

ARVUTIVÕRGU KASUTAMISE KORD

Sissejuhatus	2
Reguleerimisala	2
Mõisted	2
Üldsätted	2
Arvutisüsteemi kasutajaõiguste andmine, peatamine ja lõpetamine	2
Arvutisüsteemi kasutajaõiguste andmine, peatamine ja lõpetamine	2
Nõuded kasutajatunnusele	3
Nõuded kasutajatunnusele	3
Kasutajate õigused ja kohustused	4
Kasutajate kohustused	4
Kasutajate piirangud	4
Kasutajate õigused	5
Kasutajate vastutus	5
IT spetsialisti õigused ja kohustused	5
IT spetsialisti kohustused	5
IT spetsialisti õigused	6
IT spetsialisti vastutus	6
TK Infosüsteemide kasutamine	6
Failiserveri kasutamine	6
G Suite kasutamine	6
Interneti kasutamine	6
Kiirsuhtlustarkvara (IM – Instant Messaging)	7
E-posti kasutamine	7
Elektronpostiaadresside kuju	8
Sülearvutite kasutamine	8
Riist- ja tarkvara paigaldamine	8
Lõppsätted	8
Korra rakendamine ja järelvalve	8

I. Sissejuhatus

1. Reguleerimisala

- 1.1.1. Tartu Kunstikool (edaspidi TK) arvuti ja arvutivõrgu kasutamise kord (edaspidi kord) sätestab arvuti ja arvutivõrgu kasutajate (edaspidi kasutajate) üldised õigused ning kohustused.
- 1.1.2. Arvutite ja arvutivõrguga seonduvate täiendavate juhiste kehtestamisel lähtutakse käesolevast korrast.
- 1.1.3. Kord kehtib kõigile TK kasutajatele TK infosüsteeme kasutades nii TK-s kui ka TK-st väljaspool.

2. Mõisted

- 2.1.1. TK infosüsteemid – teave, arvutid ja nendega seonduvad tarkvara ning seadmed, arvutivõrk ja selle komponendid ning ressursid, sealhulgas internetiühendus.
- 2.1.2. Arvutisüsteem - TK infosüsteemide baasosa ehk arvutid ja nendega seonduvad seadmed, elektronpostiserver, ühiskasutusega võrguserverid ja -printerid ning internetiühendus (edaspidi arvutisüsteem).
- 2.1.3. IT-vahend - Arvutid ning nendega seonduvad seadmed ja tarkvara.
- 2.1.4. Tarkvararakendused - teatud töö- ja õpiprotsesside toetamiseks ja/või läbiviimiseks välja töötatud infotehnoloogilised lahendused, sealhulgas neis sisalduv teave.
- 2.1.5. Kasutaja – kõik isikud, kellele on antud TK infosüsteemide kasutaja- ja juurdepääsuõigused.
- 2.1.6. IT spetsialist – arvutisüsteemi haldaja.
- 2.1.7. kaasaskantav arvutustehnika – sülearvutid, projektorid, diktofonid, fotoaparaadid, videokaamerad, tahvelarvutid, mobiiltelefon.
- 2.1.8. Asutusesiseseks kasutamiseks (edaspidi AK) tunnistatud informatsioon – informatsioon vastavalt Avaliku teabe seadusele.

3. Üldsätted

- 3.1.1. TK töötajatele tagatakse TK infosüsteemide kasutamine TK ametiruumides sisekorra eeskirjas toodud tööaja vältel ning vastavalt TK tööd reguleerivatele õigusaktidele.
- 3.1.2. TK infosüsteemid on TK omand, mille kasutamisel tuleb alati juhendada:
 - 3.1.2.1. TK tegutsemise eesmärkidest, mis on määratud TK põhimäärusega,
 - 3.1.2.2. kehtivast seadusandlusest,
 - 3.1.2.3. käesolevast korrast,
 - 3.1.2.4. muudest asjassepuutuvatest TK regulatsioonidest,
 - 3.1.2.5. heast tavast.
- 3.1.3. TK infosüsteemid ning sellega seonduvate ruumide haldajad võivad lähtuvalt vajadusest kehtestada täiendavaid reegleid, mis ei vähenda käesoleva korra nõudeid.
- 3.1.4. Kasutajatoe telefoninumber on **+372 5334 1545** ja e-posti aadress **it@tartukunstikool.ee**.

