Kammeri Kooli infosüsteemi kasutamise kord

1. Eesmärk ja reguleerimisala

1.1. Kammeri Kooli infosüsteemi (edaspidi *infosüsteem*) kasutamise korra eesmärk on sätestada infovarade sh kasutajaõiguste, arvutivõrgu, andmekogude ja IT-vahendite kasutamise reeglid.

1.2. Korda rakendatakse Kammeri Kooli (edaspidi Kool) töötajate, õpilaste ja väliste kasutajate suhtes (edaspidi kõik koos ka *kasutaja)*.

2. Kasutajaõiguse haldamine

2.1. Kasutajaõiguse andmisel lähtutakse kasutajate töö- või õppealase vajaduse ja minimaalsete õiguste põhimõttest. Installeerimise õigusi omavad ainult domeeni administraatorid.

2.2. Kasutajaõiguse andmisel asutuse välisele kasutajale (edaspidi *väline kasutaja*) lähtutakse punkt 3 lõikes 10 toodud nõuetest.

2.3. Igal infosüsteemi kasutajal on autentimiseks personaalne kasutajanimi ja parool, mida ei tohi edastada teistele isikutele.

2.4. Töötajale annab infosüsteemi ja andmekogude õigusi koolijuht. Töölt lahkudes lõpevad töötajal juurdepääsuõigused.

2.5. Õpilastele kehtivad pääsuõigused ainult arvutiklassis arvutites ja tahvelarvutites.

3. Kasutajakonto loomine, haldamine ja kustutamine

3.1. Arvutivõrgu (domeeni) kasutajakonto ja personaalne e-posti aadress luuakse töötajale pärast tööle võtmist ja õpilasele pärast Kooli nimekirja arvamist. Konto loob Kooli vastavate õigustega töötaja või IT-juht.

3.2. Arvutivõrgu kasutajakonto annab õiguse kasutada personaalset ja jagatud võrguressurssi ning e-posti süsteemi vastavalt töö- või õppealasele vajadusele.

3.3. Esmakordsel sisselogimisel peab kasutaja kasutajakonto parooli koheselt ära muutma ainult enda teada olevaks parooliks.

3.4. Lepinguliste ülesannete täitmiseks lühikeseks ajaperioodiks (praktika, projektipõhine töö jne) tehakse isikule ajutine tööalane kasutajakonto.

3.5. Õpilase või töötaja nimekirjast välja arvamisel infosüsteemi kasutajaõigus lukustatakse. Konto ja sellega seotud andmed kustutatakse asutuse vastavate õigustega töötaja või IT-toe poolt.

3.6. Töösuhte peatumisel pikemaks kui 60 päeva töötaja kasutajakonto ja juurdepääsuõigused infosüsteemile lukustatakse asutuse juhi korraldusel, mis edastatakse e-posti teel IT-toele. Juurdepääsuõiguse lukustusest teavitatakse konto kasutajat.

3.7. Töötaja peab enne töösuhte lõppemist kustutama oma postkastist, võrgukettalt ja arvuti andmekandjalt mittetööalased ning ebaolulise sisuga e-kirjad ja failid.

3.8. Töösuhte lõppemisel kasutajaõigused ja personaalne postkast suletakse ning saabuvat e-posti edasi ei suunata.

3.9. Kõik varukoopiatele salvestatud töötaja postkastis olevad kirjad ja võrgukettal olevad failid arhiveeritakse.

3.10. Välistele kasutajatele antakse infosüsteemi kasutajaõigused ainult kokkuleppel asutuse juhiga.
3.11. Arvutiklassis toimuvatele üritustele (olümpiaadid, nutivõistlused jms), milles osalevad teiste koolide õpilased antakse ajutine ligipääs.
3.12. Kasutajakonto loomisega Domeeni (Active Directory) tekib kasutajal ligipääs järgnevatele teenustele:
    3.12.1. failihaldusteenus;
    3.12.2. printimisteenus;
    3.12.3. e-posti teenus;
    3.12.4. arvuti töökohateenus;
    3.12.5. kohtvõrgu teenus.

4. Kasutajakonto omaniku õigused

4.1. Kasutajal on õigus:
    4.1.1. omada juurdepääsu talle tööülesannete täitmiseks vajalikule teabele ja teenustele kokku lepitud tööajal;
    4.1.2. saada mõistliku aja jooksul infot planeeritud muudatustest ja häiretest süsteemides ning arvutivõrgus;
    4.1.3. pöörduda infotehnoloogiaalase abi saamiseks IT-toe poole punktis 16 kirjeldatud viisil.

