Kinnitatud
peadirektori käskkirjaga 27.10.2025 nr 1-1/25/48-1

# Infosüsteemide kasutamise kord (K8)

Protsess: Infosüsteemide kasutamine

Protsessi omanik: ISO juhataja

Versioon: 7

Infosüsteemide kasutamise kord sisaldab:

1. Üldpõhimõtted
2. Mõisted
3. Arvuti taotlemine ja kasutamise üldpõhimõtted
4. Piirangud arvuti kasutamisel
5. E-posti kasutamise põhimõtted
6. Infosüsteemide ja võrguressursside kasutamise põhimõtted
7. Infosüsteemi intsidendist teavitamine
8. Infoturbeintsidentide käsitlemine
9. Kasutajanimed ja salasõnad
10. Kasutajaõiguste andmine ja kehtetuks tunnistamine

## 1. Üldpõhimõtted

- **Sisu ja eesmärk:** Riigi Tugiteenuste Keskusele (edaspidi *RTK*) osutavad teenuslepete alusel infotehnoloogia- ja kommunikatsiooniteenuseid (IKT teenuseid) Rahandusministeeriumi Infotehnoloogiakeskus (edaspidi RMIT) ja Riigi Info- ja Kommunikatsioonitehnoloogia Keskus (edaspidi *RIT*). Käesolev kord reguleerib IKT teenuste kasutamise põhimõtteid ja korda RTK-s. Korra eesmärk on tagada RTK-ga avalik-õiguslikus teenistus- ja usaldussuhtes olevate ametnike või eraõiguslikus töösuhtes olevate töölepinguliste töötajate (edaspidi läbivalt kasutatud *töötajad)* infosüsteemide otstarbekas ja turvaline kasutamine. Lisaks käesolevale korrale on infosüsteemide kasutamise põhimõtted kirjeldatud erinevates juhistes, mis on koondatud ja kättesaadavad RIT teenusveebist https://teenused.rit.ee/
- **Kasutusulatus**: kord laieneb kõigile RTK töötajatele ja kehtib nii RTK füüsilistes asukohtades kui ka väljaspool füüsilisi asukohti infosüsteeme ja arvuteid kasutades.
- **Vastutajad**: protsessi omanik on infosüsteemide arendamise osakonna juhataja. Korra ajakohasena hoidmise eest vastutab infoturbe spetsialist. Korra rakendamise eest vastutavad kõik RTK töötajad.
- **Korra lisa**: RTK infoturvapoliitika
- **Viited:**
  - Avaliku teabe seadus (AvTS) https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv
  - Isikuandmete kaitse seadus (IKS) https://www.riigiteataja.ee/akt/112072014051?leiaKehtiv
  - RTK ja RITi vaheline koostöö kokkulepe (teenuslepe)
  - RTK ja RMIT vaheline koostöö kokkulepe (teenuslepe)
  - RTK Personali värbamise ja töö- ning teenistussuhete haldamise kord (K11)
  - RTK töökoha tellimise ankeet
- **Kontaktid:**

- IT-abi iseteenindusportaal https://itabi.sise.rit.ee/, RIT IT-abi 663 6464, itabi@rit.ee;
- Maksu-ja Tolliameti teabejuhtimiskeskus 676 2888, valve@emta.ee;
- RTK infoturbe spetsialist maris.riba@rtk.ee, 5917 6160.