II. Arvutisüsteemi kasutajaõiguste andmine, peatamine ja lõpetamine

4. Arvutisüsteemi kasutajaõiguste andmine, peatamine ja lõpetamine

- 4.1.1. Arvutisüsteemi kasutaja- ja juurdepääsuõigused (edaspidi kasutajaõigused) annab ja muudab IT spetsialist.
- 4.1.2. Kasutajaõigusi antakse:
 - 4.1.2.1. TK töötajale - reeglina nende TK-s töötamise ajaks;
 - 4.1.2.2. ajutistele töötajale – tähtaegselt kuid tavaliselt mitte kauemaks kui üks aasta;

- 4.1.2.3. TK õpilastele - õppetöö ajaks;
- 4.1.2.4. IT-teenuseid osutavatele isikutele, kes vajavad teenuse osutamiseks kasutajaõigusi – tähtaegselt teenuse osutamise ajaks,
- 4.1.2.5. Muudele isikutele – tähtaegselt, kuid mitte kauemaks kui 6 kuud. Kui muu isik vajab kasutajaõigusi pärast nimetatud tähtaega, tuleb esitada uus taotlus.
- 4.1.3. Taotlejateks on
 - 4.1.3.1. TK töötajale ja ajutisele töötajale – vahetu juht või tugistruktuuri juht;
 - 4.1.3.2. IT teenust osutavale isikule – tugistruktuuri juht;
 - 4.1.3.3. TK õpilastele - administraator ja IT spetsialist;
 - 4.1.3.4. muule isikule – isikut kutsunud ja/või võõrustava TK struktuuriüksuse juht.
- 4.1.4. Kasutajaõigus luuakse taotluse alusel ja kasutajaõiguse saamise eelduseks on kehtiv leping TK-ga või õppimine TK-s.
- 4.1.5. Kasutajaõiguste taotlus peab sisaldama kasutaja nime, töökohta, tööle asumise alust ja kuupäeva, kasutajale vajalikku kasutajaõiguste ulatust ning vajadusel tähtaega.
- 4.1.6. Kasutajaõigused antakse kasutajatunnuse loomisega, milleks omistatakse kasutajale unikaalne kasutajanimi ning antakse esmane salasõna. Esmane salasõna tuleb vahetada esmakordsel arvutisüsteemi sisenemisel vastavalt punktis 5.1.4 toodud nõuetele.
- 4.1.7. Korda tutvustatakse kõikidele töötajatele ja õpilastele.
- 4.1.8. Kasutajaõigusi ei laiendata ilma taotluseta.
- 4.1.9. Töösuhte lõppemisel või tähtajaliselt antud kasutajaõiguste tähtaja saabumisel kasutajaõigused suletakse. Kauem kui üks aasta suletud kasutajaõigused kustutatakse.
- 4.1.10. Töölepingu peatamisel (välja arvatud puhkuse ajaks ja ajutise töövõimetuse ajaks) kasutajaõigused peatatakse.
- 4.1.11. Kasutajaõiguste taastamiseks (peatatud või suletud kasutajaõiguste korral) esitab taotleja IT-spetsialistile vastava taotluse.

III. Nõuded kasutajatunnusele

5. Nõuded kasutajatunnusele

- 5.1.1. Kasutajatunnus koosneb kasutajanimest ja salasõnast.
- 5.1.2. Kasutajatunnus on personaalne ja seda pole lubatud ühelt inimeselt teisele edasi anda.
- 5.1.3. Kasutajatunnus suletakse koheselt peale töösuhte lõppemist või kui selgub, et kasutaja tööülesanded on muutunud selliselt, et ta enam ei vaja oma tööülesannete täitmiseks vastavat kasutajatunnust.
- 5.1.4. Kasutajatunnus on reeglina kujul eesnimi.perekonnanimi. Korduvate nimede puhul lisatakse lõppu number.
- 5.1.5. Salasõna **peab**
 - 5.1.5.1. olema vähemalt 8 kirjamärki pikk;
 - 5.1.5.2. sisaldama vähemalt ühte väike- (u, i, d vms) ja suurtähte (G, R, A vms) ning vähemalt ühte numbrit (5, 3, 9 vms). Pole soovitatav kasutada täpitähti.
- 5.1.6. Salasõna **ei tohi**
 - 5.1.6.1. olla kergesti äraarvatav (näiteks nimi, kuupäev, auto number, vms);
 - 5.1.6.2. sisaldada järjestikku rohkem kui kahte sama kirjamärki;
 - 5.1.6.3. sarnaneda varem kasutatud salasõnadele;
 - 5.1.6.4. sarnaneda teistes TK infosüsteemides kasutatavatele salasõnadele.
- 5.1.7. Salasõna **tuleb**

