Valgamaa Kutseõppekeskuse infosüsteemide ja arvutikasutaja reeglistik

1. Eesmärk

1.1 Käesolev arvutikasutaja eeskiri on osa Valgamaa Kutseõppekeskuse (edaspidi "VKÕK") infoturbe korraldusest. Arvutikasutaja reeglistik kehtestab elementaarsed sätted, mis aitavad vähendada VKÕK infosüsteemi halduskulusid ning tõhustavad selle turvalisust ja efektiivsust.

1.2 Antud reeglistiku eesmärgiks on tekitada organisatsioonisisene turvateadlikkus ning saavutada infosüsteemi kasutajate ja haldajate individuaalset vastutust ja aktiivset osalust turvalisuse tagamisel.

1.3 VKÕK pühendub kõrgeima taseme infoturbe tagamisele ja isikuandmete kaitsmisele oma õpilaste, töötajate ja partnerite suhtes. Infoturbepoliitika eesmärk on tagada tundlike ja konfidentsiaalsete andmete, infosüsteemide ja digitaalsete ressursside terviklikkus, konfidentsiaalsus ja kättesaadavus.

1.4 Infoturbe tagamine on iga VKÕK töötaja ja õpilase ühine vastutus. Iga töötaja ja õpilane peab järgima infoturbereegleid ja -protseduure.

2. Üldsätted

2.1. VKÕK infosüsteem - VKÕK mitteavalik teave, arvutid ja nendega seonduvad tarkvara ning seadmed, arvutivõrk ja selle komponendid ning ressursid (kaasa arvatud Interneti ühendus) - on VKÕK omand, mille kasutamisel tuleb alati lähtuda eelkõige VKÕK huvidest.

2.2. VKÕK infosüsteemi kasutamisel tuleb juhinduda:

2.2.1. seadustest;

2.2.2. VKÕK tegutsemise eesmärkidest, mis on määratud VKÕK põhikirjaga;

2.2.3. antud reeglistikust;

2.2.4. headest tavadest (kaaskasutajatele ei tohi tekitada asjatut tüli, tuleb austada privaatsust, tuleb tagada tundlike andmete kaitse).

2.3. Antud reeglistik sätestab infosüsteemi kasutajate ja haldajate õigused ning kohustused.

2.4. Antud reeglistik kehtib kõigis VKÕK infosüsteemi lülitatud arvutisüsteemides (k.a. kaasaskantavates arvutites).

2.5. VKÕK infosüsteemi ning sellega seonduvate ruumide haldajad võivad ülaltoodud põhimõtetest ja seadmete sihtotstarbest lähtuvalt kehtestada täiendavaid reegleid, mis ei vähenda käesoleva reeglistiku nõudeid.

2.6. Kui VKÕK infosüsteemi erinevad kasutusviisid satuvad konflikti, mille lahendamisel ei saa ühtselt lähtuda antud reeglistikust ega täiendavatest reeglistikest, tuleb lähtuda järgnevatest prioriteetidest:

2.6.1. VKÕK põhitegevusega seotud tegevused;

2.6.2. muud VKÕK tegevuse eesmärkidega otseselt seotud tegevused;

2.6.3. VKÕK tegevuse eesmärkidega kaudselt seotud tegevused;

2.6.4. muud tegevused, mis ei häiri teiste infosüsteemi tööd.

2.7. Asutuse infosüsteemi vahendusel kogutud andmed, sh e-kirjad, ja loodud spetsiaalrakendused on asutuse omand.

2.8. VKÕK infosüsteemi haldajaks on IT-spetsialist.

2.9 Infosüsteemi turvalisuse tagamise eest vastutab VKÕK IT-spetsialist ja IT-teenuste pakkujad, kellele (või tema poolt määratud kontaktisikule) tuleb teavitada kõikidest turvaintsidentidest. VKÕK IT-spetsialist vastutab infoturbepoliitika elluviimise eest ja peab jälgima, et see vastaks kehtivatele regulatsioonidele.

