KINNITATUD
direktori käskkirjaga nr 1-2/25/64
09.12.2025
„Infoturbe poliitika kehtestamine“

JÄRVAMAA KUTSEHARIDUSKESKUSE INFOTURBE POLIITIKA

SISUKORD

JÄRVAMAA KUTSEHARIDUSKESKUSE INFOTURBE POLIITIKA

1. ÜLDSÄTTED

1.1. Rakendusala

1.1.1. Infoturbe poliitika kehtib kogu Järvamaa Kutsehariduskeskuses (edaspidi JKHK).

1.2. Infoturbe poliitika

1.2.1. Infoturbe poliitika on eeskirjade kogum, mis suunab infovarade haldust ja kaitset JKHK-s ning JKHK IT-süsteemis.

1.2.2. Infoturbe poliitika hõlmab JKHK personali, õpilasi, infrastruktuuri, andmeid ja dokumentatsiooni, IT-riist- ja tarkvara ning sidesüsteeme.

1.2.3. Infoturbe poliitika puudutab JKHK suhtlust ja seoseid partnerite, klientide, kolmandate isikute ning meedia ja avalikkusega.

1.3. Infoturbe poliitika eesmärk ja põhimõtted

1.3.1. Infoturbe eesmärgiks on JKHK infosüsteemis töödeldava informatsiooni tervikluse, käideldavuse ja konfidentsiaalsuse tagamine.

1.3.2. Informatsiooni terviklus, käideldavus ja konfidentsiaalsus tuleb tagada ulatuses, mis võimaldab JKHK tõenäolisemate ohtude realiseerumisel häireteta oma ülesandeid täita.

1.3.3. Turvameetmed peavad olema majanduslikult õigustatud ja proportsioonis võimaliku kahjuga, mis võib tekkida meetmete puudulikkuse tõttu ning nende häiriv toime JKHK tegevusele ja töötajate tööle peab olema võimalikult väike.

1.4. Õiguslikud raamtingimused

1.4.1. JKHK lähtub infoturbe alases tegevuses põhiliselt:

1.4.1.1. isikuandmete kaitse üldmäärusest;

1.4.1.2. avaliku teabe seadusest;

1.4.1.3. töötervishoiu ja tööohutuse seadusest;

1.4.1.4. tuleohutuse seadusest, teistest infosüsteemidega seotud seadustest (näiteks riigisaladuse ja salastatud välisteabe seadus, arhiiviseadus, digitaalallkirja seadus, elektroonilise side seadus jne);

1.4.1.5. konkreetse infosüsteemi valdkonna kohta käivatest regulatsioonidest.

1.5. JKHK lähtub nimetatud seadustest niivõrd, kuivõrd on see mõistlik ja otstarbekas infoturbe tagamiseks.

2. INFOTURBE ORGANISATSIOON JA VASTUTUS

2.1. Kooli juhtkond

2.1.1. Üldvastutus infoturbe tagamise eest on direktoril, kes:

2.1.1.1. loob infoturbe tagamise tegevuste eeldused;

2.1.1.2. moodustab infoturbe tagamise töörühma.

2.1.2. Infoturbe erandid kooskõlastatakse, jääkriskid hinnatakse ja aktsepteeritakse juhtkonna tasemel.

2.2. Infoturbe töörühm

2.2.1. Kooli üldise infoturve eest vastutab kooli direktori käskkirjaga määratud töörühm.

2.2.2. Töörühma ülesanded on:

2.2.2.1. infoturbe järjepidev kavandamine ja korraldamine (sh turvameetmete otstarbekuse ja riskide hindamine ning rakendamise koordineerimine);

2.2.2.2. infoturbe dokumentide (sh poliitikad, korrad, juhendid) koostamine ja nende asjakohasena hoidmine;

2.2.2.3. infoturbe seire ja järelevalve korraldamine;
2.2.2.4. töötajate infoturbe alase teadlikkuse tõstmise koordineerimine;
2.2.2.5. regulaarne aruandlus kooli juhtkonnale infoturbe hetkeolukorrast ja arengutest.

2.3. Kooli infoturbejuht

2.3.1. Kooli infoturbe tegevuste rakendamise eest vastutab infoturbejuht, kes:
2.3.1.1. tagab infoturvet reguleerivate juhiste olemasolu, elluviimise ja ajakohastamise käesoleva poliitika põhimõtetest lähtuvalt;
2.3.1.2. korraldab organisatoorsete, füüsiliste ja infotehniliste infoturbe meetmete rakendamist;
2.3.1.3. teeb oma ülesannete täitmisel koostööd andmekaitsespetsialistiga;
2.3.1.4. kontrollib infoturvet reguleerivate juhiste täitmist, hindab asutuse infoturbe tõhusust ning koostab sellekohase raporti, mille sisu ja esitamise sagedus määratakse kindlaks töörühma otsusega;
2.3.1.5. nõustab infoturbe riskide hindamisel, uute turvameetmete loomisel või olemasolevate parendamisel;
2.3.1.6. dokumenteerib kooli turvaintsidendid ning korraldab peale nende lahendamist järelhindamise;
2.3.1.7. koostab olulise mõjuga küberintsidendi lahendamise raporti ning edastab selle Riigi Infosüsteemi Ametile või teistele asjakohastele isikutele;
2.3.1.8. korraldab infosüsteemide valmisoleku hädaolukorraks ning taasteplaani koostamise;
2.3.1.9. teavitab vajadusel töötajaid turva reeglitest, nõustab neid infoturbe alaselt ning vajaduse korral korraldab asutuse töötajatele koolitusi üldise turvateadlikkuse tõstmiseks;
2.3.1.10. täidab teisi õigusaktides sätestatud ülesandeid.

