LISA 1

direktori 27.10.2025

käskkiri nr 1-2/25/11

IT-halduse kord

Ahtme Kool

Sisukord

1. Sissejuhatus

1.1. Käesolev kord on Ahtme Kooli (edaspidi kool) IT teenuste halduse alusdokument, mis on vastu võetud kooli infoturbepoliitika alusel ja sellega kooskõlas.

1.2. Korra eesmärk on määratleda kooli IT teenuste osutamise põhimõtted ja korraldus, tagades nõuetekohane infovarade kaitse. Eeskiri kehtib kõikidele kooli IT teenustele ja varadele, samuti puudutab see kooli suhtlust ja koostööd teiste riigiasutuste, partnerite ning kolmandate isikutega.

1.3. Korra järgimine on kohustuslik kõikidele kooli IT töötajatele, töövõtu või muu lepingu alusel IT teenust osutavatele isikutele.

1.4. Korra ajakohasuse ja rakendamise eest vastutab haridustehnoloog. Dokument uuendatakse peale igat suuremat muudatust kuid vähemalt kord aastas. Korra ja selle muudatused kinnitab haridustehnoloogi ettepanekul kooli direktor.

2. IT organisatsioon

2.1. Kooli IT-d juhib haridustehnoloog.

2.2. Haridustehnoloogi kontaktid: Aleksandr Girejev, aleksandr.girejev@ahtmekool.ee.

3. IT teenuste osutamise lähtekohad

3.1. IT hoiab saladuses andmeid, mis on saanud talle teatavaks seoses töökohustuste täitmisega ja mille avaldamiseks puudub luba.

3.2. IT tagab IT-teenuste katkematu ja kvaliteetse toimimise ning kõrvaldab esimesel võimalusel infotehnoloogilistes seadmetes ja süsteemides tekkinud tõrked.

3.3. IT osutab kasutajatele igakülgset abi tekkinud probleemide ja küsimuste lahendamisel, tagades seeläbi infotehnoloogiliste seadmete ja süsteemide turvalise kasutamise.

3.4. IT lähtub IT-teenustega seotud intsidentide ja probleemide lahendamisel nende prioriteetsusest, tagades kiireima ja tõhusaima lahenduse.

3.5. IT-l on õigus ning kohustus vajadusel oma tööülesannete täitmiseks peatada ajutiselt infotehnoloogiliste seadmete ja süsteemide töö, teavitades sellest eelnevalt kasutajaid.

4. IT teenuste halduse põhimõtted

4.1. E-ITS infoturbe meetmete juurutamise põhimõtted

4.1.1. Infoturbe meetmete juurutamise lähtekoht on kehtiva E-ITS standardi meetmete nimekiri, millele täiendavalt rakendatakse vajadusel EITS väliseid kaitsemeetmeid.

4.1.2. Turbehalduse meetmete korraldamise üldvastutust kannab kooli direktor, meetmete täitmise eest tervikuna vastutab haridustehnoloog. Turbehalduse meetmete täitmiseks teeb haridustehnoloog koostööd kõikide seotud osapooltega, sealhulgas andmekaitsespetsialistiga, ning tagab asjakohaste osapoolte kaasatuse infoturbega seotud otsuste tegemisse.

4.1.3. IT-juht vastutab IT-korralduse infoturbe järjepideva vastavuse eest parimatele praktikatele, sealhulgas E-ITS tehniliste meetmete juurutamisel:

4.1.3.1. tagab haridustehnoloog kaasamise oma vastutusala IT projektidesse ning IT-süsteemide arendusprotsessi;

4.1.3.2. lähtub meetmete juurutamisel määratud turvaeesmärkidest ja kaitsetarbest, ning võtab arvesse toimivust, tõhusust ja majanduslikku otstarbekust;

4.1.3.3. dokumenteerib süsteemselt rakendatavad turvameetmed ning tagab dokumentatsiooni ajakohasuse;

4.1.3.4. dokumenteerib süsteemselt määratud kuid mitterakendatavate turvameetmete põhjuse ja asjaolud, korraldab põhjendamise aluseks oleva riskianalüüsi läbiviimise;

4.1.3.5. hindab regulaarselt juurutatud meetmete piisavust ja ajakohasust;

4.1.3.6. korraldab riskianalüüside läbiviimist ning nende alusel teeb vajadusel ettepanekuid riskide täiendavaks maandamiseks, sh edasikindlustamiseks;

4.1.3.7. inventeerib regulaarselt E-ITS kataloogi meetmeid ning tagab kõikide ettenähtud meetmete tähtaegse juurutamise;

4.1.3.8. teeb vajadusel õigeaegselt ettepanekuid täiendavate meetmete juurutamise kaalumiseks, arvestades organisatsiooni IT-arhitektuuri võimalusi ja piiranguid, ning äripoole vajadusi;

4.1.3.9. annab õigeaegselt ja regulaarselt aru meetmete täitmise seisust infoturbejuhile, sealhulgas juhtunud intsidentidest;

4.1.3.10. tagab IT töötajate tegevus- ja kontrollikohustuste lahususe, sh määratledes rollid või kohustused mida ei saa täita sama isik.