5. Kasutajakonto omaniku kohustused

5.1. Kasutaja on kohustatud:
    5.1.1. kasutama võrguressursse optimaalselt ning mitte koormama arvutivõrku mittetööalaste tegevustega;
    5.1.2. regulaarselt korrastama personaalset e-posti ja failiserveris asuvaid andmeid, kustutades ebaolulise sisuga kirjad ja failid. Pidama kinni infosüsteemis kehtestatud mahupiirangutest;
    5.1.3. riist- ja tarkvara lisamiseks, ümberpaigutamiseks, häälestamiseks ja eemaldamiseks pöörduma IT-toe poole abi@atrauma.ee;
    5.1.4. mitte ühendama asutuse sisevõrku asutusele mittekuuluvat riistvara;
    5.1.5. arvuti juurest lahkudes välja logima, lukustama ja arvuti sulgema koolipäeva lõpus;
    5.1.6. hoidma enda teada paroolid. Kui parool on saanud teatavaks kõrvalistele isikutele või on kahtlus, et see on võinud juhtuda, on kasutaja kohustatud parooli koheselt muutma või laskma selle IT-toe kaudu konto lukustada.

6. Paroolinõuded

6.1. Esmaselt väljastatud parool on ühekordne (kui vastava infosüsteemi või andmekogu kasutusjuhendis ei ole märgitud teisiti) ning kasutaja kohustub selle vahetama esimesel sisselogimisel ainult temale teadaoleva parooli vastu.
6.2. Parool peab koosnema suur- ja väiketähtede ning numbrite kombinatsioonist. Soovitav on lisaks kasutada kirjavahemärke. Parooli pikkus peab olema vähemalt 10 sümbolit.

Parool ei tohi olla kergesti aimatav (näiteks nimed, auto numbrimärgid, sünnikuupäevad) ega sisaldama täpitähti.

6.3. Maksimaalne parooli kehtivusaeg asutuse infosüsteemis on 90 päeva.

6.4. Parooli vahetamisel peab infosüsteem meeles viis viimast parooli.

6.5. Viiekordsel vale parooli sisestamisel konto lukustatakse. Konto avab asutuse vastavate õigustega töötaja või IT-tugi.

7. Failihalduse teenus

7.1. Iga kasutaja jaoks võib vajadusel eraldada personaalse võrguketta ja mahu serveris, millele ligipääs on vaid kasutajal endal.

7.2. Töötajale juurdepääsu andmine jagatud võrguketastele toimub kasutajakonto loomisel.

7.3. Töötaja peab hoidma tööalaseid faile failiserveri võrguketastel. Varundamine tagatakse vaid töökaustadele ja võrguketastel olevatele failidele.

7.4. Kasutaja peab vältima suuremahulise info salvestamist Töölauale.

7.5. Isiklikke faile ei tohi hoida töökaustades.

7.6. Suuremahuliste failide jagamiseks võib kasutada ainult asutuse hallatavat pilveteenust.

8. Printimisteenus

8.1. Õppetööd toetavate materjalide printimine koolis on tasuta.

8.2. Isiklikul otstarbel printimine ei ole koolis lubatud.

8.3. Konfidentsiaalse informatsiooni printimisel või paljundamisel tuleb väljaprinditud/paljundatud materjal koheselt pärast printimist printerist eemaldada.

8.4. Leides printerisse või koopiamasinasse unustatud konfidentsiaalse materjali tuleb see kas omanikule koheselt ära viia (kui on teada) või hävitada paberipurustajat kasutades.

9. E-posti teenus

9.1. Kõigil on ühtne IT-toe hallatav e-postisüsteem domeeninimega kammerikool.ee.

9.2. E-posti süsteemi võib kasutada nii veebipõhiselt kui arvutisse paigaldatud e-posti tarkvaraga järgides infoturbenõudeid.

9.3. Igal töötajal on personaalne e-posti konto kujul eesnimi.perenimi@kammerikool.ee koos e-postiga võimalik kasutada kalendrite ja pilveketta teenust. Samanimeliste kasutajate korral lisatakse kasutajaga kokkuleppel perenimele number.