## 2. Mõisted

- **Andmete töötlemine** – andmete kogumine, salvestamine, korrastamine, säilitamine, muutmine, nende kohta päringute teostamine, nendest väljavõtete tegemine, andmete kasutamine, üleandmine, ühendamine, sulgemine, kustutamine või hävitamine või mitu eeltoodud toimingut.
- **Arvuti** – sülearvuti või nutitelefon.
- **Arvutitöökoha profiil** – struktuurüksus(t)ele või töötaja(te)le kokku pandud riist- ja tarkvara kogum, kasutaja õigused ning juurdepääsud.
- **Infosüsteem** – inimestest, tark- ja riistvarast koosnev süsteem, mis töötleb ja tõlgendab infot. Selle mõiste all on mõeldud ka andmekogusid ja erinevaid IT rakendusi.
- **Infosüsteemi kasutaja** – RTK töötaja, kellele töö- või teenistusülesannetest tulenevalt ja nende täitmiseks on antud õigused infosüsteemide kasutamiseks.
- **Infosüsteemi omanik** – struktuuriüksus, kelle huvides on antud infosüsteem loodud või kasutusele võetud.
- **Infoturbeintsident** – realiseerunud oht, mis põhjustab RTK-le ja/või RTK infovarale kahju, mis võib olla: rahaline, konfidentsiaalsete andmete lekkimine, andmete hävimine, tööseisak, asutuse maine kahjustamine.
- **Intsident** – planeerimata teenuse katkestus või selle kvaliteedi langus ning samuti seadme või rakenduse tõrge, mis pole veel teenusele mõju avaldanud.
- **IT teenus** – infotehnoloogiat kasutav ja äriprotsesse toetav teenus, mis on inimeste, protsesside ja tehnoloogiate kombinatsioon ning mis peab olema kirjeldatud teenusleppes.
- **Kasutajatugi** – RIT või vastava infosüsteemi kasutajatugi.
- **Krüpteerimine** – informatsiooni kaitsmise võimalus, muutes andmed loetamatuks ja kasutamiskõlbmatuks inimesele, kellel puudub vastav dekrüpteerimisvõti.
- **Kaugtöö** – töö korraldamise ja tegemise vorm, kus infotehnoloogiliste vahendite abil täidetakse tööülesandeid väljaspool tööandja ruume.
- **Mitmikautentimine** – autentimine mitme eri tüüpi identsustõendiga, näiteks kiipkaardi, parooli ja biomeetrikuga.
- **Probleem** – ühe või mitme intsidendi tekkimise põhjus või mingisugune puudus teenuse või rakenduse toimivuses.
- **Tootmiskeskkond** - tegelikke talitlusprotsesse toetav infosüsteem, erinevalt arendus- või testimiskeskkonnast.
- **Tööseisak** – olukord, kus töö on häiritud kauem kui vastavale rakendusele omistatud maksimaalne lubatud seisaku aeg infotehnoloogiliste rakendustega toetatud ärikriitilistes töölõikudes ja mis puudutavad kogu RTK-d või RTK struktuuriüksust. Juhul kui rakendusele pole lubatud seisaku aega määratud, loetakse tööseisakuks enam kui 30 minutilist katkestust, mis puudutab tervet RTK-d, osakonda või talitust ühtselt.

## 3. Arvuti taotlemine ja kasutamise üldpõhimõtted

3.1. Uue töötaja arvuti tellib vahetu juht, täites töökoha tellimise ankeedi (RTK töö- ja teenistussuhete korra alusel). Personali- ja haldusosakond edastab täidetud ankeedi RIT kasutajatoele.

3.2. Peale arvuti kättesaamist kinnitab arvuti kasutaja e-posti teel IT varade registrist saabunud lingi kaudu, et ta on arvuti kätte saanud ning teadlik sellega seonduvatest kohustustest. Arvuti tagastamisel saab kasutaja e-posti teel IT varade registrist vastavasisulise teavituse.

3.3. Kasutajakonto luuakse kujul eesnimi.perenimi@rtk.ee.

3.4. Vaikeseadetes on igale kasutajale loodud OneDrive kataloog kettaruumiga 100 GB, mille suurus on põhjendatud vajaduse korral muudetav tehes vastavasisulise taotluse RIT kasutajatoele.
3.5. Printimisel on kohustuslik prinditud dokumendid printerist koheselt eemaldada või hävitada. Töösuhte lõppemisel tuleb arvuti tagastada komplektselt ja terviklikult koos laadija ning dokiga.

