KINNITATUD
Dir kk nr 1-1/19
03.07.2019. a.

INFOTURBEPOLIITIKA

1. ÜLDSÄTTED

1.1. Rakendusala

1.1.1. Infoturbe poliitika kehtib kogu Tartu Kunstikoolis (edaspidi TK).

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

1.1.3. Infoturbe poliitika hõlmab TK

1.1.3.1. personali;

1.1.3.2. õpilased;
1.1.3.3. infrastruktuuri;
1.1.3.4. andmeid ja dokumentatsiooni;
1.1.3.5. IT-riistvara;
1.1.3.6. tarkvara;
1.1.3.7. sidesüsteeme.

1.1.4. Infoturbe poliitika puudutab TK suhtlust ja seoseid järgmiste subjektidega:
1.1.4.1. partnerid, kliendid;
1.1.4.2. riigiasutused ja kolmandad isikud;
1.1.4.3. meedia ja avalikkus.

1.2. Infoturbepoliitika eesmärk ja põhimõtted

1.2.1. Infoturbe eesmärgiks on TK infosüsteemis töödeldava informatsiooni tervikluse, käideldavuse ja konfidentsiaalsuse tagamine.

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

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

1.3. Õiguslikud raamtingimused

1.3.1. TK lähtub infoturbe alases tegevuses põhiliselt
1.3.1.1. isikuandmete kaitse üldmäärusest;
1.3.1.2. avaliku teabe seadusest;
1.3.1.3. töötervishoiu ja tööohutuse seadusest;
1.3.1.4. tuleohutuse seadusest;
1.3.1.5. teistest infosüsteemidega seotud seadustest (näiteks riigisaladuse seadus, arhiiviseadus, digitaalallkirja seadus, elektroonilise side seadus jne);
1.3.1.6. konkreetse infosüsteemi valdkonna kohta käivast seadusandlusest.

1.4. TK sõltuvus IT kasutamisest

1.4.1. TK põhiprotsesside toimimine ilma IT-ta on oluliselt raskendatud.

1.4.2. Enamuse TK töötajate esmaseks töövahendiks on arvuti.

2. INFOTURBE ORGANISATSIOON JA VASTUTUS

2.1. Juhtkond

2.1.1. Üldvastutus infoturbe tagamise eest on direktoril.

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

2.2. Infoturbe töörühm

2.2.1. Infoturbe töörühma määrab direktor.

2.2.2. Infoturbe töörühma kohustused on:
2.2.2.1. infoturbe järjepidev planeerimine ja korraldamine;
2.2.2.2. infoturbega seotud dokumentatsiooni koostamise ja menetlemise korraldamine;
2.2.2.3. infoturbe järelevalve teostamine;

2.2.2.4. infoturbealase teadlikkuse tõstmise korraldamine;

2.2.2.5. infoturbeintsidentide menetlemine;

2.2.2.6. juhtkonnale perioodiliste ja sündmustepõhiste aruannete esitamine.

2.3. Valdkondade juhid

2.3.1. Valdkondade juhtide kohustused on:

2.3.1.1. infovarade käideldavuse, tervikluse ja konfidentsiaalsuse ning infovarade kaitset reguleerivate õigusaktide kehtestamine ja täitmise tagamine juhitavas üksuses;

2.3.1.2. kõigi vahetute alluvate teavitamine kehtivatest infoturbega seotud haldusaktidest;

2.3.1.3. kõigi vahetute alluvate infosüsteemi kasutamise õiguspärasuse ja infosüsteemi toimimise õiguspärasuse jälgimine;

2.3.1.4. infoturbealastest probleemidest teatamine, vastavate ettepanekute tegemine ja tagasiside andmine turbealaste haldusaktide toimimise kohta.

2.4. Töötajad

2.4.1. Kõik TK töötajad vastutavad

2.4.1.1. oma töövaldkonnas infoturbe eesmärkide saavutamise ja kehtestatud kordade täitmise eest;

2.4.1.2. kõigi talle määratud kasutajatunnuste kasutamisel sooritatud tegude eest;

2.4.1.3. kõigi tema kasutusse antud infosüsteemi komponentide säilimise ning turbe eest.