- 5.1.7.1. koheselt asendada kui on teise isiku poolt teada saadud. Administraatorilt või IT spetsialistilt saadud salasõna tuleb ära muuta esimesel sisselogimisel.
- 5.1.7.2. vahetada regulaarselt vähemalt 365 päeva järel. Enne uue salasõna aktiveerimist tuleb kasutada endist salasõna. Kui muutmine ei ole võimalik, siis tuleb sellest kohe teavitada administraatorit või IT spetsialisti;
- 5.1.7.3. sisestada teistele isikutele märkamatu.

IV. Kasutajate õigused ja kohustused

6. Kasutajate kohustused

- 6.1.1. Kasutaja on kohustatud TK infosüsteemide turvalisuse tagamiseks:
 - 6.1.1.1. hoidma saladuses kasutajaõigusi tagavaid salasõnu ja kasutajanimed. Salasõnu ega viiteid selle sisule ei tohi anda teistele isikutele ega edastada neid e-postiga;
 - 6.1.1.2. mitte võimaldama või lubama teistel isikutel kasutada oma kasutajatunnuseid, sh lastel, tuttaval, kolleegidel;
 - 6.1.1.3. vältima volitamata isikute juurdepääsu oma valduses olevatele andmetele ja informatsioonile;
 - 6.1.1.4. teavitama vahetut juhti või IT spetsialisti kõikidest TK infosüsteemide häiretest, turvaaukudest, turvainsidentidest ja ohtudest, näiteks defektidest, avariidest või vargustest;
 - 6.1.1.5. arvuti juurest lahkudes (ka lühiajaliselt) lukustama ekraani, pikemaks ajaks lahkudes, näiteks õhtul koju, logima arvutist välja.
 - 6.1.1.6. säilitama tema kasutada antud IT vahendite riist- ja tarkvaralise kompleksuse;
 - 6.1.1.7. järgima IT spetsialisti poolt kehtestatud TK infosüsteeme puudutavaid piiranguid ja täitma nende poolt tehtud asjassepuutuvaid korraldusi;
 - 6.1.1.8. kontrollima kõiki enda poolt välisel andmekandjal toodavaid või allalaaditavaid faile viirustõrje programmiga. Kõigist arvutiviirusega nakatumise kahtlustest tuleb kohe teavitada IT spetsialisti ja mitte jätkata tööd TK infosüsteemides ilma IT spetsialisti nõusolekuta.
 - 6.1.1.9. vältima esemete ja vedelike sattumist arvutisse ja lisaseadmetesse;
 - 6.1.1.10. võimaldama teostada tema valdusesse antud IT vahendite ülevaatus ja tehnilist hooldust ning toimetama vahendid vajadusel IT spetsialisti kätte;
 - 6.1.1.11. töösuhte või õpilasstaatuse lõppemisel tagastama tema kasutusse antud IT-vahendid ning üle andma tema arvutis olevad säilitamist vajavad failid IT-spetsialistile.

