseadmega juurdepääs asutuse poolt määratud isikutele kalendrile, elektronpostile ja mobiilse dokumendihalduse DELTA rakendusele.
- 20.2. Juurdepääsu saamiseks tuleb pöörduda IT-abi poole. Avalduses peab olema märgitud nutiseadme tootja ning mudel, millega soovitakse kalendrit ja elektronposti sünkroniseerida või mobiilset dokumendihaldust kasutada.
- 20.3. Toodud IT-teenuste kasutamise võimaldamisel rakenduvad nutiseadmele järgmised piirangud:
- 20.3.1. seade lukustub automaatselt, kui seda pole üle 5 minuti järjest kasutatud;
- 20.4. iga seadme ekraani lahtilukustamise korral küsitakse kasutajalt vähemalt 5-kohalist lukukoodi, välja arvatud juhul kui telefon võimaldab rakendada sõrmejäljega kasutaja tuvastamist;
- 20.4.1. lukukood aegub iga kuue kuu tagant;
  - 20.4.2. juhul, kui lukukood sisestatakse kaheksa korda valesti, kustutatakse telefonist kõik failid, sätted ja kontaktid. Telefon läheb vaikimisi sätetele. Andmed on võimalik taastada vaid viimasest varukoopiast juhul, kui telefoni omanik on andmetest varukoopia teinud. RIK nutisedmete andmeid ei varukopeeri;
  - 20.4.3. nutiseadme mälu ja mälukaart krüpteeritakse nii, et sinna salvestatud faile ja elektronposti ei oleks võimalik ilma telefoni PIN-koodi teadmata kätte saada.
- 20.5. Kui kasutaja telefon ülal toodud piirangute rakendamist ei toeta, siis kaugjuurdepääsu ei võimaldata.
- 20.6. Tagamaks AK teabe töötlemisel turvalisuse, kohustub kasutaja:
- 20.6.1. mitte kasutama lukukoodina ühesuguseid numbreid, järjestikuseid numbreid või kasutajaga seotud andmetest tuletatavaid numbreid (sünniaasta, sünnikuupäev, lapse sünniaasta jne), mis on kergesti ära arvatavad või leitavad näiteks sotsiaalmeedia vahendusel;
  - 20.6.2. mitte avaldama oma lukukoodi ega krüpteerimata kujul jäädvustama ühelegi andmekandjale;
  - 20.6.3. uuendama seadme tarkvara kui seadme tarkvaras avastatakse turvaauke;
  - 20.6.4. paigaldama uusi rakendusi ja uuendusi, sh personaalseks kasutamiseks mõeldud, ainult usaldusvääretest allikatest (nt seadme tootja enda tarkvaramust) ning veenduda enne rakenduse paigaldamist nende turvalisuses (st lugedes nende kohta kommentaare ja jälgides, et need ei küsiks telefonis liigselt erinevaid õiguseid);
  - 20.6.5. mitte eemaldama oma seadmelt tootjapoolset kasutuspiirangut (*jailbreak, rooting*);

- 20.6.6. mitte ühendama seadet üle Bluetoothi või USB kaabli tundmatute või mitteusaldusväärsete seadmetega;
- 20.6.7. seadme ühendamisel teiste seadmetega üle Bluetoothi, kasutama turvalist sidumiskoodi;
- 20.6.8. seadme varastamisel või kaotamisel koheselt kustutama portaali „post.rik.ee“ kaudu seadme mälu sisu ja sätted (juhised on leitavad IT-abi siseveebilehelt - <https://rik.just.sise.itabi>) ning teavitama juhtunust võimalikult kiiresti IT-abi;
- 20.6.9. mitte andma seadet kasutamiseks teistele isikutele ja sellega võimaldama volitamata isikute juurdepääsu elektronpostile ja kalendritele;
- 20.6.10. enne seadme müümist, utiliseerimist, edasikinkimist, väljavahetamist, parandusse või garantiisse viimist peab teavitama sellest IT-abi ja kustutama seadme mälu sisu ja sätted nii, et telefoni kaudu poleks võimalik teenistus- või töölastele andmetele juurdepääsu saada.

## **21. Sisevõrgu väärkasutuse tagajärjed**

- 21.1. Kahtluse tekkimisel sisevõrgu kasutamise reeglite rikkumise või võrgu väärkasutuse osas on RIKi IT-spetsialistidel õigus peatada või piirata kasutusõigusi kuni asjaolude selgitamiseni. Kasutaja õiguste peatamisest või piiramisest peab RIKi IT-spetsialist viivitamatult teavitama kasutajat ja tema struktuuriüksuse juhti.
- 21.2. Sisevõrgu kasutamise reeglite rikkumise kahtlusega isikul on õigus esitada omapoolne selgitus.
- 21.3. Riistvara süülise rikkumise korral on vara soetanud asutusel õigus nõuda kahju hüvitamist.
- 21.4. IT-teenuste kasutamist reguleerivate õigusaktide mittetäitmine võib tuua kaasa kriminaal-, väärteo- või distsiplinaar karistuse või kui kasutaja tegutseb lepingu alusel, siis muu tagajärje kohustuste rikkumise eest.