4.1.4. haridustehnoloog tagab tehniliste meetmete arvestuse korraldamise, seejuures tagades varadele määratud kaitsetarvetele vastavate tehniliste meetmete nimekirja ja rakendamise seisu aja- ja asjakohasuse. Arvestust korraldatakse E-ITS kohustuslike meetmete osas vastavas dokumendis (Exceli fail nimetusega nn),

4.1.5. haridustehnoloog määrab selgelt vastutused teabe, rakenduste ja IT-komponentide osas koos kohustuste, õiguste ning järelevalve korraldamisega, sealhulgas tagades kokkusobimatute rollide lahususe.

4.1.6. haridustehnoloog korraldab IT osakonna töövahendite ja seadmete halduse kooskõlas infoturbe nõuetega ning tagab IT-osakonna töötajate teadlikkuse infoturbe nõuetest.

4.2. Riist- ja tarkvara turve

4.2.1. Riist- ja tarkvara konfiguratsioon peab olema kaitstud volitamata muudatuste eest.

4.2.2. Riist- ja tarkvara peab ühilduma infosüsteemiga. Uue riistvara ja tarkvarakomponentide soetamisele eelnevalt tuleb kontrollida nende ühilduvust olemasolevate komponentidega.

4.2.3. Kõiki infovara muudatusi tuleb enne nende läbiviimist kaaluda infoturbe seisukohast. Selle käigus tehakse kindlaks, kas ja kuidas muutus mõjutab süsteemi ja protsessi

turvalisust ning vähendatakse igakülgselt muudatustega kaasnevate riskide mõju. Muutunud nõuete või uute ohtude korral tuleb turvameetmed ümber hinnata.

4.2.4. Varade hindamisel tuleb arvestada lisaks vara otsesele rahalisele väärtusele selle võimalikust turberikkest (hävimisest, kahjustusest, andmelekkest) tulenevat kaudset kahju tööprotsesside pidurdumise, mainekahju jms näol.

4.2.5. Kõik infovarad (töövahendid, seadmed, kulumaterjalid, seonduv tarkvara, andmekandjad jms) on keskselt registreeritud ja neile on määratud vara eest vastutav töötaja, kes korraldab vara halduse ja infoturbe vastavuse kooskõlas esitatud nõuetega.

4.2.6. Kasutatavad infovarad peavad olema hangitud legaalselt ning nende kasutusviisid olema vastavuses tootja nõuetega.

4.2.7. Riist- ja tarkvara ning nende andmete tervikluse, käideldavuse ja konfidentsiaalsuse kaitsmise eesmärgil on reguleeritud:

4.2.7.1. lubatud riist- ja tarkvara kasutusviisid;

4.2.7.2. tööarvutite seadistamise protsess;

4.2.7.3. eraldiseisvate seadmete kasutamine;

4.2.7.4. tarkvara uuendamine ja versioonihalduses;

4.2.7.5. tarkvara installeerimise, kasutamise, konfigureerimise ja deinstalleerimise protsess;

4.2.7.6. turvanõuded IT-rakendustele;

4.2.7.7. riistvara ja tarkvara inventeerimisprotsess, mis tagab kord aastas või vajadusel sagedamini infovarade nimekirja ning töökohaarvutitesse paigutatud tarkvara ja litsentsilepingute kehtivuse kontrolli;

4.2.7.8. rakendustele ja andmetele juurdepääs;

4.2.7.9. serverite, töökohaarvutite ja mobiilseadmete turve;

4.2.7.10. isikuandmete töötlemise kord ja kasutatavate seadmete dokumenteerimine;

4.2.7.11. riist- ja tarkvara muudatuste haldus;

4.2.7.12. IT-vahendite hooldus ja remont;

4.2.7.13. kaugtöö.

4.2.8. Haridustehnoloog peab hoidma end kursis vastavalt ametialastele vajadustele turvaaukude osas.

4.2.9. Tark- ja riistvara soetamine tuleb planeerida vastava teenuse kasutusse võtmisest lähtuvalt kooskõlas infoturbe nõuetega.

4.2.10. Turvameetmed peavad enne infosüsteemi või selle muudatuse kasutusele võtmist toimima plaanipäraselt.

4.3. Serverite turve

4.3.1. Serverid peavad olema varustatud katkematu vooluallikaga.

4.3.2. Kõigi teenuste puhul, mis seda võimaldavad, peab andmesideks kasutama krüpteeritud SSL/TLS ühendust.

4.3.3. Serverite kaughaldus peab toimuma läbi eraldi oleva kaughaldusvõrgu kaudu.

4.3.4. Serverites kasutatavad teenused peavad olema dokumenteeritud.

4.3.5. Pärast serverite operatsioonisüsteemi baasinstalleerimist tuleb häälestada üksnes tööks vajalikud teenused.

4.4. Tööjaamade, sülearvutite ja mobiilseadmete turve

4.4.1. Tööjaamade, sülearvutite ja mobiilseadmete jaoks peab olema tagatud piisav juurdepääsu kaitse.

4.4.2. Peab olema kehtestatud tööjaamade kasutuse ja seadistamise protsess.

4.4.3. Peavad olema kehtestatud infoturbe-eeskirjad:

4.4.3.1. sülearvutite kasutuse kohta;

4.4.3.2. mobiiltelefonide kasutuse kohta;

4.4.3.3. turvaeeskirjad juhtmeta lisaseadmete kasutamiseks.