## 4. Piirangud arvuti kasutamisel

4.1. Arvuti on tööülesannete täitmiseks. Isiklikul otstarbel arvutit kasutades tuleb arvestada, et kõiki tehtavaid tegevusi võidakse jälgida.
4.2. Tarkvara või võrgu konfiguratsiooni muutmine (või uue võrgu installeerimine) ja viirusetõrje ning tulemüüri tarkvara välja lülitamine ei ole lubatud.
4.3. Arvuti ja selle lisaseadmete korpuseid ei tohi ise avada ega eemaldada või lisada komponente.
4.4. Arvutiga ei ole lubatud ühendada RIT poolt kontrollimata andmekandjaid (telefonid, mälupulgad jne). Samuti ei ole lubatud ühendada RTK sisevõrguga seadmeid, milleks puudub RIT luba, sh kasutada RTK võrgu või arvutite skaneerimise, pealtkuulamise või muid võrguliiklust segavaid rakendusi või seadmeid.
4.5. Arvuti kahjustumisel, vargusel või kaotamisel tuleb koheselt teavitada RIT kasutajatuge ja struktuuriüksuse juhti. Arvuti varguse korral tuleb esitada avaldus ka politseile ja välismaal viibides võtta avalduse esitamise kohta vastav tõend.
4.6. Välisriikidesse reisimisel tuleb arvuti kaasa võtmine kooskõlastada vastavalt RIT reisimise kasutusjuhendile: https://teenused.rit.ee/et/kasutusjuhendid/infoturve/reisimine.
4.7. Arvutit ja selle lisaseadmeid tuleb kohelda heaperemehelikult ja vältida materiaalse kahju tekkimist, sh puhastada neid tolmust ja mustusest selleks ette nähtud vahenditega ning kaitsta neid kahjustumise eest kasutades arvuti transpordiks alati sobivat polsterdusega arvutikotti.
4.8. Arvuti ja andmete turvalisuse tagamiseks on oluline:
  4.8.1. arvuti juurest lahkudes lukustada ekraan;
  4.8.2. mitte jätta arvutit järelevalveta selle kasutamisel väljaspool RTK ruume ja võtta ruumist lahkudes arvuti endaga kaasa. Kui seda ei saa teha, siis lukustada arvuti ekraan eemal viibimise ajaks;
  4.8.3. mitte kasutada arvutit viisil või kohtades, mis võimaldab võõrastel näha arvuti ekraani (näiteks: ühistranspordis, kohvikus, lennujaamas või kaugtööl muudes kohtades);
  4.8.4. kaitsta sülearvutit kahjulike keskkonnatingimuste (liigniiskus, äärmuslikud temperatuurid) eest;
  4.8.5. arvuti mootorsõidukisse jätmisel veenduda, et arvuti ei oleks väljastpoolt sõidukit nähtav;
  4.8.6. reisimisel kanda arvutit käsipagasis;
  4.8.7. arvuti pikemaajalisel mobiilsel kasutamisel kanda kaasas laadijat ja aku kasutusea pikendamiseks kasutada vaid tootja heakskiidetud laadijat;
  4.8.8. akutoitel töötades salvestada andmeid piisavalt tihti, et tagada nende säilimine;
  4.8.9. hoiduda arvuti kasutamisest mis tahes viisil, mille tulemusel võib juurdepääsupiiranguga teave saada teatavaks kolmandatele isikutele või põhjustada informatsiooni hävinemise.
4.9. Arvuti veebibrauseri kaudu ei ole lubatud külastada veebilehekülgi, mille külastamine töötaja poolt võib tuua kaasa RTK maine kahjustumise ega laadida arvutisse või võrguserverisse järgmist materjali (v.a. juhul, kui see tegevus kuulub töötaja töö- või teenistusülesannete hulka):
  4.9.1. mistahes tarkvara, sh mänge, programme, programmiuuendusi jms;
  4.9.2. ebaseaduslikult omandatud autoriõigusega kaitstud elektroonses vormis andmeid (muusika, tekst, pildid, filmid jms);
  4.9.3. hea tavaga vastuolus oleva sisuga materjale.