3. INFORMATSIOONI TUNDLIKKUS JA RISKID

3.1. Informatsiooni tundlikkuse tasemed

3.1.1. TK-s kasutuselolev informatsioon jaguneb avalikuks informatsiooniks ning asutusesiseseks kasutamiseks (edaspidi AK) mõeldud informatsiooniks.

3.1.2. AK-ks mõeldud informatsioon on informatsioon, mis sisaldab

3.1.2.1. eriliigilised isikuandmeid;

3.1.2.2. isikuandmeid;

3.1.2.3. seadusest tulenevad kaitsed.

3.2. Ülevaade asutuse informatsioonist

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

3.2.3. Olulisemad andmekogud on:

3.2.3.1. G Suite

3.2.3.2. Riigitöötaja Iseteenindusportaal - RTIP

3.2.3.3. Eesti koolide haldamise infosüsteem - EKIS

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. Raamatupidamine - SAP

3.2.3.8. Moodle

3.2.3.9. Koduleht

3.2.4. Andmekogude omadused ja kasutus on kirjeldatud andmekogude registris.

3.3. Isikuandmete töötlemistoimingute registreerimine

3.4. Arvestust tuleb pidada isikuandmete töötlemistoimingute üle, mis sisaldab järgmisi elemente:

3.4.1. vastutav töötleja;

3.4.2. töötlemise eesmärk;

3.4.3. andmesubjektide kategooriad ja isikuandmete liigid;

3.4.4. andmete säilitamise tähtajad;

3.4.5. turvameetmete kirjeldus.

3.5. Riskihalduse strateegia

3.5.1. Kehtivate turvameetmete otstarbekust ja efektiivsust tuleb regulaarselt kontrollida.

3.5.2. Enne uue infotehnoloogilise lahenduse (riist- ja tarkvara) kasutuselevõttu tuleb läbi viia analüüs ja hinnata selle mõju terviksüsteemile.

3.6. Turvaintsidentide haldus

3.6.1. Turvaintsident on iga teenuse/protsessi mitteplaneeritud katkestus või kõrvalekalle, mis mõjutab teenuse/protsessi käideldavust ja/või terviklust ja/või konfidentsiaalsust.

3.6.2. Turvaintsidendist teavitamine on iga töötaja kohustus.

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

3.6.4. Turvaintsidendid tuleb dokumenteerida ja teostada nende järelhindamist. Järelhindamine peab andma ülevaate turvameetmete parandamise vajadustest.

4. RIIST- JA TARKVARA TURVE

4.1. Üldturve

4.1.1. Riist- ja tarkvara soetamise, paigaldamise, infosüsteemi lülitamise, konfigureerimise ja haldamise eest vastutab IT spetsialist.

4.1.2. Paigaldatav riist- ja tarkvara peab ühilduma TK infosüsteemiga ning vastama vähemalt TK-s kehtestatud riist- ja tarkvara standardile.

4.1.3. Riist- ja tarkvara konfiguratsioon peab olema kaitstud volitamatute muudatuste eest.

4.2. Pääsu reguleerimine

4.2.1. Juurdepääs infovaradele tuleb anda ainult tööalase vajaduse ja vastutuse alusel.

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

4.2.3. Kasutada tuleb turvalisi paroole. Paroole tuleb regulaarselt vahetada.

4.2.4. Kõigi arvutitega tohib saada tööd alustada alles pärast kasutajanime ja parooli sisestamist.

4.2.5. Riist- ja tarkvara algparoolid peavad olema muudetud.

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

4.2.7. Töösuhte lõppedes tuleb kõik pääsuõigused viivitamatult tühistada.

4.2.7.1. Vajadusel kooskõlastatakse erandid vastavalt punktile 11

4.2.8. Pääsuõiguste vastavust tegelikele vajadustele tuleb regulaarselt kontrollida.

4.3. Kurivaratõrje

4.3.1. Kurivaratõrje programmid peavad hõlmama kogu TK IT süsteemi.

4.3.2. Kurivaratõrje programmid peavad töötama reaalajas.

4.3.3. Viirusekirjeldusi tuleb igapäevaselt otstarbeka regulaarsusega uuendada.

4.3.4. Enne installeerimist ja kasutusele võtmist tuleb kogu hangitud tarkvara üle kontrollida kurivaratõrje 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. Kaughaldustarkvaraga 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 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 ja kasutamiseks kinnitada juhtkonna poolt.

