Kehtna Kutsehariduskeskuse arvutivõrgu ja arvutite kasutamise eeskiri

Sisukord

1. Üldpõhimõtted ja mõisted

Kehtna Kutsehariduskeskuse arvutivõrgu ja arvutite kasutamise eeskiri (edaspidi: *eeskiri*) reguleerib Kehtna Kutsehariduskeskuse (edaspidi: *kool*) arvutite ja arvutivõrgu kasutamist, kasutajate õigusi, kohustusi ja vastutust.

Kehtna Kutsehariduskeskuse arvutid ja arvutivõrk (edaspidi: *arvutivõrk*) on digitaalseadmete kompleks, mis koosneb kasutaja sisend- ja väljundseadmetest (monitor, klaviatuur, hiir, printer jm seadmed), arvutitest (PC, sülearvuti, tahvel vms), võrgust (kaabeldus- ja võrguseadmed), serveritest ning võrgu välisühendusest.

Arvutivõrgu kasutaja on Kehtna Kutsehariduskeskuse töötaja, kes kasutab mõnda Kehtna Kutsehariduskeskuse arvutit või muud Kehtna Kutsehariduskeskuse arvutivõrku ühendatud seadet. Kasutaja peab omama elementaarseid oskusi arvuti kasutamiseks. Kasutaja on kohustatud teadma ning järgima käesolevas eeskirjas toodud reegleid ning ta annab juhendiga tutvumise kohta allkirja.

Arvutivõrgu kasutamine on:

1) serveriressursside, võrguressursside ja interneti kasutamine;
2) tööks erinevate infosüsteemide kasutamine (Tahvel, EKIS, EHIS, RTIP, Moodle jne...);
3) elektronposti kasutamine;
4) interneti kasutamine.

2. Arvutivõrgu kasutusõiguse saamise kord

Arvutivõrgu kasutusõigus ehk personaalne kasutajakonto antakse kooli töötajatele oma tööülesannete täitmiseks, kes saab vajadusel saab koolituse vahetult juhilt või haridustehnoloogilt. Kasutajakontol puuduvad administraatori õigused. Kooli arvutivõrgu kasutamise õigus on personaalne ning seda pole lubatud teistele isikutele edasi anda. Arvutivõrgu kasutusõigus kehtib kasutajale kogu koolis töötamise aja. Kasutusõiguse andmisel tutvustatakse kasutajale arvutivõrgu kasutamist puudutavaid kordi, mille töötaja kinnitab oma digiallkirjaga. Töösuhte lõppemisel kasutajakonto üldjuhul suletakse või suunatakse ümber.

3. Riist- ja tarkvara kasutamise üldnõuded

Arvuti koos tarkvaraga on kooli omand või kooli poolt liisitav vara, mis antakse kasutajale kasutamiseks tema tööülesannete täitmiseks. Kasutaja peab tema kasutusse antud arvutiga ümber käima säästlikult ja heaperemehelikult ning teistele kasutajatele ei tohi tekitada asjatuid takistusi ega ebameeldivusi. Võrgu kasutamisel tuleb austada privaatsust ja tagada turvalisus.

Arvutivõrgus ja arvutis võib kasutada ainult litsentseeritud ja registreeritud tarkvara. Tööks vajaliku tarkvara paigaldab IT-spetsialist. Tarkvara ja operatsioonisüsteemi uuendused ja turvaaukude parandused paigaldatakse automaatselt. Arvutis võib kasutada vaid eelnevalt kontrollitud ja viirusvabu andmekandjaid. Viiruse avastamisel tuleb sellest teatada IT-spetsialistile.

Arvutites ja muudes infotehnoloogilistes seadmetes ning arvutivõrgu kasutajale ligipääsetavates infosüsteemides hoitakse ainult tööülesannetega seotud andmeid.

Arvuti juurest lahkumisel lühikeseks ajaks tuleb arvuti ekraan lukustada (Windows + L). Pikemaks ajaks lahkumisel tuleb arvutist välja logida, tööpäeva lõpus arvuti sulgeda.