2.4. Kooli struktuuriüksuste juhid

2.4.1. Kooli struktuuriüksuste juhid vastutavad asjakohaste ja ametikohast tulenevate infoturbe tegevuste eest struktuuriüksustes ning peavad:
2.4.1.1. tagama infoturbe tegevuste täitmise juhitavas üksuses;
2.4.1.2. jälgima kõigi vahetute alluvate infosüsteemide kasutamise ja toimimise õiguspärasust;
2.4.1.3. tegema infoturbejuhile ettepanekuid infoturbealaste tegevuste parenduseks.

2.5. Töötajad

2.4.2. Kõik JKHK töötajad vastutavad oma töövaldkonnas infoturbe eesmärkide saavutamise ja kehtestatud kordade täitmise eest ning peavad:
2.4.2.1. tagama informatsiooni tervikluse, käideldavuse ja konfidentsiaalsuse töötaja töölõigus;
2.4.2.2. tagama kõiki talle määratud kasutajatunnuste sihipärase kasutamise;
2.4.2.3. tagama kõigi tema kasutusse antud infosüsteemi komponentide säilimise ning turvalisuse.

3. INFORMATSIOONI TUNDLIKKUS JA RISKID

3.1. JKHK-s kasutusel olev informatsioon

3.1.1. JKHK-s kasutusel olev informatsioon jaguneb avalikuks informatsiooniks ning asutusesiseseks kasutamiseks (edaspidi AK) mõeldud informatsiooniks.
3.1.2. Asutusesiseseks kasutamiseks (AK) mõeldud teave on teave, millele on avaliku teabe seaduse § 35 alusel kehtestatud juurdepääsupiirang. AK-teabe hulka kuulub eelkõige isikuandmeid sisaldav teave, sealhulgas eri liiki isikuandmed, ning muu teave, mille avalikustamine võib kahjustada asutuse, töötajate, õppijate või koostööpartnerite õigusi ja huve või millele on kehtestatud juurdepääsupiirang õigusaktide või lepingute alusel.

3.2. Ülevaade JKHK informatsioonist

3.2.1. JKHK töötleb informatsiooni, mis on vajalik:
3.2.1.1. seadustega ettenähtud ülesannete täitmiseks;
3.2.1.2. õppetöö toetamiseks;
3.2.1.3. asutuse toimivuse tagamiseks.

3.2.2. JKHK-s töödeldakse informatsiooni digitaalsel kujul (andmekogudes, registrites, tabelites, digitaalsetes dokumentides, e-kirjades) ja paberkandjatel (dokumendid).

3.2.3. Olulisemad andmekogud on:

3.2.3.1. Office 365
3.2.3.2. Riigitöötaja Iseteeninduspordaal – RTIP
3.2.3.3. Dokumendihaldussüsteem – PINAL
3.2.3.4. Eesti Hariduse infosüsteem – EHIS
3.2.3.5. Õppeinfosüsteem – TAHVEL
3.2.3.6. Sisseastumise infosüsteem – SAIS
3.2.3.7. Finantsarvestuse rakenduskeskkond – SAP
3.2.3.8. Õppeprotsessi rakenduskeskkond – Moodle
3.2.3.9. Kooli koduleht

3.3. Riskihalduse strateegia

3.3.1. Infoturbe töörühm vastutab infoturbe regulaarse riskide maandamise eest:
3.3.1.1. kontrollides regulaarselt turvameetmete otstarbekust ja efektiivsust;
3.3.1.2. viies uute infotehnoloogiliste lahenduste kasutuselevõtul läbi riskianalüüsi ja hinnates nende mõju terviksüsteemile.

3.4. **Turvaintsidentide haldus**

3.4.1. Turvaintsident on iga teenuse/protsessi mitteplaneeritud katkestus või kõrvalekalle, mis mõjutab teenuse/protsessi käideldavust ja/või terviklust ja/või konfidentsiaalsust.
3.4.2. Turvaintsidenti käsitletakse viisil, mis minimiseerib ja/või piirab turvaintsidentidest tekkida võivaid kahjusid.
3.4.3. Turvaintsidendi avastanud töötaja on kohustatud sellest teavitama infoturbejuhti.