4.10. Arvuti kasutamisel tuleb arvestada, et kogu võrguliiklus logitakse ja salvestatakse. Infoturbe spetsialistil on tööalasest vajadusest tulenevalt õigus ette teatamata tutvuda kasutaja võrguliikluse logidega.

## 5. E-posti kasutamise põhimõtted

5.1. E-posti konto luuakse kujul eesnimi.perenimi@rtk.ee. Mitme ees- ja perenimega töötaja puhul kasutatakse üht ees- ja perenime. Samanimeliste töötajate puhul lisatakse hiljem tööle tulnud inimese perekonnanime lõppu number.
5.2. Vaikeseadetes on e-posti lubatud kogumaht 100 GB, mille suurus on põhjendatud vajaduse korral muudetav. E-postkast on mõeldud ainult tööalase kirjavahetuse jaoks.
5.3. E-postiga ei saa saata suuremaid manuseid kui 20 MB.
5.4. Turvalisuse tagamiseks ei tohi avada kahtlusi äratava pealkirjaga ja/või e-posti aadressilt saabuvat e-posti ega selles sisalduvaid manuseid või linke või käivitada sellega kaasas olevaid programme ning skripte. Kahtlust äratav e-post lisada uue e-posti kirja manusesse ja edastada RIT kasutajatoele ning infoturbe spetsialistile.
5.5. Juurdepääsupiiranguga või isikuandmeid sisaldavat informatsiooni võib e-posti teel edastada ainult krüpteeritud kujul.
5.6. Tööalase informatsiooni saatmiseks ja vastuvõtmiseks kasutatakse ainult tööalast e-posti aadressi ning seda ei suunata RTK-välistele e-posti aadressidele.
5.7. Tööalast e-posti aadressi ei kasutata RTK-välistes postiloendites ja foorumites, v.a. juhul, kui see tegevus kuulub töötaja töö- või teenistusülesannete hulka.
5.8. E-postiga ei tohi saata käivitatavaid ning süsteemseid faile, näiteks: exe, vbs, pif, scr, bat, cmd, com, cpl, dll jms, v.a juhul kui selline tegevus kuulub töötaja töö- või teenistusülesannete hulka.

## 6. Infosüsteemide ja võrguressursside kasutamise põhimõtted

6.1. Infosüsteemide kasutamisel tuleb täita kõiki kehtivaid andmekaitse- ja autoriõigusealaseid õigusakte ning järgida asutuses kehtivat andmekaitsepoliitikat.
6.2. Infosüsteemide kasutamine on lubatud ainult töötajale isiklikult loodud konto või juurdepääsuõiguste kaudu. Neid juurdepääse ei ole lubatud edasi anda ega kasutada infosüsteeme kellegi teise konto või õigustega.
6.3. Kasutajal ei ole lubatud vaadata, kasutada või väljastada RTK sisest teavet, mis ei ole avalik või otseselt seotud tema töö- või teenistusülesannete täitmisega.
6.4. Infosüsteeme ja võrguressursse kasutakse ainult töö- või teenistusülesannete täitmiseks ning sisevõrku ei koormata mittetööalaste failide ja tegevustega. E-posti ja failiservereid tuleb regulaarselt korrastada, kustutades ebaolulise sisuga kirjad ja failid.
6.5. ID-kaart või digi-ID tuleb kaardilugejast eemaldada, kui see ei ole enam infosüsteemi kasutamiseks vajalik.
6.6. Asutusesiseseks kasutamiseks mõeldud teavet ei tohi salvestada kohta, kus see võib olla kättesaadav volitamata isikutele. Kui tööülesannetest lähtuvalt on vaja välisele andmekandjale salvestada asutuse siseseks kasutamiseks mõeldud informatsiooni, mille avalikuks saamine kahjustaks RTK-d või RTK partnereid/kliente, tuleb see krüpteerida. Krüpteeritud andmed tuleb lahti krüpteerida säilitamiseks ja töödelda vastavalt eesmärgile.
6.7. Kõik tööalased failid hoitakse RTK pilvteenusel, et tagada andmete säilimine, mille kadumine võib põhjustada RTK-le olulist kahju.
6.8. Tootmiskeskkonna infosüsteemidesse andmete sisestamisel tuleb tagada nende õigsus. Tootmiskeskkonda ei sisestata andmeid testimise eesmärgil.
6.9. Kui töötaja on mobiiltelefoni sünkroniseeritud tööandja pilvteenustega, tuleb mobiiltelefoni kaotuse või varguse korral teavitada RIT kasutajatuge, kes kaughalduse teel