7. Kasutajate piirangud

- 7.1.1. Kasutajal on keelatud
 - 7.1.1.1. kasutada teistele isikutele omistatud kasutajatunnuseid (näiteks kasutada kaastöötaja kasutajanime arvutisse logimisel, e-kirjade lugemisel, rakendustes töötamisel);
 - 7.1.1.2. salasõnade üleskirjutamine krüpteerimata kujul;
 - 7.1.1.3. kasutada TK infosüsteemi ja selle kasutajatunnuseid isikliku või muu tulu saamise eesmärgil, mis ei lähtu TK põhimääruse kohasest tegevusest;
 - 7.1.1.4. TK infosüsteemide võimalike turvaaukude kasutamine täiendavate juurdepääsuõiguste ja privileegide saamiseks;
 - 7.1.1.5. omavoliline muudatuste tegemine arvuti standardseadistustes, sh riist- ja tarkvarakonfiguratsioonis, võrguaadresside ning muude süsteemsete parameetrite muutmine;
 - 7.1.1.6. peatada IT-spetsialisti poolt paigaldatud haldus- ja viirustõrje programme;
 - 7.1.1.7. töökohustustest mittetulenev andmete eemaldamine, kustutamine, loetamatuks muutmine või ülekirjutamine;
 - 7.1.1.8. TK infosüsteemis olevast infost tööks mittevajalike väljatrükkide tegemine või sellise info kopeerimine mistahes andmekandjatele;

- 7.1.1.9. jätta AK tunnistatud informatsiooni sisaldavaid andmekandjaid kergesti nähtavatesse või ligipääsetavatesse kohtadesse või arvuti seadmesse. Kasutaja eemalolekul tuleb andmekandjaid hoida lukustatavas sahtlis või kapis.
- 7.1.1.10. viia TK ruumidest välja arvuteid ja lisaseadmeid, va kaasaskantav arvutustehnika;
- 7.1.1.11. hoida mistahes välistel andmekandjatel AK dokumente krüpteerimata kujul. (erandiks on varundus ja arhiivindus, aga neid hoitakse turvatud ruumis)
- 7.1.1.12. tegevus, mis häirib TK infosüsteemide tööd või kasutust ning segab teisi kasutajaid nii otseselt kui ka kaudselt (näiteks ressursside tahtliku raiskamise teel või e-posti masspostitusega selleks konkreetset soovi mitte avaldanud isikutele);
- 7.1.1.13. hoida võrguketastel isiklikke faile.
 - 7.1.2. TK infosüsteemides on keelatud hoida, kasutada või levitada:
 - 7.1.2.1. illegaalselt omandatud või litsentseerimata tarkvara;
 - 7.1.2.2. autorikaitse alla kuuluvat tarkvara või andmefaile vms., mille kohta ei ole TK-l kasutusluba;
 - 7.1.2.3. sündsusetu sisuga faile.

8. Kasutajate õigused

- 8.1.1. Kasutajal on õigus saada informatsiooni kõigist muudatustest ja sündmustest TK infosüsteemides, mis mõjutavad oluliselt selle kasutamist või kasutajate privaatsust.
- 8.1.2. Kasutajal on õigus teha ettepanekuid TK infosüsteemide töö, teenuste ja halduste paremaks korraldamiseks.

9. Kasutajate vastutus

- 9.1.1. Kasutaja vastutab
 - 9.1.1.1. kõigi talle määratud kasutajatunnuste kasutamisel sooritatud tegude eest ja kõigi tema käes olevate IT vahendite säilimise ning turbe eest;
 - 9.1.1.2. oma arvutis olevate töö ja õpiülesannetega seotud failide tõstmise eest serverikettale tagavarakoopiate tegemiseks.

V. IT spetsialisti õigused ja kohustused

10. IT spetsialisti kohustused

- 10.1.1. Primaarseteks kohustusteks on tagada TK infosüsteemide toimivus, turvalisus ning teenuste kättesaadavus oma vastutusala ulatuses.
- 10.1.2. Oma vastutusala ulatuses on IT spetsialist kohustatud
 - 10.1.2.1. looma ja juurutama juurdepääsuõiguste haldamise põhimõtted, mis tagaksid arvutisüsteemis ja tarkvararakendustes autentse ja usaldusväärse teabe loomise ja haldamise;
 - 10.1.2.2. tagama juurdepääsuõiguste andmise ning haldamise arvutisüsteemis ja tarkvararakendustes, sh nende muutmise kasutaja volituste muutumisel;
 - 10.1.2.3. andma kasutajatele eelteavet olulistest muudatustest arvutisüsteemis ja tarkvararakendustes ning teavitama sündmustest, mis võivad mõjutada kasutajate privaatsust ning arvutisüsteemi ja tarkvararakenduse kasutamist;
 - 10.1.2.4. hoiatama kasutajaid ette võimalikest häiretest arvutisüsteemis ja tarkvararakendustes, mis on seotud plaaniliste remont- ja häälestustöödega;
 - 10.1.2.5. pidama saladuses oma töökohustuste täitmise käigus teatavaks saanud andmeid, mille kohta neil puudub andmete omaniku luba seda edasi anda, v.a. juhud, kui seadus kohustab informatsiooni teatavaks tegema;
 - 10.1.2.6. koostama ja tegema kasutajatele kättesaadavaks arvutisüsteemi ja tarkvararakenduste vastavad juhised;
 - 10.1.2.7. tagama tagavarakoopiate tegemise ja säilimise vastavalt kehtivale varundusplaanile, samuti vajadusel andmete taastamise;
 - 10.1.2.8. kontrollima TK infosüsteemide hooldust teostavate kolmandate osapoolte tööd.