Arvutivõrku ühendatud seadmeid paigutab ümber IT-spetsialist.

Töölt lahkumise korral annab kasutaja üle töökohaarvutis tööülesannete täitmisega seotud failid vahetule juhile. Nimetatud failide kustutamine, muutmine või hävitamine töölt lahkudes on keelatud.

Arvutivõrgu tööd koordineerib IT-spetsialist, kelle pädevus tuleneb ametijuhendist ja käesolevast eeskirjast.

4. Elektronposti kasutamine

Igale kasutajale antakse koos arvutivõrgu kasutamisõigusega elektronposti (edaspidi: *e-post*) aadress kujul eesnimi.perekonnanimi@kehtna.edu.ee. Kooli e-posti aadress on ette nähtud tööalaseks suhtluseks. Personaalse kirjavahetuse jaoks tuleb kasutada personaalset e-posti aadressi. Keelatud on tööalase e-posti suunamine üks kõik millisele mitte kooliga (@kehtna.edu.ee) seotud aadressile.

Enne kirjade saatmist tuleb veenduda, et kirja adressaat on õige, kirjale on märgitud asjakohane teemarida ning kiri ei sisalda liigset informatsiooni. Saates kirja mitmele tööalasele kontaktile korraga, kirjutatakse see kellelt vastust ootate kirja saaja ehk adressaat reale ning teised e-posti aadressid kirjutatakse koopia reale. Saates kirja mitmele eraisikule korraga, kirjutatakse nende e-posti aadressid pimekoopia/salakoopia reale. Kirjade saatmisel Kehtna Kutsehariduskeskusest väljapoole tuleb kontrollida, et kiri ei sisaldaks asutusesisest infot. Konfidentsiaalseid andmeid (sealhulgas isikuandmeid) sisaldavad kirjad tuleb krüpteerida RIA DigiDoc programmiga nii, et ainult adressaat saab kirja avada.

Kasutajal on keelatud avada kahtlusi tekitava pealkirjaga või kahtlustäratavalt elektronposti aadressilt saabuvat elektronkirja ning käivitada elektronkirjade manuses olevaid programme või skripte.

Kirjakasti saabuvaid kirju kontrollitakse automaatselt viirusetõrjevahenditega. Lisaks võib asutus kirjakasti saabuvaid kirju vajadusel kontrollida ning kasutada vastavalt seadusele.

Kasutaja töölt lahkumise korral rakendatakse kasutaja e-posti aadressile saabuvatele kirjadele kahe kuu jooksul automaatvastust teavitusega konto sulgemise kohta ja viidetega asutuse üldisele e-posti aadressile. Seejärel e-posti konto suletakse või suunatakse ümber.

5. Parooli kasutamine

Kasutajakonto parool peab koosnema vähemalt 9 märgist, sisaldama suurtähti, väiketähti ja numbreid. Süsteem kontrollib nende keerukusnõuete täitmist ning ei luba sisestada lihtsamat parooli. Parooli tuleb iga 180 päeva järel vahetada

Parool ei tohi olla seostatav millegagi, mis võib kolmandatele isikutele kasutaja kohta teada olla. Sealjuures ei tohi kasutada paroolina oma nime või ettevõtte nime või juba kasutatud viimasele 24'le paroolile sarnast parooli.

Kahtluse korral, et parool on lekkinud (näiteks keegi on jälginud parooli sisestamist), tuleb parool viivitamatut vahetada ja teavitada juhtunust IT spetsialisti.

6. ID-kaardi kasutamine

Digitaalseks isikutuvastamiseks elektroonilises keskkonnas peab kasutama ID-kaarti, Smart-ID, Mobiil-ID või digi-IDd (edaspidi: *ID kaart*). Pärast infosüsteemi kasutamise lõppu tuleb veebilehitseja sulgeda ja arvuti juurest lahkudes ID-kaart kaardilugejast eemaldada.