2.10 Infosüsteemi kasutamise ja turvalisusega seonduvate intsidentide puhul tuleb pöörduda VKÕK tugipersonali poole telefonil: 766 8575 või aadressil: admin@vkok.ee.

2.11 VKÕK andmekaitsespetsialist on kantseleijuhataja, intsidentide puhul tuleb pöörduda: 766 8575, ivita.ersto@vkok.ee.

2.12 VKÕK õppeinfosüsteem on TAHVEL. TAHVEL on isikuandmete volitatud töötleja ja kooli kontaktisik on IT-spetsialist.

2.13 VKÕK õppekeskkond koosneb järgmistest platvormidest: Moodle, Schoolaby ja Opiq.

2.13.1 OPIQ on isikuandmete volitatud töötleja ja kooli kontaktisik on kaugõppe logistik.

2.13.2 Moodle on samuti isikuandmete volitatud töötleja. Moodle kooli kontaktisikud ja haldurid on haridustehnoloog ja kaugõppe logistik.

2.13.3 Schoolaby on samuti isikuandmete volitatud töötleja, ja kooli kontaktisik on haridustehnoloog.

3. Kasutaja kohustused

3.1. Kasutaja on kohustatud täitma oma rolli infosüsteemi turvalisuse tagamises. Selleks peab ta:

3.1.1. Hoidma saladuses kasutusõigusi tagavaid paroole vastavalt VKÕK paroolide hoidmise nõuetele (vt. 8.3);

3.1.2. Mitte võimaldama või lubama teistel isikutel kasutada oma kasutajaõigusi;

3.1.3. Vältima oma valduses olevate andmete ja informatsiooni lekkimist kõrvalistele isikutele;

3.1.4. Teavitama vastutavat personali kõikidest infosüsteemi tõrgetest ja turvaintsidentidest.

3.2. Kasutajad on kohustatud järgima infosüsteemi haldajate poolt kehtestatud piiranguid ja täitma haldajate poolt tehtud korraldusi.

3.3. Keelatud on kasutada teistele isikutele omistatud kasutajaõigusi (näiteks e-maili või kasutajakontot).

3.4. Keelatud on infosüsteemi tööd häiriv tegevus, mis häirib selle tööd või kasutust haldaja poolt määratud otstarbel või segab teisi kasutajaid nii otseselt kui ka kaudselt (näiteks ressursside tahtliku raiskamise teel või emaili masspostitusega selleks konkreetset soovi mitte avaldanud isikutele).

3.5. VKÕK infosüsteemi ja selle kasutusõigust ei tohi kasutada isikliku või muu tulu saamise eesmärgil, mis ei lähtu VKÕK põhikirjalisest tegevusest. VKÕK infosüsteemi maksuliseks kasutamiseks sõlmitakse vajadusel eraldi leping.

3.6. Arvutivõrku ühendatud arvutites on rangelt keelatud hoida, kasutada ja VKÕK arvutivõrgus levitada:

3.6.1. Illegaalselt omandatud või litsentseerimata tarkvara;

3.6.2. Autorikaitse alla kuuluvat tarkvara või andmefaile vms, millede kohta ei ole ostu tõendit;

3.6.3. Sündsusetu sisuga faile.

3.7. Rangelt on keelatud mistahes tarkvara (litsentseeritud või litsentseerimata) omavoliline paigaldamine VKÕK arvutitesse ja/või arvutivõrku.

3.8. Keelatud on infosüsteemi võimalike turvaaukude kasutamine täiendavate juurdepääsuõiguste ja privileegide saamiseks.

3.9. Kasutajal on kohustus turvaaukudest teadlikuks saamisel koheselt teavitada IT-spetsialisti.

3.10. Keelatud on arvutite või seadmete omavoliline ühendamine arvutivõrku, nende ümberühendamine ja nendele mistahes perifeeriaseadmete ühendamine. Mistahes isikliku riistvara paigaldamine peab olema kooskõlastatud infosüsteemi haldajatega.

3.11. Kasutaja on kohustatud kontrollima enda poolt VKÕK ruumidesse toodava tarkvara/andmefaile viirusetõrje programmiga.