katkestab ühenduse asutuse sisuga. Ühtlasi tuleb pöörduda mobiilside teenusepakkuja poole, et viivitamatult blokeeritaks SIM-kaart ja lisataks mobiiltelefon musta nimekirja.

6.10. Kui tööalaselt teatavaks saanud RTK-d ja/või kliente puudutavat informatsiooni soovitakse kasutada koolitöödes (lõputööd, praktikakokkuvõtted jms), tuleb see kooskõlastada vahetu juhi ja andmete omanikuga.

6.11. Kui infosüsteemi kasutamist reguleerib mingi õigusakt, siis selle õigusakti mittetäitmine võib tuua kaasa kriminaal- või distsiplinaarkaristuse.

6.12. Infosüsteemi kasutamise reeglite eiramise kahtluse korral on infoturbe spetsialistil järelkontrolli käigus õigus kontrollida töötajale väljastatud arvutit (sh arvutisse salvestatud ja installeeritud programme ning asutuse e-posti sisu).

6.13. Töötajal on õigus esitada ettepanekuid infosüsteemide turvalisuse tõstmise, efektiivsema toimimise või muu töökorraldusliku muudatuse kohta.

# 7. Infosüsteemi intsidendist teavitamine

7.1. Infosüsteemi intsidendi (teenuse katkestus või tõrge vms) puhul peab töötaja edastama vastava infosüsteemi kasutajatoele järgneva informatsiooni:

7.1.1. oma ees- ja perenime, telefoninumbri;

7.1.2. infosüsteemi nimetus, kus intsident tekkis;

7.1.3. intsidendi tekkimise kuupäev, kellaaeg ja asukoht;

7.1.4. korrektne kirjeldus tekkinud veasituatsioonist;

7.1.5. veateade ekraanilt, lisades võimalusel ekraanipildi failina;

7.1.6. lisades võimalusel näite konkreetsete andmetega (isikukood/registrikood, summad, kuupäevad jm);

7.1.7. kui tegemist on veakahtlusega, siis tuleb lisada teatele kirjeldus õigeks peetavast lahendusest.

# 8. Infoturbeintsidentide käsitlemine

8.1. Töötaja peab teavitama infoturbeintsidendist (potentsiaalne või realiseerunud oht teabe turvalisusele) RIT kasutajatuge ja RTK infoturbe spetsialisti. Kiiruse huvides tuleb infoturbeintsidendist teatada koheselt telefoni teel. Väljaspool tööaega (E-N 17:00-8:00, R 15:45-E 8:00) tuleb toimunud infoturbeintsidendist teavitada Maksu- ja Tolliameti teabejuhtimiskeskust.

8.2. Infoturbeintsidendi puhul peab töötaja edastama:

8.2.1. oma ees- ja perenime, telefoninumbri;

8.2.2. infoturbeintsidendi või selle ohu kirjelduse;

8.2.3. infoturbeintsidendi tekkimise kuupäeva, kellaaja ning asukoha;

8.2.4. infoturbeintsidendi hinnangulise tõsiduse.