4.4.4. Mobiiltelefoni kasutajad peavad olema teadlikud turvaeeskirjadest ja selle järgimist tuleb kontrollida. Täiendavate nutivahendite kasutamine peab olema reguleeritud. Mobiilseadmete rakendused tuleb valida vastavalt tööülesannetele.

4.5. IT vahendite hooldus ja remont

4.5.1. Väliste isikute läbiviidavaid hooldustöid tuleb jälgida.

4.5.2. Hooldustööde kohta peavad olema tõendid.

4.5.3. Hooldustööde läbiviimiseks peavad olema hooldusgraafikud.

4.5.4. Töötajad peavad olema teadlikud, kelle poole tark- ja riistvaraga seotud probleemidega pöörduda.

4.6. Side ja infovahetuse turve

4.6.1. Infotöötlusvahendite õigeks ja turvaliseks käitluseks ning kaitseks tuleb reguleerida:

- võrgutaristu haldus;
- tulemüüri haldus;
- internetiühenduse haldus;
- wifi-haldus;
- paberdokumentide ja elektrooniliste andmekandjate turve,
- info edastamise turve nii suuliselt kui e-kirja, telefoni jm sidevahendite kaudu.

4.6.2. Konfidentsiaalsed andmed seadmetel, millega töötatakse väljaspool kooli ruume, peavad olema krüpteeritud.

4.6.3. Konfidentsiaalsete andmete edastamisel peab olema tagatud andmete terviklus ja konfidentsiaalsus.

4.6.4. Logid peavad võimaldama tuvastada vähemalt lubatavaid ja lubamatuid ressursside poole pöördumisi või pöörduskatseid, nende täpset aega ja lähtekohta. Süsteemi- ja võrgulogisid tuleb regulaarselt analüüsida, samuti iga turvaintsidentide korral. Logisid tuleb säilitada vähemalt 4 nädalat.

4.6.5. Välisvõrgust sisevõrku pöördumisel ja tundlike andmete edastamisel üldkasutatavas võrgus on lubatud vaid turvatud sidesessioonid.

4.6.6. Seadmete konfigureerimisel ja haldamisel lähtutakse põhimõttest, et mis ei ole lubatud, on keelatud.

4.6.7. Sise- ja välisvõrgu veebiserverid peavad asuma erinevates serverites.

4.7. Pilveteenus

4.7.1. Pilvteenuse kasutamise tingimuseks on pilveteenuse strateegia. Läbi peab mõtlema seadusandlikud ja töökorralduslikud raamtingimused.

4.7.2. Kehtestatud peavad olema eeskirjad pilvteenuste kasutamiseks.

4.8. Võrgu turve ja võrguhaldus

4.8.1. Kehtestatud peab olema võrguhalduse kontseptsioon.

4.8.2. Võrgukomponente tuleb võimalusel hallata tsentraalselt.

4.8.3. Võrguliiklust tuleb logida ja auditeerida.

4.9. Võrgu infrastruktuur

4.9.1. Kehtestatud peab olema võrgukontseptsioon.

4.9.2. Kehtestatud peavad olema nõuded võrguhaldusinstrumendile.

4.9.3. Kehtestatud peavad olema eeskirjad marsruuterite ja kommutaatorite sisseseadmisele, käitamisele ning tõrgete kõrvaldamisele.

4.9.4. Aktiivsed võrgukomponendid peavad olema võimalusel paigutatud turvalistesse kappidesse.

4.9.5. Juurdepääs võrgukomponentidele peab olema piiratud.

4.9.6. Kehtestatud peavad olema eeskirjad traadita kohtvõrgu kasutamisel.

4.9.7. Traadita võrgu pääsupunktide vahelised ühendused peavad olema kaabeldatud.

4.9.8. Võrguseadmete kohalik ligipääs tuleb seadistada turvaliselt.

4.10. Võrgu tulemüür

4.10.1. Kogu sise- ja välisvõrgu vaheline liiklus peab käima läbi tulemüüri.

4.10.2. Tulemüüri kasutamisel peavad olema kehtestatud eeskirjad, mille koostamisel peab läbi mõtlema potentsiaalsed teenused ja protokollid.