4. RIIST- JA TARKVARA TURVE PÕHIMÕTTED

4.1. Üldturve

4.1.1. Riist- ja tarkvara soetamise, paigaldamise, infosüsteemi lülitamise, konfigureerimise ja haldamise eest vastutab infoturbejuht.
4.1.2. Paigaldatav riist- ja tarkvara peab ühilduma JKHK infosüsteemiga ning vastama vähemalt JKHK-s kehtestatud riist- ja tarkvara standardile.
4.1.3. 4.1.3. Riist- ja tarkvara konfiguratsioon peab olema kaitstud volitamata muudatuste eest.

4.2. Pääsu reguleerimine

4.2.1. JKHK infoturbejuht annab töötajale juurdepääsu infovaradele ainult tööalase vajaduse ja vastutuse alusel tingimusel, et
4.2.1.1. Iga väljaantud kasutajatunnus peab olema kasutajat üheselt identifitseeriv ning iga kasutajatunnuse omanik peab olema leitav.
4.2.1.2. Iga kasutaja kasutab eranditult turvalisi paroole ning paroole vahetatakse regulaarselt.
4.2.1.3. Kõigi arvutitega tohib saadatööd alustada alles pärast kasutajanime ja parooli sisestamist.
4.2.1.4. Riist- ja tarkvara esmased paroolid peavad olema muudetud.
4.2.1.5. Serverite ja võrguseadmete administraatoritasemel pääsuõigust tagavad paroolid tuleb deponeerida turvalises kohas.
4.2.1.6. Töösuhte lõppedes tühistatakse kõik pääsuõigused viivitamatult.
4.2.2. Infoturbejuht kontrollib regulaarselt pääsuõiguste vastavust tegelikkusele.

4.3. Viirusetõrje

4.3.1. Viirusetõrje programmid peavad hõlmama kogu JKHK IT-süsteemi.
4.3.2. Viirusetõrje programmid peavad töötama reaalajas.
4.3.3. Viirusetõrje programmid peavad olema otstarbeka regulaarsusega uuendatud.
4.3.4. Enne installeerimist ja kasutusele võtmist tuleb kogu hangitud tarkvara üle kontrollida viirusetõrje programmiga.

4.4. Serverite turve

4.4.1. Serverid peavad asuma serveriruumis ja neid tohib kasutada ainult määratud otstarbeks.

4.4.2. Avalikke teenuseid tagavad serverid peavad olema eraldatud sise- ja välisvõrgust tulemüüriga.

4.4.3. Serverid peavad olema varustatud katkematu vooluallikaga, mis tagab elektritoite vähemalt 15 minutiks.

4.5. Tööjaamade turve

4.5.1. Tööjaamades (va sülearvutid) ei tohi olla modemeid. Nende olemasolul peavad need olema blokeeritud.

4.5.2. Kasutaja peab arvuti kasutamisel tagama, et kõrvalised isikud ei pääseks ligi arvutis olevatele andmetele.

4.5.3. Kaughaldus tarkvaraga tööjaama sisenemisel peab IT-personal eelnevalt kasutajat teavitama.

4.6. Sülearvutite turve

4.6.1. Sülearvutite kasutajad peavad olema teadlikud süsteemide ja andmete väärtusest ning sülearvutite kasutamisega kaasnevatest ohtudest.

4.6.2. Sülearvuteid tuleb kaitsta varguse, kahjulike keskkonnamõjude, aku liigtühjenemise, pealtvaatamise ja –kuulamise eest.

4.6.3. Sülearvutid peavad olema varustatud personaalse tulemüüriga ja kaitstud parooliga.

4.7. Tarkvara turve

4.7.1. Kasutada tohib kasutada ainult legaalset tarkvara ja legaalsel viisil.

4.7.2. Regulaarselt tuleb paigaldada turvalisust mõjutavad tarkvara paigad ja täiendused.

4.7.3. Uue tarkvara arenduse kõikides etappides (kaasa arvatud hankekutse koostamine, tarnijate valimine, analüüs, disain, realisatsioon, testimine, üleandmine, andmete ülekanne jne) tuleb arvestada infoturbe nõuetega. Eelpoolmainitud etappide tulemid tuleb dokumenteerida.

4.7.4. Uus tarkvara tuleb enne käikuandmist testida.

4.7.5. Testimisteks ega näidiskasutamiseks ei tohi kasutada konfidentsiaalseid andmeid.

4.8. Kaugtöö

4.8.1. Kaugtööarvuti tuleb kujundada selliselt, et ebaturvalises kasutuskeskkonnas oleks võimalik selle turvaline kasutamine.

4.8.2. Kaugtööd tohib sooritada ainult turvalise side kaudu ja järgides JKHK-s kehtestatud turvanõudeid.

4.8.3. Kaugtööks kasutatavas arvutis peab reaalajas töötama viirusetõrje programm ja tagatud peab olema viirusekirjelduste igapäevane uuendamine.