8.3. Infoturbeintsidendi toimumise teate vastu võtnud töötaja (reeglina RIT töötaja) tuvastab intsidendi toimumise fakti ning intsidendi tõsiduse ja organiseerib koos vastava infosüsteemi omaniku ja haldajaga intsidendi või selle ohu kõrvaldamise. Kõigist infoturbeintsidentidest peab intsidendi vastu võtnud töötaja teavitama infoturbe spetsialisti koheselt, kasutades selleks kokkulepitud suhtluskanaleid (telefon, SMS, e-post jne). Infoturbe spetsialist korraldab intsidendi registreerimise RMIT Jiras;

8.4. Infoturbeintsidendi järelkontrolli vajaduse otsustab infoturbe spetsialist ning viib selle vajadusel läbi.

8.5. Infoturbe spetsialist esitab infoturbeintsidentide kohta läbi viidud järelkontrollide kokkuvõtte peadirektorile ning teeb muudatusettepanekud intsidentide kordumise vältimiseks.

8.6. Kõik RTK töötajad on kohustatud igakülgselt kaasa aitama infoturbeintsidendi põhjuste väljaselgitamisele.

# 9. Kasutajanimed ja salasõnad

9.1. Arvutisse sisenemiseks kasutatakse ID-kaarti, sõrmejälge või näotuvastust.
9.2. Infosüsteemidesse sisenemiseks kasutatakse ID-kaarti, Smart-IDd, mobiil-IDd või kasutajanime ja salasõna.
9.3. Iga töötaja võib omada ühes infosüsteemis ühte kasutajakontot, v.a juhul, kui mitme konto omamine on vajalik töö- või teenistusülesannete täitmiseks.
9.4. Infosüsteemi kasutajanimed on unikaalsed ja seotud vastava töötaja isikuga.
9.5. Iga töötaja peab infosüsteemi ajutise salasõna vahetama esmakordsel sisenemisel, kui see on tehniliselt võimalik.
9.6. Töötaja peab tagama, et salasõna on teada ainult temale.
9.7. Kui salasõna on saanud teatavaks kõrvalistele isikutele või on kahtlus, et see on võinud juhtuda, on töötaja kohustatud salasõna koheselt muutma või laskma salasõnaga seotud kasutajaõigused kehtetuks tunnistada.
9.8. Salasõnu tuleb muuta perioodiliselt vähemalt kord kvartalis või kui infosüsteem sellest teavitab.
9.9. Salasõnade haldamiseks on soovitatav kasutada paroolihaldurit PasswordState https://parool.srv.gov.ee/
9.10. Salasõnade talletamine kirjalikult on lubatud ainult erandjuhtudel kui neid hoitakse turvalises asukohas.
9.11. Kui IT-süsteem võimaldab, siis on soovitav kasutada mitmikautentimist (täiendav autentimine nt biomeetria, telefoninumbri või nutirakenduse abil) või autentimist MobiilID, SmartID või ID kaardiga.
9.12. Salasõnadeks ei tohi olla:
  9.12.1. kergesti ära arvatavad, järjestikuseid tähti sisaldavad vms viisil ebaturvalised kombinatsioonid, mis võivad hõlbustada kasutajakonto volitamata kasutamist;
  9.12.2. sõnastikes esinevad sõnad k.a võõrkeeltes;
  9.12.3. sõnad, mis koosnevad kasutajat isikustada võimaldavatest andmetest (nimed, mootorsõiduki registreerimismärgid, telefoninumbrid, isikukoodid, sihtnumbrid jne) kas õiget- või tagurpidi kirjutatult;
  9.12.4. salasõnad, mis on kasutuses juba mõnes teises infosüsteemis;
9.13. Kasutatavate salasõnade pikkus peab olema vähemalt 12 (kaksteist) märki.
9.14. Salasõna peab sisaldama vähemalt kolme järgmistest: suurtäht, väiketäht, number, sümbol (! “ # ¤ % & ( ) = ? \ } ] [ { $ @ ’ - . , * _ : ; < > +) .
9.15. Kasutajatunnus lukustatakse peale nurjunud sisselogimiskatseid vastavalt infosüsteemi seadistusele.
9.16. RTK-s kasutusel olevaid salasõnasid ei ole lubatud kasutada RTK-välistes infosüsteemides, jäädvustada ühelegi andmekandjale krüpteerimata kujul või dokumenteerida ega teatavaks teha ühelegi teisele isikule sh saata krüpteerimata kujul e-mailiga.
9.17. Intsidentidest kasutajaõiguste, kasutajanimede ja salasõnadega tuleb teavitada vastava infosüsteemi või RIT kasutajatuge ja RTK infoturbe spetsialisti. Intsidentidest teavitamisel on keelatud saata või öelda salasõnasid.