4.10.3. Tulemüüri seadistamisel tuleb jälgida turvaeesmärke. Olulisemad muudatused tuleb dokumenteerida.

4.10.4. Kõik välised võrkupääsud peavad olema dokumenteeritud.

4.11. Internet

4.11.1. Kehtestatud peavad olema turbe-eeskirjad interneti kasutamiseks.

4.11.2. Internetiteenuste kasutamist tuleb reguleerida tulemüüriga.

4.11.3. Veebibrauserite turvaseaded peavad olema kooskõlas asutuse turvanõuetega.

4.11.4. Kehtestatud peavad olema eeskirjad ja protseduurid veebiteenuste ja rakenduste kasutamiseks.

4.11.5. Kehtestatud peavad olema eeskirjad VPNi kasutamisel.

4.12. Füüsiline turve

4.12.1. Lubamatu füüsilise juurdepääsu vältimiseks asutuse teabele, nende kahjustamisele või häirimisele tuleb reguleerida :

- sissepääs hoonesse ja ruumidesse,
- pääsulubade (võtmete, kaartide ja koodide) haldus,
- valvesüsteemide paigaldus ja haldus,
- tuleohutuse tagamine,
- eriruumide paiknemine ja sissepääs,
- seadmete paigutus ja kaitse,
- töökohtade turve.

4.13. Personali turve

4.13.1. Töötajatest põhjustatud varguse, pettuse või varade väärkasutuse riski vähendamiseks tuleb reguleerida ja fikseerida:

- tööle võtmise tingimused,
- tööülesanded, vastutused ja asenduskord
- turvateadlikkus ja -koolitus,
- töösuhte lõpetamine või muutmine.

4.13.2. Igale töötajale antakse kooli informatsioonile juurdepääs vastavalt tema tööülesannetele. Õiguseid inventeeritakse regulaarselt. Töötaja tööülesannete muutumisel kohandatakse töötaja pääsuõigused ja tema käes olevate organisatsiooni varade valik koheselt vastavaks muutunud tööülesannetega, samuti ajakohastatakse vajadusel eriolukorra- jm tegevuskavad, kuhu töötaja oma varasemate tööülesannete tõttu oli kaasatud.

4.13.3. Kasutaja vastutab täielikult tema kasutajanime all tehtud toimingute eest kooli võrgus ja infovarades. Eeskirjade eiramine toob kasutajale kaasa kooli IT-teenustele juurdepääsu tühistamise, distsiplinaarkaristuse, kahjuhüvitusnõude ja/või lepingu lõpetamise.

4.13.4. Töö- või liikmesuhte lõppemisel algatab personalijuht kasutajakonto sulgemise protsessi ning tagab kasutajaõiguste täieliku deaktiveerimise IT-süsteemides. Õigused deaktiveeritakse hiljemalt töö- või liikmesuhte lõppemise päeva lõpuks, erisused tuleb eelnevalt kooskõlastada infoturbe juhiga. Deaktiveeritud kontod säilitatakse vähemalt 7 aastat. Vajadusel ajakohastatakse eriolukorra- jm tegevuskavad, kuhu lahkuv töötaja oli kaasatud.

4.13.5. Infoturbejuht võib algatada kooskõlas seaduste ja sisemiste regulatsioonidega IT-süsteemide või konkreetse kasutaja tegevuse monitoorimist turvaintsidentide või nõuete vastavuskontrolli uurimiseks.

4.14. Jätkusuutlikkus

4.14.1. Põhitegevuse katkestuste vältimiseks ning põhiprotsesside kaitsmiseks infosüsteemide tõrgete või avariide eest ning nende protsesside õigeaegse tagamise jätkamiseks tuleb reguleerida:

- varundamine ja taastamine;
- kontrolljälgede loomine, haldus ja analüüsimine;
- infoturbe intsidentide käsitlemine.

4.14.2. Tööandmed salvestatakse varundatavale võrgukettale, mille varundamine toimub iga tööpäeva järgselt öösiti. Avariikoopiaid säilitatakse üksteisest sõltumatute koopiatena, vajadusel väljaspool kooli põhitegevuse kohta.

4.14.3. Kasutajate ülesannete ja vastutuse asjakohast lahusust rakendatakse võimalikult suures ulatuses, et vähendada ühest isikust tulenevaid riske.

4.14.4. Infovara peab olema kaitstud volitamata juurdepääsu eest ja juurdepääs infovarale antakse vastavalt tööülesannetest tulenevale teadmis- ja kasutamisvajadusele. Infovarale juurdepääsu eeltingimuseks on seda sooviva kasutaja tuvastamine.

4.14.5. Infovara kasutajad ja nende poolt teostatavad toimingud peavad olema üheselt tuvastatavad. Vastavalt infovara tundlikkusele kehtestab juhtkond kasutajate identifitseerimise ja autoriseerimise tasemed.

4.14.6. Kriitilise infovara kohta peab eksisteerima taasteplaan, mis kirjeldab protseduurid, kuidas naasta tegevuse juurde, mille katkestas intsident.