- 10.1.2.9.seadistama arvutid nii, et ekraanilukk aktiveeruks hiljemalt 15 minuti möödudes;
- 10.1.2.10. tagama rämpsposti filtreerimise enne selle kasutajani jõudmist parimal võimalikul moel;
- 10.1.2.11. tagama viirusetõrje tarkvara installeerimise ja kaasajastamise;
- 10.1.2.12. muutma riist- ja tarkvara algsed salasõnad;
- 10.1.2.13. seadistama tööjaamad nii, et nendega saab tööd alustada alles pärast kasutajanime ja salasõna sisestamist;
- 10.1.2.14. deponeerima serverite ja võrguseadmete administraatoritasemel pääsuõigust tagavad paroolid.

11. IT spetsialisti õigused

- 11.1.1.IT spetsialistil on õigus oma vastutusalas TK infosüsteemide toimivuse ja turvalisuse tagamiseks
 - 11.1.1.1.ajutiselt piirata arvutisüsteemi ja tarkvararakenduste kasutamist nii, et see võimalikult vähe häiriks arvutisüsteemi ja tarkvararakenduste kasutajate tööd.
 - 11.1.1.2.jälgida kõikvõimalikke võrguühendusi, annulleerida võrgu ülekoormust põhjustav või pahavara levitav (Interneti) võrguühendus ette teatamata;
 - 11.1.1.3.kehtestada ressursipiiranguid üle võrgu või töökohtade kaupa;
 - 11.1.1.4.keelata remont- või häälestustööde teostamise ajaks igasugune töö terves võrgus, selle segmendis või töökohal;
 - 11.1.1.5.nõuda kasutajatelt kehtestatud reeglite ning vajalike meetmete täitmist;
 - 11.1.1.6.kasutada oma tööülesannete täitmiseks kaugadministreerimise vahendeid;
 - 11.1.1.7.teostada auditit salasõnade haldamise korra ja juurdepääsuõiguste järgimise osas (näiteks paroolide murdmine);
 - 11.1.1.8.rakendada koheselt sanktsioone reeglite rikkumise ilmnemisel või informatsiooni lekkimise vältimiseks (piirata kasutajaõigusi, eemaldada programme, lugeda ning kustutada faile jm).

12. IT spetsialisti vastutus

- 12.1.1.IT spetsialist vastutab oma vastutusala ulatuses
 - 12.1.1.1.TK infosüsteemide toimivuse ja turvalisuse tagamise eest;
 - 12.1.1.2.riist- ja tarkvara paigaldamise, TK infosüsteemi lülitamise, konfigureerimise ja haldamise eest;
 - 12.1.1.3.vastavalt kehtivale varundusplaanile andmete tagavarakoopiate tegemise, säilitamise ja taastamise eest.
- 12.1.2.IT spetsialist ei vastuta kasutaja arvutis olevate andmete tagavarakoopiate tegemise ja olemasolu eest.

VI. TK Infosüsteemide kasutamine

13. Failiserveri kasutamine

- 13.1.1.Kasutajal on andmete TK arvutivõrgus hoidmiseks võimalik kasutada TK failiserveri ressursse.
- 13.1.2.Kasutajatele on andmete failiserveril hoidmiseks defineeritud kasutajaprofiil.

14. G Suite kasutamine

- 14.1.1.Kasutajal on andmete hoidmiseks võimalik kasutada TK G-Suite ressursse.