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 TK-s kehtestatud turvanõudeid.

4.8.3. Kaugtööks kasutatavas arvutis peab reaalajas töötama kurivaratõrje 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 talletada.

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 128 bitti. Minimaalne lubatav võtme pikkus asümmeetrilise krüptosüsteemi kasutamisel on 1024 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 TK ruume, peavad olema krüpteeritud.

4.12.4. Kasutada ei tohi rakendusi, mis saadavad parooli üle avaliku võrgu krüpteerimata kujul.

5. VÕRGU TURVE

5.1. Infrastruktuur

5.1.1. Võrk peab olema jagatud vajaduse järgi väiksemateks alamvõrkudeks ning peab 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. TK 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 TK 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 ja 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 TK sisevõrgus olevatest arvutitest.

5.3.2. Interneti kasutamine TK-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 kurivaratõrje ja rämpsposti kontrollile.

5.4.3. Meiliklient tuleb konfigureerida nii, et kirja manusfaile ei käivitataks kogemata, käivitus peab nõudma kinnitust.

5.4.4. Aktiivsisuga failide edastamine e-posti teel peab olema takistatud.

6. TEGEVUSE KATKEMATUS

6.1. Varundamine

6.1.1. Turvakoopiaid tuleb teha kõigist TK 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 meediatele 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 poolt kehtestatud nõudeid.

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 komponendiga teisest, vähem oluliste funktsioonidega süsteemist.

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. Varu-tööruumid puuduvad.

7. INFOVAHETUSE TURVE

7.1. Üldturve

7.1.1. AK tunnistatud andmete edastamisel peab olema välistatud andmete tervikluse ja konfidentsiaalsuse kadu.

7.1.2. Isikuandmete ja eriliigiliste isikuandmete edastamine kolmandatele isikutele peab toimuma vastavalt avaliku teabe seadusele, isikuandmete kaitse üldmääruse (IKÜM) 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 tunnistatud informatsiooni edastamine telefoni teel on keelatud.

7.2.2. AK tunnistatud informatsiooni käsitlemisel tuleb välistada volitamata isikute pealtkuulamise võimalus.

7.3. E-kiri

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

7.4. Kiirsuhtlustarkvara

7.4.1. Elektrooniline kiirsuhtlus toimub Skype´i tarkvaraplatvormil.

7.4.2. Kiirsuhtlustarkvara abil on failide vahetamine keelatud.

7.5. Infovahetus väliste andmekandjate (nt CD-ROM, 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 tunnistatud informatsioon tuleb andmevahetuse jaoks krüpteerida. Peale andmevahetuse teostamist tuleb informatsioon andmekandjalt turvaliselt kustutada või andmekandja füüsiliselt hävitada.

7.5.4. Saadud andmekandjatele tuleb teha viirusekontroll.

8. IT-TEENUSTE VÄLJASTTELLIMINE

8.1. Kolmandad osapooled ja väljasttellimine

8.1.1. Väljasttellimine ei tohi halvendada TK infoturbe olukorda.

8.1.2. Väliseid lepingupartnereid tohib lubada töid teostama peale lepingute allakirjutamist, kus on sätestatud töövõtja kohustused, õigused ja vastutus.

8.1.3. Leping peab sisaldama üheselt mõistetavaid ja mõõdetavaid teenuste kirjeldusi.

8.1.4. Kõik kokkulepped peavad olema kirjalikult fikseeritud.

8.1.5. Lepingu lõppemine peab olema täpselt reguleeritud. Lepingu lõppemisel peab olema viimase tööpäeva lõpuks tagatud kõigi kolmanda osapoole valduses olevate pääsuvahendite tagastamine ning pääsuõiguste tühistamine.