3.12. Kasutajale on rangelt keelatud peatada haldaja poolt paigaldatud viirusetõrje programmi.

3.13. Kõik kahtlused, mis on seotud arvuti võimaliku nakatumisega viirustega, peavad olema koheselt edastatud tugipersonalile.

3.14 Hooldust või remonti vajavatest seadmetest tuleb teavitada IT-spetsialisti.

4. Kasutaja õigused

4.1. Kasutusõiguse saanud isikutel on õigus kasutada infosüsteemi vastavalt antud reeglistikule tööalasel eesmärgil igal ajal, kui see ei ole vastuolus muude kehtestatud reeglitega.

4.2. Kasutajal on õigus saada isikuandmete vastutavalt töötlejalt informatsiooni kõigist muudatustest ja sündmustest, mis mõjutavad oluliselt selle kasutamist või kasutajate privaatsust. Samuti on õigus teada, milliseid isikuandmeid töödeldakse, miks neid töödeldakse, kellele neid edastatakse ja kui kaua neid säilitatakse. Kasutajal on õigus nõuda enda kohta kogutud andmete parandamist, nõuda andmete töötlemise piiramist või nende kustutamist, kui see ei ole vastuolus sõlmitud lepingu eesmärgi ja täitmise või seadusest

tulenevate kohustuste täitmisega, või võtta tagasi nõusolek oma andmete töötlemiseks. Kasutajal on õigus esitada kaebus järelevalveasutusele. Kontaktandmed asuvad kodulehel: https://vkok.ee/et/jarelvalve-teostaja.

4.3. Kasutajal on õigus teha ettepanekuid infosüsteemi töö, teenuste ja halduse parema korraldamise osas.

4.4. Kasutajal on õigus infosüsteemi häiretest teatada selle teenindajatele.

4.5. Kui kasutajal on pretensioone infosüsteemi teenindajate suhtes, on tal õigus need esitada VKÕK juhtkonnale.

5. Infosüsteemi haldajate kohustused

5.1. Haldajate primaarseteks kohustusteks on tagada ning jälgida infosüsteemi turvalisust, ettenähtud toimimist ja teenuste kättesaadavust kasutajatele.

5.2. Haldajad peavad tegema kasutajatele kättesaadavaks infosüsteemi kasutamise vastavad juhised.

5.3. Haldajad on kohustatud kasutajatele andma eelteavet olulistest muudatustest infosüsteemis. Samuti on haldajad kohustatud teavitama sündmustest, mis võivad mõjutada kasutajate privaatsust.

5.4. Haldajad on kohustatud saladuses pidama oma töökohustuste täitmise käigus neile avalikuks saanud andmeid, mille kohta neil puudub andmete omaniku luba seda edasi anda, v.a. juhud, kui seadus kohustab informatsiooni teatavaks tegema. Antud reeglistiku rikkumisi puudutav informatsioon kuulub teatavaks tegemisele rikkumisi arutama volitatud isikutele.

5.5. Haldajad on kohustatud teostama andmebaaside ja failiressursside turvakopeerimist vastavalt kehtivale varundusplaanile (vt. punkti andmete varundamine).

5.6. Rikkumise tuvastamisel on haldaja kohustatud koostama vastava sisulise aruande.

5.7. Haldaja on kohustatud regulaarselt hindama rakendatud turvameetmete otstarbekust ja efektiivsust.

5.8. Uute lahenduste kasutusele võtmisel tuleb haldajal läbi viia riskianalüüs ning hinnata mõju terviksüsteemile.

5.9. Haldajad on kohustatud käsitlema turvaintsidente viisil, mis minimiseerib ja/või piirab turvaintsidentidest tekkida võivad kahjud. Turvaintsidendid tuleb dokumenteerida ning vajalik on teostada järelhindamist.