# 10. Kasutajaõiguste andmine ja kehtetuks tunnistamine

10.1. Töötaja tohib omada vaid tema töö- või teenistusülesannete täitmiseks otseselt vajalikke kasutajaõigusi. Välistele infosüsteemidele antakse kasutajaõigused vastavalt infosüsteemide omanikega sõlmitud lepingutele.
10.2. Kõigi taotletavate õiguste kohta peab õiguste taotlemise taotluses olema märgitud lühidalt, milliste töö- või teenistusülesannete täitmiseks läheb töötajal konkreetset õigust vaja. Õiguste taotlus tuleb edastada e-kirja teel vastava infosüsteemi kontaktisikule või RIT kasutajatoele.

10.3. Kasutajaõiguste taotluse esitaja peab olema veendunud, et töötaja või isik, kellele õiguseid taotletakse, omab ülevaadet õigustega seonduvatest kasutusjuhenditest ja on teadlik õiguste kasutamisega kaasnevatest riskidest ning oskab neid maandada.

10.4. Arvuti lokaalse administreerimise õiguse saamiseks esitab töötaja vahetu juht põhjendatud taotluse RIT kasutajatoele. RIT kasutajatugi kooskõlastab taotluse RTK infoturbe spetsialistiga.

10.5. Infosüsteemi testimise kasutajaõiguste saamiseks esitab taotleja struktuurüksuse juht vastava infosüsteemi kasutajatoele e-kirja teel taotluse. Juhul kui testimine toimub reaalsete isikustatud andmetega, peab taotluse eelnevalt kooskõlastama RTK infoturbe spetsialist.

10.6. RTK-sse praktikale asunud isikute infosüsteemide kasutajaõigused tellib RIT või vastava infosüsteemi kasutajatoelt praktikale asunud isiku struktuuriüksuse juht. Kasutajaõiguste taotlusse tuleb märkida õiguste kehtivuse algus- ja lõpukuupäev. Lõpukuupäeva saabudes peab konto automaatselt lukustuma.

10.7. Kui töötaja ei vaja töö- või teenistusülesannete täitmiseks enam infosüsteemi kasutajaõigust edastab töötaja vahetu juht koheselt sellekohase teate e-kirja teel vastava infosüsteemi kasutajatoele, kes korraldab vastava kasutajaõiguse kehtetuks tunnistamise.

10.8. Töötaja töölt lahkumisest, teenistus- või töösuhte peatumisest (va puhkuse või töövõimetuslehe korral) või töötaja üleviimisest teise struktuuriüksusesse teavitab struktuurüksuse juht RIT kasutajatuge vähemalt 3 (kolm) tööpäeva enne töötaja töölt lahkumise, teenistus- või töösuhte peatamise või üleviimise kuupäeva (v.a üleviimiste puhul, mis kestavad vähem kui 30 kalendripäeva). Erakorralistel asjaoludel võib taotleda õiguste ja/või ligipääsude kohest sulgemist.

10.9. Infoturbe spetsialist kontrollib töötajatele antud õiguste õiguspärasust ja sulgemist.

10.10. Infoturbe spetsialistil on õigus põhjendatud kahtluse korral nõuda RIT või vastava infosüsteemi kasutajatoelt kahtlustäratavate õiguste kohest sulgemist, teavitades sellest vastavat struktuuriüksuse juhti ja osakonnajuhatajat.