15. Interneti kasutamine

- 15.1.1.Interneti kasutamine on ette nähtud töö- ja õpi ülesannete täitmiseks.
- 15.1.2.TK arvutivõrku ja TK poolt töötajale antud e-posti aadressi on keelatud kasutada Internetis isiklike seisukohtade avaldamiseks, isikliku tulu saamiseks, ebasüüdsaks

infovahetuseks, Interneti-ühenduse või arvutiressursside raiskamiseks või mõnel muul moel, mis ei ole TK huvides.

15.1.3. Keelatud on AK tunnistatud informatsiooni edastamine Interneti kaudu krüpteerimata kujul ja Internetist tundmatute failide käivitamine või allalaadimine.

15.1.4. Kõiki Internetist allalaetud faile tuleb esmalt kontrollida viirusetõrje programmiga.

15.1.5. Interneti kasutamisel tuleb olla tähelepanelik ja pigem umbusklik, et mitte langeda pettuste ohvriks.

15.1.6. IT spetsialistil on õigus jälgida Interneti-ühendusi ja kasutust üldvõrgu kaudu ning suunata kogu liiklust läbi vastavate kontrollmehhanismide.

16. Kiirsuhtlustarkvara (IM – Instant Messaging)

16.1.1. Elektrooniline kiirsuhtlus toimub Slack, Google Hangouts, Discord, Skype'i jne tarkvaraplatvormil.

16.1.2. Kasutajad võivad kasutada isiklikku kontot tööülesannetega seotud kirjavahetuseks.

16.1.3. Kiirsõnumi saatmisel tuleb erilist tähelepanu pöörata sellele, et sõnum ei satuks valele aadressaadile.

16.1.4. Keelatud on:

16.1.4.1. AK liigitatud dokumentide ja failivahetus kiirsuhtlustarkvara kaudu;

16.1.4.2. avada saabunud kahtlasi või tundmatuid linke, viiteid ning faile, eriti kui ka saatja on tundmatu. Kahtluse tekkimisel tuleb konsulteerida IT spetsialistiga;

16.1.4.3. edastada krüpteerimata konfidentsiaalset informatsiooni või muud teavet, sealhulgas paroole;

16.1.4.4. kiirsuhtlustarkvara ressursse raiskav, ebaviisakas või sündsusetu kasutamine, sealhulgas otseselt tööülesannetega mitteseotud masspostituse korraldamine, kasutajakonto registreerimine tööülesannetega mitteseotud elektronpostiloenditesse või vestlusruumidesse.

17. E-posti kasutamine

17.1.1. Elektrooniline kirjavahetus ja grupitöö toimub G-Suite tarkvara platvormil.

17.1.2. Kasutajale antud TK e-posti aadress on ette nähtud töö- ja õpi ülesannetega seotud kirjavahetuse jaoks.

17.1.3. E-posti saatmisel tuleb erilist tähelepanu pöörata sellele, et kiri ei satuks valele aadressaadile ning täita tuleb teema (Subject) väli.

17.1.4. Failide edastamisel e-posti teel tuleb vastuvõtjale edastada faili liik ja faili sisu lühikirjeldus. See annab saajale märku, et fail on saatja poolt teadlikult saadetud.

17.1.5. Vastuvõetava ja välja saadetava e-kirja maksimaalne lubatud suurus on 25 MB. Nimetatud mahust suuremad saabunud e-kirjad saadetakse saatjale tagasi.

17.1.6. Plaanipärase eemal viibimise ajaks tuleb sisse lülitada automaatvastuse funktsiooni (kontorist väljas teade). Vastusteade seadistada nii, et vastusteadet ei saadeta listidesse.

17.1.7. E-posti kasutamisel tuleb olla tähelepanelik ja skeptiline, et mitte langeda pettuste ohvriks.

17.1.8. Keelatud on

17.1.8.1. avada e-postiga saadetud kahtlasi või tundmatuid faile. Kahtluse korral tuleb konsulteerida IT spetsialistiga.

17.1.8.2. edastada AK tunnistatud informatsiooni krüpteerimata kujul või muud eriti tundlikku teavet (kaasa arvatud salasõnad).

17.1.8.3. e-posti aadressi registreerimine tööülesannetega mitteseotud elektronpostiloenditesse või vestlusruumidesse;

17.1.8.4. e-posti ressursse raiskav kasutamine.