4.14.7. Oluliste seadmete ja süsteemide puhul tagatakse katkematu elektriga varustamine.

4.14.8. Varunduse ja taastefunktsioone katsetatakse regulaarselt.

4.14.9. Turvaintsidendi korral võib infovara kaitseks piirata selle kasutamist vara eest vastutava töötaja või infoturbejuhi ettepanekul.

4.14.10. Andmete turvaliseks töötlemiseks tuleb kindlustada nõuetele vastav keskkond ja infoturbe kohustuste täitmine.

4.15. Infovarade pääsu haldus ja kasutajakontode haldus

4.15.1. Juurdepääs kõigile IT-süsteemidele ja teenustele on kaitstud kasutajate (sh ka teised IT-süsteemid) tuvastamise ja autentimisega. Parooliga juurdepääsuvahendi kasutamisel muudetakse parool juurdepääsuvahendi esmakordsel kasutamisel.

4.15.2. IT juht korraldab kasutajate ja kasutajarühmade halduse isikute pääsu reguleerimiseks, sh pääsupoliitikate, kasutajakontode ning õiguste profiilide ja kasutajarollide haldamiseks, lähtudes järgnevatest põhimõtetest:

4.15.2.1. juurdepääs infovaradele tuleb anda ainult tööalase vajaduse ja vastutuse alusel, kasutades minimaalsuse põhimõtet. Kasutatakse töötaja ülesannetele vastavaid standardseid õiguste profiile. Muudatuste korral tühistatakse pääsuõigused, mida

enam ei vajata. Tavapärasest suuremaid õigusi antakse töötajale vahetu ülemuse taotluse alusel ning pärast vajadust kinnitavate ja täpsustavate põhjenduse esitamist;

4.15.2.2. kasutajakontod, moodustatud kasutajarühmad ja õiguste profiilid dokumenteeritakse, samamoodi loodud erisused ja nende ajakohasust kontrollitakse regulaarselt, varundatakse regulaarselt ning õiguste dokumentatsioon on kaitstud lubamatu ligipääsu eest.

4.15.2.3. iga infosüsteemi kasutajatunnus peab olema kasutajat üheselt identifitseeriv ning iga kasutajatunnuse omanik peab olema leitav.

4.15.2.4. Töötaja kohustuste ja tööülesannete täitmiseks vajalikud IT-vahenditele ja andmetele juurdepääsuõigused on määratletud. Sissepääsuvahendina kasutatavate pääsmike (ingl security token) väljaandmine või kehtetuks muutmine dokumenteeritakse; isiku pikema äraoleku korral tema juurdepääsuõigused ajutiselt peatatakse.

4.15.2.5. Töösuhte lõppedes tuleb kõik pääsuõigused tühistada vastavalt kooli eeskirjadele. Isiku pikema äraoleku korral (alates 3 kuud) tema ligipääsuõigused ajutiselt peatatakse.

4.15.2.6. Pääsuõiguste vastavust tegelikele vajadustele tuleb regulaarselt kontrollida.

4.15.3. Parooli kvaliteedinõuetele kehtivad järgnevad nõuded:

4.15.3.1. Kasutada tuleb turvalisi paroole. Nõuded parooli kvaliteedile kehtestatakse arvestades IT-süsteemide kaitsetarvet ja kasutajate profiili.

4.15.3.2. Parool ei tohi olla nii keeruline, et kasutaja ei suuda seda regulaarse kasutuse puhul mõistlike pingutustega meelde jätta.

4.15.3.3. Paroole tuleb regulaarselt vahetada.

4.15.3.4. Riist- ja tarkvara algparoolid peavad olema muudetud.

4.15.4. Regulaarselt kontrollitakse, kas IT-süsteemide kasutajad kasutavad oma kasutajakontot ning logivad end pärast ülesande täitmist alati süsteemist välja.

4.15.5. Privilegeeritud kontode (eeliskontode) kaitseks rakendatakse alati mitmikautentimist. Eeliskontot on lubatud kasutada ainult IT-süsteemide haldustööde läbiviimiseks.

4.15.6. Suure kaitsetarbega haldustegevuste läbiviimiseks kasutatakse kahte administraatorit. Mitmikautentimise korral on autentimisvahendid administraatorite vahel jagatud. Ainult parooli kasutamise puhul on parool jagatud kaheks osaks, millest kumbki administraator teab ainult oma osa.

4.15.7. . Serverite ja võrguseadmete administraatoritasemel pääsuõigust tagavad paroolid tuleb deponeerida turvalises kohas.

4.15.8. Iga IT-süsteemi ja rakenduse jaoks on määratud autentimisnõuded ja kehtestatud autentimiskord. Autentimisandmeid hoitakse krüpteerituna ning edastatakse üle andmesidevõrkude krüpteeritult. Kasutatakse kaitsetarbele vastavaid tuvastus- ja autentimismehhanisme.

4.15.9. Kehtestatud peab olema protseduur juurdepääsuõiguste ja juurdepääsu võimaldavate vahendite andmisele ja tagasivõtmisele.