4.8.4. Kaugtööks kasutatav arvuti peab olema varustatud tulemüüriga.

4.8.5. Kaugtööks kasutatava arvuti kasutamisel peab kasutaja tagama, et kõrvalised isikud ei pääseks ligi arvutis olevatele andmetele.

4.8.6. Kaugtöö korral peab olema tagatud andmete varundamine.

4.9. Logimine

4.9.1. Logid peavad võimaldama tuvastada lubatavaid ja lubamatuid ressursside poole pöördumisi või pöörduskatseid (sh süsteemiadministraatorite), nende täpset aega ja lähtekohta.

4.9.2. Logid peavad olema kaitstud kustutuse, muutmise, võltsimise või ümberjärjestamise eest.

4.9.3. Logide revisjoni tuleb sooritada pisteliselt ning vastavate turvaintsidentide korral, kuid mitte harvem kui kord kuus.

4.10. Muudatuste (konfiguratsiooni) haldus

4.10.1. Riist- või tarkvara muudatused ei tohi ohustada üldist turvalisust.

4.10.2. Iga riist- või tarkvara muudatuse korral tuleb eelnevalt uurida muudatuse mõju terviksüsteemi turvalisusele.

4.10.3. Iga uus riist- ja tarkvara tuleb enne kasutuselevõttu testida.

4.10.4. Kõik muudatused ja sinna juurde kuuluvad valikukriteeriumid tuleb salvestada taastamist võimaldaval kujul.
4.10.5. Kõikidest kasutajaid puudutavatest muudatustest tuleb kasutajaid informeerida.
4.11. IT-vahendite hooldus ja remont
4.11.1. IT-seadmete hoolduse ja remondi teostab või organiseerib IT-spetsialist.
4.11.2. Enne IT-seadmete utiliseerimist või renditud riistvara tagastamist tuleb seadmest eelnevalt eemaldada füüsilised andmekandjad või andmed andmekandjalt kustutada viisil, mis välistaks informatsiooni taaskasutamise.

4.12. Krüpteerimine

4.12.1. Minimaalne lubatav võtme pikkus sümmeetrilise krüptosüsteemi kasutamisel on 256 bitti. Minimaalne lubatav võtme pikkus asümmeetrilise krüptosüsteemi kasutamisel on 2048 bitti.
4.12.2. Välisvõrgust sisevõrku pöördumisel ja tundlike andmete edastamisel üldkasutatavas võrgus on lubatud vaid turvatud sidesessioonid: VPN, SSL/HTTPS, krüpteerimine.
4.12.3. Konfidentsiaalsed andmed seadmetel, millega töötatakse väljaspool JKHK ruume, peavad olema krüpteeritud.
4.12.4. Kasutada ei tohi rakendusi, mis saadavad parooli üle avaliku võrgu krüpteerimata kujul.

5. VÕRGU TURBE PÕHIMÕTTED

5.1. Infrastruktuur

5.1.1. Võrk peab olema jagatud vajaduse järgi väiksemateks alamvõrkudeks ning olema sobiva füüsilise ja loogilise ülesehitusega.
5.1.2. Arvutitega sisevõrku pääsemine peab olema asutuse kontrolli all.
5.1.3. Avaliku võrgu kaudu tohib sisevõrgu ressursside poole pöördumiseks kasutada ainult krüpteeritud ühendust.
5.1.4. Tehases konfigureeritud standardsed turvaseadistused tuleb ära muuta.
5.1.5. JKHK sise- ja välisvõrgu toimivuseks olulisemad võrguseadmed tuleb varustada katkematu vooluallikaga.
5.1.6. Kogu IT-kaabeldus peab olema tähistatud ja dokumenteeritud ning paiknema varjatult.
5.1.7. Külaliste võrk peab olema JKHK sisevõrgust eraldiseisev ja Wifi puhul parooliga kaitstud.
5.1.8. Regulaarselt tuleb jälgida võrguühenduse koormust ja liiklust.

5.2. Tulemüür

5.2.1. Kogu sisevõrgu ja välisvõrgu vaheline liiklus peab käima läbi tulemüüri.
5.2.2. Tulemüüris tuleb rakendada põhimõtet, mille kohaselt välisvõrgust sisevõrgu suunas ja sisevõrgust välisvõrgu suunas on avatud võimalikult vähe porte ning ainult need, mis on vajalikud tööalaste ülesannete täitmiseks ning ainult need, mis ei ohusta IT süsteemide turvalisust.
5.2.3. Tulemüür peab täitma järgmisi põhilisi turvaeesmärke:
5.2.3.1. sisemise võrgu kaitse ebausaldusväärsest võrgust tulevate volitamata juurdepääsukatsete vastu;
5.2.3.2. välisvõrgu informatsiooni kättesaadavus kaitstavas sisevõrgus;
5.2.3.3. kaitse võimalike tarkvara turvaaukude vastu;
5.2.3.4. kaitse mittesoovitud andmeliikumise vastu.
5.2.4. Kõik olulisemad muudatused tulemüüri konfiguratsioonis tuleb kirjalikult dokumenteerida.