5.10. Haldajad on kohustatud jälgima, et paigaldatav riist- ja tarkvara vastaks kehtestatud standardile.

6. Infosüsteemi haldajate õigused

6.1. Haldajatel on oma kohustuste täitmiseks õigus ajutiselt piirata infosüsteemi kasutamist nii, et see võimalikult vähe häiriks infosüsteemi ja selle kasutajate tööd. Kõigist sellistest piirangutest on infosüsteemi haldajad kohustatud kasutajaid adekvaatselt teavitama (näiteks kasutaja ekraanile tekkiva eelneva hoiatussõnumiga). Infosüsteemi häireolukorra kiireks selgitamiseks või kõrvaldamiseks on infosüsteemi haldajatel õigus lugeda/kustutada kasutajate faile. Niimoodi saadav info ei kuulu levitamisele, v.a. juhud, kui seadus kohustab informatsiooni teatavaks tegema.

6.2. Haldajatel on õigus teostada auditit paroolide haldamise korra järgimise osas (näiteks paroolide murdmine). HOIATUS: tavalistele arvutikasutajatele on selline tegevus rangelt keelatud!

6.3. Haldajatel on õigus rakendada koheselt sanktsioone arvutikasutaja reeglite rikkumiste ilmnemisel või informatsiooni lekkimise vältimiseks (piirata kasutusõigusi, eemaldada omavoliliselt installeeritud programme, kustutada sündsusetuid või piraatlusega seonduvaid ning ressursse raiskavaid faile).

7. Kasutusõiguse saamise kord

7.1. VKÕK infosüsteemi kasutusõigus antakse kasutajakonto väljastamisega vastava taotluse esitamisel otsese ülemuse kaudu:

7.1.1. VKÕK töötajatele;

7.1.2. VKÕK ajutistele töötajatele vastava allüksuse taotluse alusel;

7.1.3. VKÕK IT-teenuseid osutavatele isikutele, kes vajavad selleks kasutusõigust;

7.1.4. Erandkorras võib anda kasutusõiguse teistele isikutele, kui esitatakse põhjendatud taotlus organisatsiooni poolt, millega see isik on seotud.

7.2. VKÕK töötajate kasutusõigus kehtib reeglina nende VKÕK töötamise aja jooksul. Ajutistele kasutajatele ja lepingulistele hooldusisikutele antakse üldjuhul tähtajaline kasutusõigus, reeglina mitte pikemaks ajaks kui üks aasta.

7.3. Kasutusõigus on personaalne ja seda pole lubatud ühelt isikult teisele edasi anda (unikaalne kasutajatunnus identifitseerib kasutajat ja kõiki tema tegevusi, mida võetakse aluseks ka rikkumiste jälgimisel).

7.4. Iga kasutaja peab esmasel kasutusõiguse väljastamisel kinnitama, et on tutvunud VKÕK arvutikasutaja reeglistikuga ning kohustub järgima neis kehtestatud nõudeid.

7.5. Kasutusõiguse saamisel omistatakse taotlejale kasutajakonto(d) unikaalse kasutajanime ja esmase parooliga. Esmane parool tuleb kasutajal endal vahetada kohe pärast esimest infosüsteemi sisenemist vastavalt VKÕK paroolide haldamise korrale (vt. 8).

7.6. Koos kasutusõigusega omistatakse kasutajale (vajadusel) ka tema e-posti aadress.

7.7. Kasutajaõigusi ei väljastata ega muudeta ilma kasutaja otsese juhi kinnituseta.

7.8. Valgamaa Kutseõppekeskus säilitab õpilase G-Suite kasutaja profiili kuni 1 kuu pärast õpingute lõppu. Töösuhte puhul säilitatakse töötaja G-suite kasutaja profiili kuni kuueks kuuks pärast töösuhte lõppu või lepitakse kokku säilitamise aeg.

7.9. Enne õpingute lõppu teavitab kursusejuhataja õpilasi e-posti teel nende e-posti ja õppeinfosüsteemide konto kustutamisest ning annab neile teada võimalusest vajadusel oma andmeid varundada.

7.10. Pärast õppegrupi lõpetamist ja õppekava täitmist teavitab õppesekretär kaugõpetöö logistikut ja haridustehnoloogi rühma lõpetamisest ning saadab teavituse nimekirjaga.