9.4. E-posti konto võib olla asutusel või kindla funktsiooni täitmiseks. Igal e-posti kontol on vastutav kasutaja. Kasutaja hoolitseb ise postkasti korrashoiu eest (kustutab järjepidevalt ebavajaliku info).

9.5. Asutusesisese töö korraldamiseks võib IT-tugi luua aadresside liste.

9.6. E-posti kontol on mahupiirang 50 GB. Iga e-posti aadressi omanik on kohustatud jälgima, et postkastis oleks käideldavuse tagamiseks piisav mahu varu.

9.7. Kasutajal on keelatud avada kahtlusi tekitava pealkirjaga, sisuga või kahtlustäratavalt aadressilt saabuvaid kirju ning käivitada neis olevaid hüperlinke ja manuseid.

9.8. Keelatud on asutuse e-posti aadressi kasutamine isiklikul otstarbel, tarbijamängude mängimiseks, isiklike kommertsteadete tellimiseks, mitte tööalaste foorumite kasutamiseks

ning muudeks tegevusteks, mis võivad põhjustada hulgalise kommertsteadete ja rämpsposti saatmise.

9.9. Kasutaja ei tohi suunata asutuse e-posti automaatselt edasi asutusevälistele aadressidele. Käsitsi edastamisel tuleb jälgida konfidentsiaalsusnõudeid.

9.10. Dokumentide edastamisel tuleb eelistada *pdf*-vormingut.

9.11. Tööalast informatsiooni võib edastada ainult asutuse e-posti süsteemi kaudu.

9.12. Konfidentsiaalse info saatmisel väljapoole asutust tuleb see krüpteerida.

9.13. Suuremahuliste failide saatmist e-posti manusena tuleb vältida. E-kirja maht ei tohi ületada 150 MB. Suure mahuga infot saab edastada asutuse pilveteenuse kaudu.

10. Interneti kasutamine

10.1. Interneti kasutamisega seotud andmed logitakse.

10.2. Kasutajal on keelatud asutuse seadmesse laadida omavoliliselt (ilma IT-toe loata) alla tarkvara ja tarkvarauuendusi, mänge, filme jms.

10.3. Töötajal on internetis uudiseportaalide ning elektroonilise ajakirjanduse uudiste või artiklite kommenteerimine lubatud üksnes juhul, kui ta teeb seda oma nime alt oma töövaldkonna kohta ning kooskõlastab selle eelnevalt vahetu juhiga.

11. Wifi kasutamine

11.1. Asutuses on kolm wifi leviala:

11.1.1. õpetajate võrk nimega: kammeri (juhtkond ja õpetajad);

11.1.2. sisevõrk nimega: kammeri-sise (ligipääsu saavad kooli arvutid);

11.1.3. vaba võrk nimega: kammeri-kylaline (ligipääs lubatud kooli külalistele).

12. Andmekandjate kasutamine

12.1. Eemaldatavate andmekandjate kasutamine on kõrgendatud ohu allikas. Neid on lihtne kaotada, varastada, need võivad rikneda ja neid võidakse kasutada arvuti pahavaraga nakatamiseks.

12.2. Infosüsteemis tohib kasutada vaid IT-toe poolt lubatud digitaalseid andmekandjaid.

12.3. Konfidentsiaalse informatsiooni salvestamine eemaldatavale digitaalsele andmekandjale on lubatud ainult tööülesannete täitmiseks ja äärmisel vajadusel kokkuleppel tööandjaga.

12.4. Konfidentsiaalset informatsiooni sisaldava andmekandja kadumisest või vargusest tuleb koheselt teavitada tööandjat.

12.5. Kasutusest eemaldatud digitaalsetel andmekandjatel oleva info hävitamise korraldab IT-tugi.

13. Arvutite kasutamine

13.1. Arvutites kasutatav tarkvara on: süsteemitarkvara, baastarkvara, standardtarkvara, lisatarkvara.

13.2. Arvutil on üldjuhul üks vastutav kasutaja.

13.3. Töötaja peab olema tutvunud kooli infoturbe põhimõtteid jt infotehnoloogiat ja infoturvet reguleerivate õigusaktidega.