5.3. Internet

5.3.1. Internetiteenuste kasutamine on võimaldatud kõigist JKHK sisevõrgus olevatest arvutitest.
5.3.2. Interneti kasutamine JKHK-s on ette nähtud tööalaseks kasutamiseks.
5.3.3. Infoturbe huvides võidakse sisevõrgu arvutitest internetiteenuste poole pöördumisi jälgida ja/või piirata.

5.4. E-kiri

5.4.1. Saadetud kirjad peavad sisaldama saatja pärisnime.
5.4.2. Sisenevad ja väljuvad kirjad tuleb allutada viirusetõrje ja rämpsposti kontrollile.
5.4.3. Meiliklient tuleb konfigureerida nii, et kirja manusfaile ei käivitataks kogemata. Käivitamine peab nõudma kinnitust.
5.4.4. Aktiivsisuga failide edastamine e-posti teel peab olema takistatud.

6. TEGEVUSE KATKEMATUSE PÕHIMÕTE

6.1. Varundamine

6.1.1. Turvakoopiaid tuleb teha kõigist JKHK jaoks olulistest infosüsteemi serverites paiknevatest andmetest ja süsteemidest.
6.1.2. Töökohaarvutis olevatest andmetest turvakoopiate tegemise eest vastutab arvuti kasutaja.
6.1.3. Turvakoopiad tuleb teha erinevatele andmekandjatele ja/või kettamassiividele.
6.1.4. Turvakoopiad peavad olema varundatavatest andmetest erinevates füüsilistes asukohtades.
6.1.5. Varundada tuleb varundusplaanides kokkulepitud perioodide seise.

6.2. Turvakoopiate säilitamine

6.2.1. Turvakoopia säilitamisel tuleb järgida andmekandja tootja kehtestatud säilitustingimusi.
6.2.2. Turvakoopiaid tuleb säilitada viisil, mis välistab nende riknemise või kao infosüsteemiväliste tegurite mõjul samaaegselt infosüsteemi serveritega.
6.2.3. Turvakoopiatele on juurdepääs ainult direktori poolt määratud isikutel.

6.3. Tegevuse katkematuse plaanid

6.3.1. Andmeid peab olema võimalik taastada vastavalt varundusplaanides kirjeldatule.
6.3.2. Turvakoopiate taaste usaldatavust tuleb regulaarselt testida vastavalt varundusplaanis ettenähtud korrale.

6.4. Riistvara

6.4.1. Vajadusel asendatakse rikkis riistvarakomponent ajutiselt teise, vähem olulise süsteemi komponendiga.

6.5. Sideliinid

6.5.1. Varuliinidena tuleb kasutada töövõime säilitanud liine.

6.6. Toide

6.6.1. Varugeneraatorite või -toiteliinide soetamine pole majanduslikult otstarbekas.
6.6.2. Oluliste seadmete ja süsteemide toide varundatakse akude või puhverallikatega.

6.7. Tööruumid

6.7.1. Varutööruumid puuduvad.

7. INFO- JA ANDMEVAHETUSE TURVE PÕHIMÕTTED

7.1. Üldturve

7.1.1. AK-ks tunnistatud andmete edastamisel peab olema välistatud andmete tervikluse ja konfidentsiaalsuse kadu.
7.1.2. Isikuandmete ja eriliigiliste isikuandmete edastamine kolmandatele isikutele peab toimuma vastavalt isikuandmete kaitse üldmäärusele, avaliku teabe seadusele ja muudes seadustes sätestatud tingimustele.
7.1.3. Isikuandmete ja eriliigiliste isikuandmete edastamise korral tuleb tagada info andmete edastamise kohta: millal, kellele, mis õiguslikul alusel ja milliseid isikuandmeid edastati. Samuti tuleb tagada selliste andmete muutusteta säilimine.

7.2. Suuline suhtlus

7.2.1. AK-ks tunnistatud teabe edastamine telefoni teel on keelatud.

7.2.2. AK-ks tunnistatud teabe koolisisesel käsitlemisel tuleb välistada tööalaselt asjassepuutumatute isikute pealtkuulamise võimalus.

7.3. E-kiri

7.3.1. AK-ks tunnistatud teavet tohib e-kirja teel edastada ainult krüpteeritult.

7.4. Kiirsuhtlustarkvara

7.4.1. Elektrooniline kiirsuhtlus toimub Microsoft Teams tarkvaraplatvormi kaudu.

7.4.2. Kiirsuhtlustarkvara abil on failide vahetamine keelatud.

7.4.3. Kiirsuhtlustarkvara kasutades on AK-ks tunnistatud teabe edastamine keelatud.

7.5. Infovahetus väliste andmekandjate (nt CD-ROM, väline kõvaketas, mälupulk jne) abil

7.5.1. Väliste andmekandjate saatmisel või transportimisel peab olema tagatud andmete käideldavus, terviklus ja vajadusel konfidentsiaalsus.