4.15.10. Pääsuõiguste taotlusi ja väljajagatud õiguste muutumist peab kinnitama ja kontrollima selle eest vastutav töötaja.

4.15.11. Kehtestatud peavad olema reeglid kasutajakontodele ja külaliskontodele.

4.15.12. Peavad olema reeglid andmete jagamiseks kolmandate osapooltega.

4.16. IT-teenuste väljast tellimine

4.16.1. Tagamaks, et infotehnoloogiaga seonduvate teenuste väljast tellimine ei halvendaks kooli infoturbe olukorda, tuleb hoolsalt läbi mõelda:

- teenusepakkuja valimine;
- tingimused ja kokkulepped;
- lepingu lõpetamine.

4.16.2. IT-teenuse väljast tellimisele eelnevalt tuleb hinnata selle põhjendatust ning asjakohaseid riske ning nende maandatust. Olemasoleva teenuse asendamisel tuleb kirjeldada teenuse osutamise hetkemaksumust ja hallatavaid andmeid.

4.16.3. Teenuste väljast tellimisel tuleb tagada kehtiva regulatsiooni, sh sisekordade järgimine.

4.16.4. Tarnija valimisel on alati oluline täitja kvalifikatsioon, töötajate arv ning finantsiline suutlikkus nii valiku hetkel kui lepingu kestuse jooksul. Lepingu täitjat tuleb monitoorida kogu lepingu kestuse jooksul, tagades nii teenuse osutamise vastavus lepingule kui ka teenuse pakkuja järjepideva vastavuse esitatud nõuetele.

4.16.5. Teenuse aspektid tuleb kirja panna ja reguleerida teenindusleppega (SLA). Sh tuleb kirjeldada, kes vastutab IT-spetsiifiliste tehniliste ülesannete täitmise eest ja millised on tellija kohustused. Leppes tuleb lisaks teenuste kirjeldusele fikseerida ka teenuste kvantitatiivsed nõuded, nt käideldavus, reageerimisaeg, latentsus, salvestimaht. Lisaks tuleb kirjeldada rakendatavad turvameetmed ja käitumine hädaolukorras, muudatuste haldamine ja testimisprotseduurid, teenuse kvaliteedi ja IT-turvalisuse regulaarsed kontrollid ning sanktsioonid.

4.16.6. Leppes tuleb määratleda kriitilised andmed. Lepingu täitja personali, kes pääseb ligi infoturbe seisukohast kriitilistele andmetele, tuleb kontrollida. Selliste kontrollide teostamine ja ulatus on vajalik kokku leppida sõlmitavas lepingus.

4.16.7. Lepingu lõppemine peab olema täpselt reguleeritud, sh peab olema kokku lepitud teenuse üleandmise tingimused ja kord. On soovitav leppida kokku üleviimisperiood, mille vältel tarnija on kättesaadav konsultatsioonideks ja abistamiseks.

4.16.8. Väliste teenusepakkujatega sõlmitud kokkulepped peavad olema kirjalikult fikseeritud.

4.16.9. Lepingule on kohustuslik määrata asutusepoolne kontaktisik (vastutav töötaja), kes vastutab lepingu täitmise korrektsuse eest.

4.16.10. Kahjurvaratõrje

4.16.11. Viirustõrjeks tuleb kasutada tarkvaralisi ja organisatoorseid meetmeid.

4.16.12. Viiruseskanneri tarkvara peab regulaarselt värskendama.

4.16.13. Kõik IT-kasutajad peavad teadma, kuidas käituda arvutiviiruse esinemise korral.

4.16.14. Välistel andmekandjatel saabuvad dokumendid tuleb üle kontrollida enne kasutamist.

4.17. Turvaintsidentide haldus

4.17.1. Turvaintsidendi mõiste peab olema selgelt defineeritud.

4.17.2. Kõik töötajad peavad olema teadlikud protseduuridest turvaintsidendi puhul.

4.17.3. Turvaintsidente tuleb käsitleda viisil, mis minimiseerib ja/või piirab turvaintsidentidest tekkida võivaid kahjusid.

4.17.4. Turvaintsidentide käsitlemiseks peavad olema planeeritud erinevad stsenaariumid ja prioriteedid.

4.17.5. Kehtestatud peavad olema protseduurid digitaalsete tõendite turvaliseks säilitamiseks.

4.17.6. Kehtestatud peab olema tsentraalne kontaktkoht turvaintsidentide registreerimiseks.

4.17.7. Peab olema määratud kuidas ja kellele turvaintsidendist teatatakse.

4.17.8. Kehtestatud peab olema ühtne protseduur turvaintsidentide ja tõrgete klassifitseerimiseks.

4.17.9. Kõik turvaintsidendid tuleb dokumenteerida.

4.17.10. Kõiki turvaintsidente tuleb järelhinnata ning vajadusel võtta vastu uued või täiendavad regulatsioonid, millest teemaga seotud töötajaskonda teavitatakse.