7.11. Pärast teavituse saamist alustavad kaugõpetöö logistik ja haridustehnoloog õppesüsteemide konto kustutamise protsessi. Konto kustutamiseks on aega kolm kuud alates teavituse saamisest. Kaugõpetöö logistik ja haridustehnoloog kustutavad vastavalt nimekirjale kontod, mille kustutamine on vajalik.

8. Paroolide haldamine

Paroolide koostamise nõuded:

8.1. Parool peab:

8.1.1. olema vähemalt 8 tähemärki pikk.

8.1.2. sisaldama vähemalt ühte igast järgnevast tüübist: väike täht, suur täht, number.

8.2. Parool ei tohi:

8.2.1. olla liiga lihtsalt ära arvatav (sarnaneda sõnaraamatu sõnaga, olla kasutaja lemmikfraas jne.).

8.2.2. sisaldada kasutajanime või kasutajaga seotud isiklikku informatsiooni (ära kasuta parooli koostamisel oma, sugulaste või näiteks lemmiklooma nime, mõnda olulist kuupäeva, auto registrinumbrit, isikukoodi, lemmikfraasi vms.).

8.2.3. sisaldada rohkem kui kahte järjestikust sama tähemärki.

8.2.4. sarnaneda varem kasutatud paroolidele või teiste kasutajate paroolidega (rangelt on keelatud isiklikke paroole kasutada tööga seotud paroolidega).

Paroolide hoidmise nõuded:

8.3. Paroole tuleb hoida konfidentsiaalsena (soovitatavalt talletada mälusse, mitte paberile või faili).

8.4. Parooli ega viiteid selle sisule ei tohi jagada teistele isikutele.

8.5. Kasutajaõigustega kaasnev esmane parool tuleb vahetada kohe pärast esmast kasutamist infosüsteemi sisenemisel.

8.6. Kasutajad on kohustatud oma paroole vahetama koheselt, kui tekib kahtlus parooli või kasutusõiguste lekkimises teistele isikutele.

9. Töökoha ja tööjaama (terminali) turvalisus

9.1. Kasutaja peab järgnevalt vältima tema kasutajakonto kasutamist teiste isikute poolt.

9.1.1. Töökohalt ajutiselt (näiteks kõrvalkabinetti või lõunale) lahkudes tuleb arvuti ALATI lukustada (vajuta klahvikombinatsiooni CTRL+ALT+DEL ja seejärel "Lukusta" või kasuta kiirkorraldust "Windowsi logoga klahv + L").

9.1.2. Töökohalt pikemaks ajaks lahkudes tuleb arvutist välja logida, ning peale töö lõppu tuleb arvuti sulgeda.

9.2. Kasutaja on kohustatud vältima tema käsutuses olevate olulist informatsiooni sisaldavate andmekandjate ja andmete sattumist kõrvaliste isikute kätte:

9.2.1. Ei tohi jätta andmekandjaid (CD/DVD, USB, väline kõvaketas jms.) kergesti nähtavatesse või ligipääsetavatesse kohtadesse või neid jätta arvuti vastavasse seadmesse.

9.2.2. Võimalusel on soovitatav kasutaja eemalolekul hoida andmekandjaid lukustatavas sahtlis või kapis (see kehtib ka lukustatavate kabinettide puhul, kui sellele omab normaalset juurdepääsu rohkem kui üks inimene).

10. Interneti kasutamine

10.1. Interneti kasutamine tööajal on lubatud eelkõige ainult tööülesannete täitmiseks.

10.2. VKÕK IT-spetsialistil on õigus inspekteerida ja jälgida kõiki Interneti ühendusi üldvõrgu kaudu ning suunata kogu liiklust läbi vastavate kontrollmehhanismide.