Kahtluse korral, et ID-kaardi PIN koodid on lekkinud (näiteks keegi on jälginud PIN koodide sisestamist), tuleb PIN koodid viivitamatult vahetada või kui see ei ole võimalik, siis teavitada ID-kaardi abiliini telefonil 1777. Samuti tuleb toimida juhul kui ID-kaart on kadunud või varastatud ning kaardi kasutamine tuleb blokeerida.

7. Andmekogude kasutamine

Töötajatele võimaldatakse juurdepääs andmekogu sellele osale, mis on sätestatud tööülesannetega. Andmekogus oleva info kasutamisel tuleb lähtuda avaliku teabe seadusest.

8. Piirangud arvutivõrgus

Kasutajal on keelatud:

1) arvutivõrgu kasutamine viisil, mis häirib süsteemide kasutust nende haldaja poolt määratud otstarbel või põhjustab häireid arvutivõrgus;
2) igasugune tarkvara omavoliline installeerimine ja kustutamine arvutites IT-spetsialisti nõusolekuta;
3) tööülesannete täitmisega mitteseotud programmide ja andmete salvestamine ning hoidmine kooli arvutisüsteemides;
4) hoida ja asutuse arvutivõrgus levitada illegaalselt omandatud tarkvara ning üldtunnustatud moraalinõuetega vastuolus olevaid materjale;
5) seadmete füüsiline avamine ja ühenduskaablite ümberühendamine, arvutite omavoliline ühendamine arvutivõrku ja võrguaadressi muutmine;
6) kõrvalistel isikutel arvuti kasutamise lubamine, välja arvatud juhul kui tegu on koolis üldkasutatava arvutiga (nt. klassi- või avaliku interneti punkti arvuti). Kasutaja vastutab personaalselt tema arvutis tehtud toimingute eest. Seejuures on kõrvaline isik ka teine koolikontot omav töötaja või õpilane!

9. Kasutajate õigused

Kasutusõiguse saanud isikul on õigus kasutada arvutivõrku tööajal; pärast tööd ja puhkepäevadel vahetu juhi loal, kui see ei ole vastuolus muude eeskirjadega. Kasutajal on õigus saada IT-spetsialistilt infot kõigist muudatustest ja sündmustest süsteemides ja arvutivõrgus, mis oluliselt mõjutavad nende kasutamist või rikuvad kasutaja privaatsust.

Kasutajal on õigus teha IT-spetsialistile ettepanekuid arvutisüsteemide töö ja teenuste paremaks korraldamiseks. Kui kasutajal on pretensioone IT-spetsialisti suhtes, saab ta need esitada IT-spetsialisti vahetule juhile.

10. Kasutajate kohustused

Kasutaja on kohustatud kaasa aitama arvutisüsteemide turvalisuse tagamisele. Selleks peab ta:

1) hoidma saladuses kasutusõigusi tagavaid paroole;
2) mitte lubama teistel isikutel kasutada oma kasutajatunnust;
3) mitte kasutama teistele isikutele omistatud kasutajatunnuseid;
4) kahtluse tekkimisel kasutajatunnuse salajaste osade (paroolid, sertifikaatide salajased võtmed jms) avalikustamisest koheselt teavitama IT-spetsialisti ja muutma kasutajatunnuseid;
5) järgima IT-spetsialisti poolt kehtestatud piiranguid.

11. IT-spetsialisti õigused

IT-spetsialistil on oma kohustuste täitmiseks õigus ajutiselt piirata arvutisüsteemide ja -võrgu kasutamist. Kõigist sellistest piirangutest peab IT-spetsialist kasutajaid teavitama. Arvutisüsteemi või -võrgu häireolukorra kiireks selgitamiseks ja parandamiseks on IT-spetsialistil õigus kontrollida kasutajate tööd ja avada kasutajate faile. Selleks on IT-spetsialistil kooli arvutites administraatori õigustega konto, ning sellisel viisil teatavaks saanud info on ametialane ja ei kuulu avalikustamisele. IT-spetsialisti tavakonto on tavaõigustega nagu iga teine kasutajakonto koolis.