4.17.11. Järelhindamise käigus avastatud puudused tuleb likvideerida.

4.17.12. Peab olema määratud kuidas ja kellele esinenud kahjudest teatatakse.

4.17.13. Turvaintsidentide käsitluse süsteemi tõhusust tuleb regulaarselt kontrollida.

4.17.14. Turvaintsidentide haldus peab olema vastavuses infoturbe halduse ja hädaolukorra haldusega.

4.17.15. Kehtestatud peab olema tõrgete käsitlemise protseduur.

4.17.16. Kriitiliste süsteemiressursside tervikluse ja kasutaja andmete tervikluse kaitseks tuleb kasutada sobivaid turvamehhanisme.

4.18. Kaugtöö

4.18.1. Kaugtööd tehes ja mobiilse töökoha korral kehtivad samad reeglid, mis koolis kohapeal töötades ja tuleb arvestada kehtiva infoturbestandardi nõuete ning infoturbe riskidega.

4.18.2. Kehtestatud peavad olema protseduurid andmekandjate ja IT-komponentide (näiteks arvutid) kaasavõtmiseks.

4.18.3. Kaugtööga edastavate andmete konfidentsiaalsus, terviklus ja autentsus peab olema tagatud.

4.18.4. Kodutöökoht peab vastama tööalastele nõuetele.

4.19. Seadmete ja informatsiooni hävitamine

4.19.1. Tundlike andmete kõrvaldamiseks andmekandjalt kasutatakse turvalist kustutust või andmekandjad hävitatakse füüsiliselt. Kõik tundlike andmetega tarbetud paberdokumendid hävitatakse.

4.19.2. Kehtestatud peab olema protseduur seadmete ja informatsiooni hävitamiseks, sh ka töötajatele. Iga allüksus määrab, milliseid tööalaseid andmeid ja millistel tingimustel kustutatakse või kasutuselt kõrvaldatakse. Andmete minimaalsete ja maksimaalsete säilitustähtaegade määramisel järgitakse seadusandlusest tulenevaid nõudeid. Isikuandmete säilitamise ja kustutuse protseduurid on kooskõlastatud andmekaitsespetsialistiga. On määratud andmete kustutuse ja hävitamise eest vastutajad, vajadusel kasutatakse spetsiaalset välisteenust. Kui andmeid pole andmekandja defekti tõttu võimalik andmekandjalt turvaliselt kustutada, hävitatakse andmekandja füüsiliselt.

4.19.3. Hävitamine peab olema volitatud.

4.19.4. Hävitamine tuleb dokumenteerida.

4.19.5. Kehtestatud peab olema protseduur IT-süsteemide ja andmekandjate väljavahetamiseks.

4.20. Muudatuste haldus

4.20.1. Kehtestatud peavad olema suunised IT-komponentide, tarkvara või konfiguratsioonifailide muudatuste tegemiseks.

4.20.2. IT-süsteemi muudatused peavad olema dokumenteeritud.

4.20.3. Infosüsteemi kasutajad ja nende kasutajaõigused (juurdepääs teabele ja IT-ressurssidele) peavad olema registreeritud.

4.20.4. Dokumentatsioon peab olema ajakohane ja täielik ning olema kaitstud volitamata isikute eest.

4.20.5. Turvapaikade ja muude muudatuste haldamiseks peab olema kehtestatud kontrollitud protsess.

4.21. Talitluspidevus ja varundamine

4.21.1. Varundamise tarbeks tuleb luua minimaalse andmevarunduse kontseptsioon, mis on kooskõlas kooli ärijätkuvusplaaniga ja lubatava andmete kaoga peale taastamist. Andmevarunduse kontseptsiooni väljatöötamisel on arvestatud kõigi oluliste IT-süsteemide ja rakendustega ning andmevarunduse mõjuritega, see on vastutajatega kooskõlastatud. Töötajad tunnevad andmevarunduse kontseptsiooni tööülesannete täitmiseks vajalikul määral. Andmevarunduse kontseptsioon ja sellega seonduvad dokumendid on turvaliselt varundatud ja kasutatavad ka juhul, kui olulised IT-süsteemid (sh dokumendihaldussüsteem) ei ole juurdepääsetavad. Andmevarunduse kontseptsiooni rakendamist kontrollitakse regulaarselt.

4.21.2. Töötajad peavad olema teadlikud enda andmevarunduse kohustustest.

4.22. Turvakoopiate säilitamine

4.22.1. Andmete säilitamiseks peab olema kehtestatud selge arhiveerimise kontseptsioon, sealhulgas:

- Varunduseks kasutatavaid andmekandjaid hoitakse lähtesüsteemist eraldi asuvas hoiustuskohas.
- Samas hoones hoiustamise puhul asuvad varundatud andmed tuletõkkega eraldatud hooneosas.
- Hoiukoha keskkonnatingimused on sobivad andmekandjate pikaajaliseks säilitamiseks.
- Andmete turvaline säilitus on tagatud vähemalt nõutud andmesäilitustähtaegade ulatuses.
- Varunduseks kasutatavaid andmekandjaid kaitstakse lubamatu juurdepääsu eest.
- Juurdepääs andmekandjatele on üksnes selleks volitatud isikutel.
- Varunduseks kasutatavad andmekandjad on kaitstud lubamatu ülekirjutamise eest.
- Varunduse andmekandjatele antakse kirjutusõigus ainult andmete varundamiseks või autoriseeritud haldustoimingute läbiviimiseks.