7.5.2. Andmete üleandmiseks kasutataval välisel andmekandjal ei tohi olla mingeid muid materjale ega peitandmeid.

7.5.3. AK-ks tunnistatud teave tuleb andmevahetuse jaoks krüpteerida. Peale andmevahetuse teostamist tuleb teave andmekandjalt turvaliselt kustutada või andmekandja füüsiliselt hävitada.

7.5.4. Saadud andmekandjatele tuleb teha viirusekontroll.

8. KOLMANDATE OSAPOOLTE PAKUTAVATE IT-TEENUSTE TELLIMISE PÕHIMÕTTED

8.1. Kolmandad osapooled ja väljasttellimine

8.1.1. IT-teenuste tellimine kolmandatelt osapooltelt ei tohi halvendada JKHK infoturbe olukorda.

8.1.2. Väliseid lepingupartnereid tohib lubada töid teostama peale lepingute allakirjutamist.

8.1.3. Lepingud peavad vastama võlaõigusseadustikus sätestatule ja lepingus peab olema selgelt määratletud töövõtja infoturbealane vastutus ning infoturbenõuete täitmise kohustus.

8.1.4. Lepingu lõppemisel peab olema viimase tööpäeva lõpuks tagatud kõigi kolmanda osapoole valduses olevate pääsuvahendite tagastamine ning pääsuõiguste tühistamine.

9. FÜÜSILINE TURVE PÕHIMÕTTED

9.1. Uksed ja aknad

9.1.1. Hoonete sissepääsud peavad olema väljaspool õppetöö aega lukustatud.

9.1.2. Tühjad tööruumid peavad olema lukustatud ja aknad turvaliselt suletud.

9.1.3. Ruumide kasutus tagatakse vaid vastavalt tööalasele vajadusele.

9.1.4. Rakendada tuleb sissepääsupiiranguid ja sissemurdmisvastaseid kaitsesüsteeme.

9.1.5. Kool säilitab andmed uste avamise logiga, milles nähtub ukse avaja isik ning avamise aeg.

9.2. Pääsuvahendite haldus

9.2.1. Pääsuvahendeid tuleb hoida viisil, mis välistab nende volitamata kasutamise, kadumise või varguse.

9.2.2. Pääsuvahendite jagamise üle tuleb pidada dokumenteeritud arvestust.

9.2.3. Kaartide ja koodide kasutajad peavad olema identifitseeritavad.

9.2.4. Üldvõti väljastatakse töötajale kooli direktori loal ainult erandjuhul.

9.2.5. JKHK säilitab kõikide hoonete uste tagavaravõtmed. Tagavaravõtmeid tuleb hoida viisil, mis välistaks nende volitamata kasutamise.

9.2.6. Töötajaga töösuhte lõpetamisel tuleb tagada kõikide tema valduses olevate pääsuvahendite tagastamine ja/või tühistamine.

9.3. Valve

9.3.1. Valvesignalisatsiooni andurid ja -süsteem peavad olema paigaldatud selliselt, mis aitaks kaasa volitamata sissepääsu kiirele avastamisele.

9.3.2. Ruumid peavad olema vastavalt otstarbele jagatud valvetsoonideks. Tsoonide valve all olev aeg määratakse kindlaks infoturbe töörühma otsusega.

9.3.3. JKHK korraldab valvesignalisatsiooni süsteemi regulaarse kontrolli ning erakorralise kontrolli valvesignalisatsiooni käivitumise järel.

9.4. Tuleohutus

9.4.1. Ruumid peavad olema varustatud tulekahjusignalisatsiooni anduritega, mis peavad olema paigaldatud vastavalt tuletõrje eeskirjadele ja valmistaja nõuetele.

9.4.2. Tulekustutite arv, paigutus ja kontrollimine peavad vastama tuletõrje eeskirjadele.

9.4.3. Arvutitega varustatud ruumide ja kilbiruumide kustutid peavad olema vastava seadme kustutamiseks ettenähtud nõuetekohased gaas- või pulberkustutid.

9.5. Eriruumide turve

9.5.1. Eriruumide asukoha valikul tuleb tagada nende ruumide spetsiifikast tulenevad turvanõuded.

9.5.2. Eriruumid peavad olema varustatud valve- ja tulekahjusignalisatsiooniga ning sobivate tulekustutusvahenditega.

9.5.3. Kui eriruumis kedagi ei ole, peab uks olema lukustatud ja valve aktiveeritud.

9.5.4. Eriruume ei tohi märgistada üldarusaadavalt ega kanda viitadele või majajuhti.

9.5.5. Eriruumides tohivad volitamata isikud viibida ainult koos volitatud saatjaga.

9.5.6. Eriruumides peab olema tagatud õhutemperatuuri reguleerimine.

9.6. Töökohtade turve

9.6.1. Kõigil töökohtadel tuleb AK-ks tunnistatud teabe suhtes järgida tühja laua printsiipi, st. enne ruumist lahkumist kõrvaldada laualt jm nähtavatest kohtadest kõik vastavaid andmeid sisaldavad dokumendid ja andmekandjad.