13.4. Automaatse ekraaniluku rakendumine on kohustuslik ja seadistatakse IT-toe poolt.
13.5. Arvuti kasutaja kohustub:
  13.5.1. kaugtööl järgima asutuse infosüsteemide kasutamise korda ja töökorralduse reegleid;
  13.5.2. hoidma sülearvutit avalikes kohtades isikliku järelevalve all;
  13.5.3. mitte laskma sülearvutit külmuda ega üle kuumeneda (otsese päikesekiirguse käes);
  13.5.4. sülearvuti või muu IT-vahendi vargusest või kaotamisest koheselt teavitama IT-tuge;
  13.5.5. ühiskasutuses oleva arvuti puhul töö lõpetades välja logima.
13.6. Konfidentsiaalse info töötlemisel kasutaja kohustub:
  13.6.1. veenduma, et arvutiekraanil toimuv ei ole teistele isikutele nähtav;
  13.6.2. sisestama kasutajatunnused nii, et teised isikud ei näeks mida sisestati;
  13.6.3. mitte kasutama sülearvutit avalikus võrgus kui on kahtlus, et arvuti turvaseaded (tulemüür, viirusetõrje, VPN) ei ole töökorras ning arvestama, et väljaspool asutuse sisevõrku võidakse ühendust pealt kuulata;
  13.6.4. viirusekahtlusega arvuti koheselt eemaldama arvutivõrgust, selle sulgema ning teatama IT-toele.
13.7. Asutusesisestele võrguressurssidele saab välisvõrgust ligi ainult läbi turvakanali, mille seadistab IT-tugi.
13.8. Asutusesiseseks kasutamiseks või delikaatseid isikuandmeid sisaldava info töötlemiseks kasutatava sülearvuti kõvaketas peab olema krüpteeritud.

14. Nutiseadmete kasutamine

14.1. Tööülesannete täitmisel on lubatud kasutada ainult turvatud ja aktsepteeritud nutiseadmeid (edaspidi *nutiseade* või *nutitelefo*n).
14.2. Töötajate nutiseadmed peavad olema kaitstud ekraanilukuga. Ekraanilukk peab rakenduma automaatselt. Mustrikombinatsioon ei ole piisav kaitse ja seda võib kasutada ainult koos PIN-koodiga.
14.3. Asutusesiseseks kasutamiseks või delikaatseid isikuandmeid sisaldavat infot ei ole lubatud nutiseadmes töödelda ega kasutada nutiseadet konfidentsiaalse info andmekandjana.
14.4. Asutuse nutitelefoni ei või kasutamiseks edasi anda teistele isikutele. Nutiseadme kaotamise või varastamise korral on kasutaja kohustatud koheselt teavitama IT-tuge.
14.5. Õppetöös kasutatavaid nutiseadmeid ei tohi siduda kasutajate isiklike kontodega.

15. Krüpteerimine

15.1. Isikuandmeid või konfidentsiaalset infot sisaldavaid dokumente asutusest välja saates peavad need olema krüpteeritud. Krüpteerimiseks kasutatakse ID-kaardi lahendust.
15.2. ID-kaardi lahendusega krüpteeritud dokumendid tuleb säilitamiseks lahti krüpteerida.

16. Kasutajatoe teenus

16.1. IT-vahendite hankimist korraldab IT-tugi ja nende üle peetakse arvestust IT-toe poolt.

16.2. IT-vahendid annab kasutajale või vastutavale kasutajale üle IT-tugi ja töösuhte või vajaduse lõppemisel võtab tagasi IT-tugi.
16.3. Kasutaja on kohustatud esimesel võimalusel teavitama IT-tuge infotehnoloogiliste teenuste kasutamist takistavatest juhtumitest, võimalikest ohtudest ja infoturbeintsidentidest. Juhtumitest teatada:
    16.3.1. e-posti aadressil: abi@atrauma.ee
    16.3.2. telefoni teel: 54558600
16.4. IT-toele saabunud juhtumid registreeritakse.
16.5. Juhtumi kiireks lahendamiseks on soovitav edastada vähemalt järgmine info:
    16.5.1. tõrkega seotud seadme number, nimetus, asukoht;
    16.5.2. kasutaja nimi;
    16.5.3. probleemi kirjeldus;
    16.5.4. mida on eelnevalt tehtud juhtumi lahendamiseks.
16.6. Arvutihooldustöödeks või kasutaja abistamiseks võib IT-tugi asutuse seadmetes kasutada kaughaldustarkvara võttes üle seadme pildi ja juhtimise ilma kasutaja aktseptita.