9. FÜÜSILINE TURVE

9.1. Uksed ja aknad

9.1.1. Hoonete sissepääsud peavad olema väljaspool õppetöö aega lukustatud.

9.1.2. Kui tööruumides kedagi ei ole, peavad tööruumide uksed olema lukustatud ja aknad turvaliselt suletud.

9.2. Sissepääs ruumidesse

9.2.1. Sissepääs ruumidesse tuleb tagada vastavalt tööalase vajaduse ja vastutuse alusel.

9.2.2. Välistatud peab olema uste ja akende kaudu volitamata sissepääs hoonetesse ja ruumidesse. Rakendada tuleb sissepääsupiiranguid ja sissemurdmisvastaseid kaitsesüsteeme.

9.2.3. Tagantjärgi peab olema võimalik kindlaks teha kelle poolt, millal ja milliseid uksi on avatud.

9.3. Pääsuvahendite haldus

9.3.1. Pääsuvahendeid tuleb hoida viisil, mis välistaksid nende volitamata kasutamise, kadumise või varguse.

9.3.2. Pääsuvahendite jagamise üle tuleb pidada dokumenteeritud arvestust.

9.3.3. Kaartide ja koodide kasutajad peavad olema identifitseeritavad.

9.3.4. Üldvõti väljastatakse töötajale ainult erandjuhul ja selle väljastamine peab olema juhtkonna poolt heaks kiidetud.

9.3.5. Olemas peavad olema hoonete kõikide uste tagavaravõtmed. Tagavaravõtmeid tuleb hoida viisil, mis välistaks nende volitamata kasutamise.

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

9.3.7. Vastutab administraator.

9.4. Valve

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

9.4.2. Ruumid peavad olema vastavalt otstarbele jagatud valvetsoonideks.

9.4.3. Valvetsoonist viimasena lahkuv töötaja peab aktiviseerima valve.

9.4.4. Valvesignalisatsiooni süsteemi tuleb regulaarselt kontrollida, samuti kontrollida alarmi korral.

9.4.5. Turvaalarm peab olema suunatud turvafirmasse.

9.5. Tuleohutus

9.5.1. Ruumid peavad olema varustatud tuletõrjesignalisatsiooniandurite ga, mis peavad olema paigaldatud vastavalt tuletõrje eeskirjadele ja valmistaja nõuetele.

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

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

9.5.4. Tuletõrjealarm tuleb automaatselt edastada häirekeskusesse.

9.5.5. Personali tuleb instrueerida tuleohutusest ja kasutama esmaseid tulekustutusvahendeid.

9.6. Eriruumide turve

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

9.6.2. Eriruumid peavad olema varustatud valve- ja tuletõrjesignalisatsiooniga ning sobivate tulekustutusvahenditega.

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

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

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

9.6.6. Eriruumides peab olema tagatud õhutemperatuuri reguleerimine.

9.7. Töökohtade turve

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

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

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

9.8. Andmekandjate turve

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

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

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

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

9.8.5. Arhiveerimisele kuuluvaid andmeid sisaldavad andmekandjad tuleb arhiveerida, arhiveerimistähtaja möödumisel aga hävitada.

9.8.6. Arhiveeritud andmekandjaid tuleb säilitada vastavalt seadusandlusele ja asjaajamis-korrale.

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

9.9. Mobiilse aparatuuri turve

9.9.1. Mobiiltelefonide ja sülearvutite turbe eest vastutavad nende valdajad.

9.9.2. Turvariskide maandamiseks nt võimaliku infolekke korral sülearvuti sattumisel kõrvaliste isikute valdusse, peab konfidentsiaalse sisuga tööalane informatsioon sülearvutis olema krüpteeritud.