9.6.2. AK-ks mõeldud dokumente, neid andmeid sisaldavaid andmekandjaid ning väikesemõõtmelisi väärtuslikke füüsilisi varasid tuleb hoida lukustatud kapis, sahtlis või seifis.

9.6.3. Töökohast ajutiselt lahkudes tuleb arvuti lukustada ja pikemaks ajaks lahkudes tuleb arvutist välja logida.

9.7. Andmekandjate turve

9.7.1. Paberdokumentide, elektrooniliste dokumentide ja elektrooniliste andmekandjate kättesaadavus tuleb tagada ainult volitatud töötajatele. Vajadusel varustada ruumid valvesignalisatsiooniga, turvakapiga või seifiga.

9.7.2. Eriliigilisi isikuandmeid sisaldavaid dokumente tohib andmekandjatel hoida krüpteerimata kujul ainult seifis, lukustatavas turvakapis või eriruumis.

9.7.3. Andmekandjad tuleb märgistada nii, et oleks teada, millega on tegu, kuid mis ei viita andmete tundlikkusele.

9.7.4. Andmekandjaid tuleb säilitada selliselt, et oleks tagatud andmekandjatel olevate andmete säilimine.

9.7.5. Arhiveerimisele kuuluvaid andmeid sisaldavad andmekandjad tuleb arhiveerida ning säilitustähtaja möödumisel hävitada vastavalt koolis kehtestatud teabehalduse korrale.

9.7.6. Arhiveeritud andmekandjaid tuleb säilitada vastavalt seadusandlusele ja koolis kehtestatud teabehalduse korrale.

9.7.7. Andmekandjad, mis sisaldavad AK-ks tunnistatud teavet, tuleb hävitada viisil, mis välistaks informatsiooni taasesitamise.

9.8. Mobiilse aparatuuri turve

9.8.1. Mobiiltelefonide ja sülearvutite turbe eest vastutavad nende valdajad.

9.8.2. Turvariskide maandamiseks (näiteks võimaliku infolekke korral sülearvuti sattumisel kõrvaliste isikute valdusse) peab konfidentsiaalse sisuga tööalane informatsioon sülearvutis olema krüpteeritud.

9.9. Muu aparatuuri turve

9.9.1. Mittemobiilset aparatuuri tohib JKHK hoonetest välja viia ainult IT spetsialisti loal.

9.9.2. Näitustel, messidel ja teistes inimeste massilise kogunemise kohtades tuleb kasutada vahendeid aparatuuri turvaliseks kinnitamiseks aluse või kandja külge.

9.10. Hoolde- ja remonditööd

9.10.1. Hoolde- ja remonditööde käigus tuleb järgida andmeturbe nõudeid.

9.10.2. Hoolde- ja remondipersonalile tohib avada töödeks ainult minimaalselt vajalik arv ruume ning vältida tuleb nende juurdepääsu andmetele.

9.10.3. Eriruumidesse tohib hoolde- ja remondipersonali lubada ainult koos volitatud saatjaga.

9.11. Puhastusteenistujad

9.11.1. Puhastusteenistujatele tohib anda ligipääsu ainult koristustöödeks vajalikele ruumidele ja ainult vajalikel aegadel.

9.11.2. Pääsuvahendeid tohib väljastada puhastusteenindajatele ainult allkirja vastu ja ajalise piiranguga.

9.11.3. Puhastusteenistujaid tuleb teavitada IT-ga ja dokumentidega ümberkäimise eeskirjadest.

9.11.4. Eriruumidesse tohib puhastusteenistujaid lubada ainult koos volitatud saatjaga.

9.12. Kolimine

9.12.1. Kolimise ajal peab olema tagatud infosüsteemide ja andmekandjate nõuetekohane turvataseme säilimine.

10. PERSONALI TURVE PÕHIMÕTTED

10.1. Töölevõtmine ja töölt vabastamine

10.1.1. Enne töötaja tööle võtmist tuleb kontrollida võimaluste piires iga kandidaadi tausta turvariski aspektist lähtuvalt.

10.1.2. Tööandja ja töövõtja vahel sõlmitavates lepingutes ja muudes kokkulepetes tuleb esitada asjakohased viited infoturbe tagamiseks.

10.1.3. Uue töötaja töölevõtul tuleb töötajale tutvustada infoturvet reguleerivaid dokumente, kehtivaid eeskirju ja tegevusjuhiseid ning vajadusel läbi viia esmane infosüsteemi kasutamise koolitus.