10.3. Salastatud ja konfidentsiaalse informatsiooni edastamine Interneti kaudu krüpteerimata kujul on rangelt keelatud.

10.4. Keelatud on kasutada rakendusi, mis saadavad parooli üle avaliku võrgu krüpteerimata kujul.

10.5. Keelatud on Interneti kasutamine isikliku tulu saamiseks, ebasündsaks käitumiseks, ebasündsate failide vaatamiseks või allalaadimiseks, Interneti ühenduse või arvuti ressursside raiskamist põhjustades või muul moel, mis ei ole VKÕK huvides.

10.6. Keelatud on internetist tundmatute failide käivitamine või allalaadimine (vältimaks nakatumist viirusega või rünnakut pahatahtliku tarkvara läbi)

11. E-posti kasutamine

11.1. Kasutajale antud e-posti kasutusõigus ja e-posti aadress on ette nähtud tööülesannetega seotud kirjavahetuse jaoks.

11.2. E-posti saatmisel tuleb erilist tähelepanu pöörata sellele, et kiri ei satuks valele adressaadile.

11.3. Keelatud on avada e-postiga saadetud kahtlasi või tundmatuid faile tundmatutelt isikutelt. Kahtluse tekkimisel tuleb konsulteerida tugipersonaliga.

11.4. Keelatud on edastada e-posti vahendusel krüpteerimata konfidentsiaalset informatsiooni või muud eriti sensitiivset teavet.

11.5. Keelatud on e-posti ressursse raiskav, ebaviisakas või sündsusetu kasutamine.

11.6. E-posti aadress luuakse kasutajale kujul eesnimi.perenimi@vkok.ee. Keelatud on kasutada katusega tähti ja täpitähti (š, ž, õ, ä, ö, ü asendatakse vastavalt s, z, o, a, o, u).

11.7. Kasutajatunnuse sulgemisega kaasneb e-kirjade postkasti sulgemine. Kirju edasi ei suunata. Teisele töötajale suunatakse e-kirjad direktori ettepaneku alusel.

12. Faili jagmise teenus

12.1. Faile tohib jagada ainult domeeni piires ja konkreetsete inimestega või gruppidega. Soovitatav on kasutada grupitööks tiimikettaid.

12.2. Konkreetseks ürituseks vm. sündmusteks ühistöö dokumentidele/failidele tuleb lisada jagamise lõpu kuupäev.

12.3. Keelatud on ressursse raiskav, ebaviisakas või sündsusetute failide jagamine.

12.4. Töösuhte või õpingute lõpetamisel tuleb lõpetada kõik jagamised või vajadusel anda üle teisele kasutajale.

12.5. Ametlik faili jagamise teenus on Google Workspace Drive.

12.6. Keelatud on failide jagamine kaasaskantavatest või statsionaarsetest tööjaamadest vm. seadmetest.

13. Mobiilsed kasutajad

13.1. Kaasaskantava arvuti kasutamisele kehtivad samad miinimumreeglid nagu statsionaarsetele tööjaamadele.

13.2. Kõik reeglid kehtivad kaasaskantava arvuti kasutamisel nii sisevõrgus kui ka VKÕK-st väljaspool.

13.3. Et tegemist on mobiilse IT-vahendiga, mida kasutatakse ka väljaspool VKÕK infosüsteemi ja selle turvakeskkonda, siis kehtivad kaasaskantavale arvuti kasutamisele ka järgnevad lisareeglid:

13.3.1. Kaasaskantavat arvutit on rangelt keelatud jätta üldkäidavates kohtades ilma järelvalveta (k.a. pargitud sõiduautodes).

13.3.2. Kaasaskantaval arvutil ei tohi töödelda sensitiivseid andmeid avalikus kohas või kohtades, kus töödeldavaid andmeid võivad näha kõrvalised isikud.

13.3.3. Kaasaskantava arvuti kasutusvõimalust on keelatud edasi anda isikutele, kellel puudub selleks VKÕK poolt antud spetsiaalne kasutusõigus koos vastava kasutajakontoga (k.a. kasutaja pereliikmetele).