4.22.2. Kontseptsiooni aktuaalsust tuleb regulaarselt kontrollida.

4.22.3. Turvakoopiate taaste toimivust tuleb regulaarselt kontrollida, veendudes andmevarunduse toimivuses ja varundatud andmete taastamise funktsioneerimises.

4.22.4. Kontseptsiooni loomisel tuleb arvestada vajalike funktsioonide ja jõudlusega.

4.22.5. Arhiivisüsteemi kasutamise reeglid peavad olema dokumenteeritud ja vastutav isik määratud.

4.23. Tegevuse katkematuse plaanid

4.23.1. Kehtestatud peab olema hädaolukorra plaan, mille abil on võimalik hädaolukordi efektiivselt likvideerida ja kriitilised äriprotsessid kiiresti taaskäivitada.

4.23.2. Haridustehnoloog peab määratlema hädaolukorrahalduse strateegia, mis iseloomustab asutuse sihte ja riskiga leppimise taset.

4.23.3. Hädaolukorra halduse aspekte tuleb arvestada kooli kõikides protsessides.

4.23.4. Hädaolukorrahalduse rollidesse peavad olema nimetatud kvalifitseeritud töötajad.

4.23.5. Hädaolukorra haldamise tarbeks peavad olema eraldatud piisavad finantsilised, tehnilised ja personalialased ressursid kooli eelarve raames.

4.23.6. Hädaolukorraks valmisolekut tuleb regulaarselt kontrollida. Tulemusi tuleb hinnata ja vastavalt vajadusele muudatused sisse viia.

4.23.7. Turvakoopiate taaste usaldatavust tuleb regulaarselt kontrollida.

4.24. Krüptograafia

4.24.1. Krüptomehhamismide kasutamise põhimõtted:

- eelistatakse sõltumatutes uuringutes heakskiidetud krüptoalgoritme, mida on põhjalikult kontrollitud ja mis on teadaolevate turvanõrkusteta. Enne krüptograafiliste vahendi valimist määratakse, millistele nõuetele peab toode vastama ning otsustatakse, kas on vajalik kasutada ainult sertifitseeritud krüptovahendeid.
- kasutatakse soovitatavaid võtmepikkusi, arvestades plaanitud võtme kasutusaega.

- krüpteeritud andmete varundamisel on krüptovõtmed kaitstud lubamatu juurdepääsu eest.
- krüpteeritud andmete pikaajalisel säilitamisel on tagatud andmetele juurdepääs. Krüpteerimiseks kasutatud krüptoalgoritmide ja võtmepikkuste vastavust hetkel soovitavatele väärtustele kontrollitakse regulaarselt.
- pika kasutuskestusega krüptovõtmeid hoitakse väljaspool kasutatavat IT-süsteemi paiknevas võrguühenduseta asukohas.
- kasutusest võetud krüptograafilised vahendid on arhiveeritud ning vastav riist- ja tarkvarakonfiguratsioon on varundatud.

4.25. Logimine

4.25.1. Kehtestatud peavad olema eeskirjad logimisfunktsioonide kasutamiseks.

4.25.2. Kehtestatud peab olema hädaolukorra plaan, mille alusel reageeritakse logimisel avastatud turvaintsidentidele.

4.25.3. Kehtestatud peavad olema eeskirjad, mis tagavad logimise turvalisuse ja efektiivsuse.

4.25.4. Kehtestatud peab olema protseduur logiandmete kontrollimiseks ja analüüsimiseks.

4.25.5. Kehtestatud peavad olema andmeprivaatsuse suunised logimisprotseduurides.

4.26. Välised andmekandjad

4.26.1. Andmekandjate kohta peab olema ülevaade inventariloetelus.

4.26.2. Peavad olema kehtestatud eeskirjad andmekandjate kasutamiseks ja halduseks.

4.26.3. Andmekandjad peavad edasiandmisel olema eeskirjade kohaselt märgistatud.

4.26.4. Andmekandjad peavad edasiandmisel olema eeskirjade kohaselt pakitud.

4.26.5. Väliseid andmekandjaid kasutavad töötajad peavad olema tuttavad andmekandjate halduse eeskirjadega.

4.27. Toide

4.27.1. Vooluahelate turvalisust ja elektrisüsteemi vastavust tegelikkusele tuleb regulaarselt kontrollida.

4.27.2. Varutoite allika funktsioonivõimet tuleb regulaarselt kontrollida.

4.27.3. Kehtestatud peavad olema selged protseduurid puhvertoiteallika kasutamisel.