10.1.4. Uue töötaja sissejuhatava instrueerimise tööülesannetest tulenevate kohustuste ja vastutuse osas peab läbi viima või organiseerima struktuuriüksuse juht.

10.1.5. Töötajaid tuleb teavitada, et nende tegevust infosüsteemis võidakse jälgida.

10.1.6. Töötajaga töösuhte lõpetamisel tuleb tagada viimase tööpäeva lõpuks kõigi tema valduses olevate varade ja pääsuvahendite tagastamine ning pääsuõiguste tühistamine.

10.2. Turvateadlikkus ja –koolitus

10.2.1. Vajaliku turvateadlikkuse taseme saavutamiseks tuleb välja töötada tõhus infoturbe teadlikkuse programm ning läbi viia vastavasisulisi koolitusi.

10.2.2. Igal töötajal on õigus saada teenistuseks vajalikku eri-, kutse- ja ametialast koolitust.

10.2.3. Igale töötajale peab olema tagatud tema tööülesannetest lähtuv infoturbealane juhendamine.

10.2.4. IT-spetsialist peab pakkuma töötajale esmast abi infotehnoloogiaga seotud küsimuste korral.

11. ERANDITE KOOSKÕLASTAMISE PÕHIMÕTTED

11.1. Infoturbe poliitikat tagavast käitumisest kõrvalekaldumine üldjuhul lubatud ei ole. Kui kõrvalekaldumine on möödapääsmatu, tuleb see igakordselt juhtkonna liikme poolt kooskõlastada. Ilma kooskõlastuseta ei tohi turvajuhendist kõrvale kalduda.
11.2. Enne kooskõlastust tuleb erandolukorda ja riske põhjalikult hinnata. Kui riski hinnatakse talutavaks, tohib erandi kooskõlastada, seejuures peab kooskõlastus olema ajaliselt piiratud.

12. SANKTSIOONIDE PÕHIMÕTTED

12.1. Kasutajatelt, kes antud reeglistiku rikkumisega kahjustavad JKHK vara või tekitavad JKHK-le lisakulutusi, võib JKHK nõuda tekitatud kahju hüvitamist. Kokkuleppe mittesaavutamisel toimub kahju hüvitise sissenõudmine seadusega sätestatud korras.
12.2. Antud reeglistiku rikkumisel on JKHK juhtkonnal õigus rikkujat karistada distsiplinaarkorras vastavalt töötajate distsiplinaarvastutuse seadusele.
12.3. Turvanõuete rikkumisel kohaldatakse süüdlasele karistusi vastavalt kehtivale seadusandlusele.

13. INFOTURBE POLIITIKA MUUDATUSED

13.1. Infoturbe poliitika vaadatakse infoturbe töörühma poolt üle vähemalt kord aastas.
13.2. Infoturbe poliitikat muudetakse kooli direktori käskkirjaga infoturbe töörühma ettepanekul.

14. MÕISTED

14.1. Eriruum – arhiivi-, serveri- , side- ja elektrikilbiruum või mõni muu ruum, mille funktsioon on infoturbe seisukohast kriitilise tähtsusega.
14.2. Infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem koos selle normaalseks talituseks vajalike vahendite, ressursside ja protsessidega.
14.3. Infoturve – turvameetmete loomise, valimise ja rakendamise protsesside kogum.
14.4. Infovara – teave, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid.
14.5. Juurdepääs – võimalus kasutada informatsiooni või andmeid.
14.6. AK – asutusesiseseks kasutamiseks mõeldud teave.
14.7. Kasutaja – isik, kellele on väljastatud JKHK infosüsteemi kasutajatunnus.
14.8. Konfidentsiaalsus - teabe, toote või teenuse kättesaamatus volitamata isikutele, olemitele või protsessidele.
14.9. Terviklus – teabe, toote või teenuse õigsus ja täielikkus, lubamatute muudatuste puudumine.
14.10. Käideldavus – teabe, toote või teenuse omadus olla õigel ajal kättesaadav ja kasutuskõlblik.
14.11. Logi – teabe töötluskäigu taastamist ja kontrolli võimaldavad andmed.
14.12. Oht – süsteemi või organisatsiooni kahjustada võiva soovimatu intsidendi potentsiaalne põhjus.
14.13. Pääsuvahend – võti, sissepääsukaart, uksekood või valvekood.

14.14. Tulemüür – tark- ja riistvara tehnilistest komponentidest koosnev süsteem arvutivõrkude turvaliseks ühendamiseks.
14.15. Turvaintsident – iga teenuse/protsessi mitteplaneeritud katkestus või kõrvalekalle, mis mõjutab teenuse/protsessi käideldavust ja/või terviklust ja/või konfidentsiaalsust.
14.16. Viirus - arvutiprogramm, mis on kirjutatud spetsiaalselt selleks, et arvutit ilma selle kasutaja teadmata kahjustada või kuritarvitada.