- 17.1.9. Kasutaja kasutajaõiguste sulgemisega kaasneb kasutaja e-kirja postkasti sulgemine. Kirju kasutajale edasi ei suunata.
- 17.1.10. Erandkorras taasesitlust võimaldaval kujul esitatud avalduse alusel ja kokkuleppel osakonna juhi ning IT spetsialistiga võib endisele kasutajale saabuva e-posti kuni kolmeks kuuks suunata kasutaja poolt nimetatud e-posti aadressile.

18. Elektronpostiaadresside kuju

- 18.1.1. Kasutaja e-posti aadressi kuju on eesnimi.perenimi@tartukunstikool.ee.
- 18.1.2. Mitme ees- ja perenime korral kasutatakse ainult esimesi nimesid. Kasutaja soovi korral liidetakse või asendatakse teised ametlikud nimed.
- 18.1.3. Liitnimes kasutatakse sidekriipsu sisestamiseks miinusmärki (-). Kui kasutaja ees- või perenimes on täpitähed, siis luuakse aadress, kasutades täpitähtede aluseks olevaid tähti järgmiselt:
- 18.1.3.1. „õ” asendatakse tähega „o”;
- 18.1.3.2. „ä” asendatakse tähega „a”;
- 18.1.3.3. „ö” asendatakse tähega „o”;
- 18.1.3.4. „ü” asendatakse tähega „u”; või vajadusel tähega „y”;
- 18.1.3.5. „ž” asendatakse tähega „z” ning
- 18.1.3.6. „š” asendatakse tähega „s”.
- 18.1.4. Nimetamata erandite kasutamine lepitakse kokku IT spetsialistiga.

19. Sülearvutite kasutamine

- 19.1.1. Sülearvutit on keelatud jätta järelvalveta kohtades, kus sellele võib olla ligipääs kolmandatel isikutel, k.a. sõiduautodesse.
- 19.1.2. Avalikus kohas või kohtades, kus töödeldavaid andmeid võivad näha kõrvalised isikud, ei tohi sülearvutis töödelda AK tunnistatud informatsiooni.
- 19.1.3. Sülearvuti kasutaja vastutab, et töödokumendid on dubleeritud vastavates võrgukataloogides või G-Suite Drive.
- 19.1.4. Vastavalt vajadusele võib TK kehtestada sülearvuti kõvaketta või selle osa krüpteerimise nõude spetsiaalse tarkvara abil.
- 19.1.5. AK tunnistatud informatsiooni tohib sülearvutis hoida ainult krüpteeritult.
- 19.1.6. Külaliste arvuteid ei tohib ühendada ainult “kunstikool” nimelisse Wifi võrku.

20. Riist- ja tarkvara paigaldamine

- 20.1.1. IT vahendeid soetab IT spetsialist ja/või tugistruktuuri juht.
- 20.1.2. TK infosüsteemi ühendatakse IT vahend, mis vastab vähemalt TK-s kehtestatud riist- ja tarkvara miinimumnõuetele.
- 20.1.3. Kui kasutaja vajab oma tööks riist- või tarkvara standardist erinevat IT vahendit, esitatakse vastav taotlus IT spetsialistile.
- 20.1.4. Riist- ja tarkvara ei paigaldata, kui see ei ühildu TK infosüsteemidega või ilmneb oht TK infosüsteemide toimivusele ja turvalisusele.

VII. Lõppsätted

21. Korra rakendamine ja järelvalve

- 21.1.1. Kui kasutaja korrast kinni ei pea, võtab IT spetsialist viivitamatult kasutusele meetmed võimalike TK infosüsteemide turvalekete, volitamata juurdepääsu ja infokao vältimiseks:
- 21.1.1.1. korraldab kasutusõiguste peatamise kuni asjaolude väljaselgitamiseni;
- 21.1.1.2. korraldab TK infosüsteemide turvalisuse kontrolli;
- 21.1.1.3. teavitab juhtkonda võimalikest TK infosüsteemide ründeohtudest ja nende vältimisest;

21.1.2. kasutajatelt, kes korra rikkumisega kahjustavad TK vara või tekitavad lisakulutusi, võib nõuda tekitatud kahju hüvitamist.

21.1.3. Korrast kinnipidamise järelvalvet teostab IT spetsialist.