12. IT-spetsialisti kohustused

IT-spetsialisti kohustused on järgmised:

1) tagab arvutivõrgu ja arvutisüsteemide normaalse toimimise ja teenuste kättesaadavuse oma ametijuhendis sätestatud tööülesannete ulatuses;
2) jälgib oma hoolduses olevate süsteemide töökorras olekut ja turvalisust, probleemide avastamisel annab neist võimaluse korral kasutajatele teada;
3) kontrollib arvutivõrgu aktiivseadmete korrasolekut ja kaitseb neid igakülgselt kahjustuste eest;
4) annab eelteavet kasutajatele olulisematest muudatustest arvutisüsteemides ja –võrkudes;
5) teavitab sündmustest, mis rikuvad kasutajate privaatsust;
6) peab saladuses andmeid, mis ta on saanud seoses oma töökohustuste täitmisega ja mille kohta tal puudub nende andmete omaniku luba seda levitada, v.a. juhud, kus seadus kohustab info teatavaks tegema;
7) vastutab kvaliteetsete ja andmete taastamist võimaldavate varukoopiate tegemise eest;
8) tagab arvutites toimiva viirusetõrjetarkvara;
9) korraldab arvutite administreerimist ja vajaliku standard- ja spetsiaaltarkvara installeerimist;
10) kontrollib, et arvutites ei oleks tööks mittevajalikku tarkvara. Selle esinemisel teavitab kasutajat selle olemasolust ja vajadusel kõrvaldab tarkvara.

13. Arvutivõrgu või infosüsteemide väärkasutuse tagajärjed

Kui on tekkinud kahtlus, et arvutivõrgu ja infosüsteemide kasutamise reegleid on rikutud, võtab IT-spetsialist ühendust kasutajaga ja selgitab välja, millega on tegemist. IT-spetsialist võib peatada tema arvutivõrgu kasutusõiguse kuni asjaolude selgitamiseni. Reeglite rikkumises kahtlustataval on õigus esitada omapoolne selgitus.

Vältimatu vajaduse korral on IT-spetsialistil õigus peatada, takistada või piirata arvutivõrgu ja infosüsteemi(de) kasutamist väärkasutuse uurimise ajaks. Kui osutub, et rikkumine toimus infosüsteemi(de) mitteküllaldase tundmise tõttu, annab IT-spetsialist juhtnööre edasise tegevuse jätkamiseks.

Kasutajad, kes arvutivõrgu ja arvuti kasutamise reeglite rikkumisega kahjustavad Kooli vara või tekitavad lisakulutusi, hüvitavad tekitatud kahju Kehtna Kutsehariduskeskusele poolte kokkuleppel. Kokkuleppe mittesaavutamisel toimub hüvituse sissenõudmine seadusega ettenähtud korras.

14. Infoturbe intsidendid

Infoturbe intsidendid on sellised sündmused, mille tagajärjel võib tekkida kahju ning mille õigel lahendamisel saab sellist kahju ära hoida või vähendada. Suur kahju on näiteks kooli töövõime häirimine, andmete rikkumine ning andmete leke.

Turvaintsidentide edukaks lahendamiseks peavad kasutajad neid avastama ning nendest IT-spetsialistile teada andma. Turvaintsidendid on näiteks:

1) kasutaja vale käitumine, mille tagajärjeks on andmete kadu;
2) turvaaukude esinemine riist- või tarkvarakomponentides;
3) kooli sissemurdmine, arvutite või andmekandjate vargus;
4) infosüsteemidesse sissemurdmine ning volitamata juurdepääs andmetele;
5) viirus;
6) parooli, ID-kaardi või Smart-ID PIN koodide lekkimine;
7) konfidentsiaalsete andmete avalikustamine;
8) võõraste inimeste lubamine kohtadesse kus nad ei tohi viibida, nt. serveriruum, arhiiv jne.

Turvaintsidendi avastamisel tuleb käituda nii:

1) säilitada rahu ning vältida abimeetmete rakendamisel liigset kiirustamist;
2) teavitada intsidendist direktorit ja IT-spetsialisti ning järgida nende juhiseid;
3) kui inimeste elu või tervis on ohus siis teavitada lähtuvalt koolis kehtestatud juhistele.