13.3.4. Kaasaskantav arvuti peab olema lisaks kasutaja paroolile kaitstud ka haldaja poolt seatud BIOSi parooliga.

13.3.5. Kaasaskantaval arvutil asuvate oluliste failide tagavarakoopiate olemasolu eest VKÕK failiserveris vastutab kaasaskantava arvuti kasutaja ise. Haldajad vastutavad ainult failiserveris olevate andmete turvakoopiate ja taastamise eest.

13.3.6. Kaasaskantava arvuti ühendamisel Internetti või mistahes võrku väljaspool VKÕK sisevõrku tuleb kasutada personaalset tulemüüri, mis on konfigureeritud vastavalt VKÕK nõuetele.

13.4. Vastavalt vajadusele võib VKÕK kehtestada kaasaskantava arvuti kõvaketta või selle osa krüpteerimise nõude spetsiaalse tarkvara abil.

14. Riist- ja tarkvara kasutuselevõtt

14.1. Asutuse infosüsteemi ühendatakse arvuti, mille konfiguratsioon vastab riistvara miinimumnõuetele ja sisaldab kohustuslikku tarkvara. Riistvara konfiguratsiooni miinimum tagab kohustusliku tarkvara installeerumise ja toimimise. Sõltuvalt kasutatavast lubatud tarkvarast tulenevad optimaalsed nõuded töökohaarvutile.

14.2. Tarkvara ja riistvara, mis ei ole loetletud vastavas standardis, kasutamise infosüsteemis otsustab direktor vastava taotluse alusel. Otsustamise aluseks on uue riist- ja/või tarkvara:

14.2.1. Ühilduvus asutuse infosüsteemiga;

14.2.2. Kooskõla andmeturbe nõuetega.

14.3. Kõigi asutuse infosüsteemi ühendatud arvutite üle peetakse arvestust IT-spetsialisti poolt peetavas loendis (Cisco Meraki).

15. Andmete varundamine

15.1. Haldaja on kohustatud tegema turvakoopiaid vastavalt varundusplaanile.

15.2. Kaasaskantavast arvutist teeb haldaja varukoopia (kasutajaprofiile sisaldava andmekandja ulatuses) juhul, kui arvuti on VKÕK sisevõrgus kättesaadav. Vastasel juhul vastutab andmete turvakoopiate tegemise eest kasutaja ise.

15.3. Kasutajatel on õigus teha ettepanekuid neile vajaminevate andmete varundamiseks ja varundamise automatiseerimiseks (nt. töökohaarvutist, kaasaskantavast arvutist, erinevatest andmekandjatest). Haldaja varustab ja arhiveerib läbitud e-kursused üks kord aastas augustis.

15.4. Haldaja vastutab rändprofiili salvestatud andmete varundamise eest.

15.5. Haldajal pole kohustust sündsusetuid või piraatlusega seonduvaid ning ressursse raiskavaid (nt. .avi,.mp3, .img) failide turvakoopiate tegemiseks.

15.6. Kasutajatel on keelatud ressursse raiskavate failide hoidmine andmekandjatel või andmekandja osas, kust tehakse turvakoopiaid.

15.7. Haldajatel on õigus muuta andmete varundamise korda ja kohustus teavitada kasutajaid muutustest, kui muudatus puudutab kasutaja andmete varundamist.

16. Turvanõute täitmise kontrollimine

16.1. Turvanõuete täitmist kontrollib IT-spetsialist.

16.2. Tööjaamade/terminalide turvakontrolli tehakse jooksvalt keskselt hallatava tarkvara kaudu.

16.3. Kaasaskantavate arvutite/seadmete kontroll viiakse läbi kasutajaga eelneval kokkuleppel, kuid mitte harvem kui kord aastas.

16.4. Turvanõuete rikkumise avastamisel tuleb sellest koheselt informeerida IT-spetsialisti või kooli personali.

16.5 Avastamine ja Tuvastamine:

16.5.1 Iga VKÕK töötaja ja koostööpartner, kes kahtlustab või avastab infoleket, peab sellest viivitamatult teavitama VKÕK IT-spetsialisti. IT-spetsialist või vastutav isik peab koheselt alustama lekke allika ja ulatuse kindlakstegemist.

16.5.2. Peatamine ja Eemaldamine: Kui infoleke on tuvastatud, tuleb koheselt kasutusele võtta meetmed selle peatamiseks ja lekke allika kõrvaldamiseks. Lekke allika juurdepääs tundlikele andmetele tuleb kohe peatada, kuni uurimine on lõpule viidud.

16.5.3 Hindamine ja Ulatus: IT-spetsialist või vastutav isik peab hindama infolekke ulatust, sealhulgas millist tüüpi andmed on ohustatud, millised seadmed või süsteemid on mõjutatud ja kui palju inimesi võib olla mõjutatud.

16.5.4. Kriitilisuse astme määranguid isikuandmete lekke korral:

- Madal tõsidusaste: Madal tõsidusaste hõlmab tavaliselt juhtumeid, kus lekkinud andmed on avalikult saadaval või ei ole väga tundlikud. Andmed ei sisalda isikuandmeid ega muud tundlikku teavet.

- Mõõdukas tõsidusaste: Mõõdukas tõsidusaste hõlmab tundlikumaid andmeid, kuid lekke ulatus ja mõju on siiski piiratud.

- Kõrge tõsidusaste: Kõrge tõsidusaste hõlmab juhtumeid, kus lekkinud andmed sisaldavad tundlikku teavet, nagu täielikud isikuandmed või finantsandmed.

- Väga kõrge tõsidusaste: Väga kõrge tõsidusaste hõlmab erakordselt tõsiseid juhtumeid, kus lekkinud andmed võivad potentsiaalselt põhjustada tõsist kahju organisatsioonile ja isikutega seotud kriitilisi riske.

16.5.5. Teavitamine ja Raporteerimine: Kui infoleke mõjutab isikuandmeid, tuleb sellest koheselt teavitada asjakohaseid reguleerivaid asutusi ja andmesubjekte vastavalt kehtivatele seadustele ja määrustele, nagu GDPR. Organisatsiooni tuleb teavitada, et koheselt reageeritaks infolekkele ja selle mõjule.

16.5.6. Infoturbe Parandamine: IT-spetsialist või andmekaitsespetsialist peab hindama infolekke põhjuseid ja kasutusele võtma meetmeid, et vältida sarnaste juhtumite kordumist tulevikus. Vajadusel täiustada turvameetmeid, koolitada töötajaid või rakendada täiendavaid protseduure.

16.5.7. Järelvalve ja Dokumenteerimine: Infolekke ja sellele järgnevad tegevused dokumenteeritakse. Dokumenteerib andmekaitsespetsialist rikkumisjuhtumite registrisse. VKÕK regulaarselt jälgib infoturbe olukorda, et tuvastada potentsiaalseid nõrkusi ja ennetada tulevasi lekkeid.

17. Sanktsioonid

17.1. Antud reeglistiku mittetundmine ei vabasta rikkumistega kaasnevast vastutusest.

17.2. Antud reeglistiku rikkumise kahtluse korral võib IT-spetsialist peatada kasutusõiguse kuni asjaolude väljaselgitamiseni.

17.3. Reeglite rikkumises kahtlustataval on õigus esitada omapoolne selgitus.

17.4. Antud reeglistiku rikkumist käsitletakse kui VKÕK huvide otsest ja sihilikku kahjustamist.

17.5. Antud reeglistiku rikkumisel on juhtkonnal õigusrikkujat karistada distsiplinaarkorras.

17.6. Antud reeglite korduva või tahtliku rikkumise puhul võib IT-spetsialist kitsendada kasutaja õigusi VKÕK huvisid silmas pidades vastavalt oma äranägemisele.

17.7. Kasutajatelt, kes antud reeglistiku rikkumisega kahjustavad VKÕK vara või tekitavad lisakulutusi (teenindajate lisatöö aeg, väljakutsed väljaspool põhitöö aega, vms.), võib ettevõte nõuda tekitatud kahju hüvitamist VKÕK poolte kokkuleppel. Kokkuleppe mittesaavutamisel toimub kahju hüvitise sissenõudmine seadusega ettenähtud korras.