9.10. Muu aparatuuri turve

9.10.1. Mittemobiilset aparatuuri tohib TK hoonetest välja viia ainult IT spetsialisti loal.

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

9.11. Hoolde- ja remonditööd

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

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

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

9.12. Puhastusteenistujad

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

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

9.12.3. Puhastusteenistujaid tuleb informeerida IT-ga ja dokumentidega ümberkäimise eeskirjadest.

9.12.4. Eriruumidesse tohib puhastusteenistujaid lubada ainult koos volitatud saatjaga.

9.13. Kolimine

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

10. PERSONALI TURVE

10.1. Tööle võtmine ja töölt vabastamine

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

10.1.2. Kandidaadid tuleb valida vakantsete töökohtade ametijuhendite alusel.

10.1.3. Ametijuhendisse tuleb lülitada asjakohased turvanõuded, sh tähtajatu konfidentsiaalsuskohustus ja kehtiva infoturbe dokumentatsiooni järgimise kohustus.

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

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

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

10.1.7. Töötajaga töösuhte lõpetamisel tuleb tagada viimase tööpäeva lõpuks kõikide 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 turvateadlikkuse 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 koolitus.

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

11. ERANDITE KOOSKÕLASTAMINE

11.1.1. Turvajuhenditest kõrvalekaldumine üldjuhul lubatud ei ole. Kui on vajalik mõnest turvajuhendist kõrvalekaldumine, tuleb see igakordselt juhtkonna liikme poolt kooskõlastada. Ilma kooskõlastuseta ei tohi turvajuhendist kõrvale kalduda.

11.1.2. Enne kooskõlastust tuleb erandolukorda ja riske põhjalikult hinnata. Kui riski hinnatakse talutavaks, tohib erandi kooskõlastada, seejuures peab kooskõlastus olema ajaliselt piiratud.

11.1.3. Erandid ja nende kooskõlastamised peavad olema dokumenteeritud.

12. SANKTSIOONID

12.1.1. Kasutajatelt, kes antud reeglistiku rikkumisega kahjustavad TK vara või tekitavad TK-le lisakulutusi, võib TK nõuda tekitatud kahju hüvitamist. Kokkuleppe mittesaavutamisel toimub kahju hüvituse sissenõudmine seadusega sätestatud korras.

12.1.2. Antud reeglistiku rikkumisel on TK juhtkonnal õigus rikkujat karistada distsiplinaarkorras.

12.1.3. Turvanõuete rikkumisel kohaldatakse süüdlasele karistusi vastavalt kehtivale seadusandlusele.

13. INFOTURBEPOLIITIKA MUUDATUSED

13.1.1. Infoturbepoliitika vaadatakse juhtkonna poolt üle vähemalt kord aastas.

13.1.2. Infoturbepoliitikat muudetakse, kui

13.1.2.1. seda nõuavad turvaseire tulemused;

13.1.2.2. oluliste tehniliste, organisatsiooniliste, õiguslike vm sisemiste või väliste muudatuste korral selgub muudatuste vajadus.

14. MÕISTED

14.1.1. Eriruum – arhiivi-, serveri- , side- ja elektrikilbiruum.

14.1.2. Infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talituseks vajalike vahendite, ressursside ja protsessidega.

14.1.3. Infoturve – turvameetmete loomise, valimise ja rakendamise protsesside kogum;

14.1.4. Infovara – informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid.

14.1.5. Juurdepääs - Juurdepääsu all mõistetakse informatsiooni või andmete kasutamise võimaldamist.

14.1.6. Kasutaja – isik, kellele on väljastatud TK infosüsteemi kasutajatunnus.

14.1.7. Konfidentsiaalsus – andmete konfidentsiaalsus on andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile.

14.1.8. Käideldavus – andmete käideldavus on eelnevalt kokku lepitud vajaliku ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus (st vajaliku ja nõutaval ajahetkel ja vajaliku ning nõutava aja jooksul) selleks volitatud isikule või tehnilisele vahendile.

14.1.9. Logi – info töötluskäigu taastamist ja kontrolli võimaldavad andmed.

14.1.10. Oht – süsteemi või organsatsiooni kahjustada võiva soovimatu intsidendi potentsiaalne põhjus.

14.1.11. Pääsuvahend – võti, sissepääsukaart, uksekood või valvekood.

14.1.12. Terviklus – andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

14.1.13. Tulemüür – tark- ja riistvara tehnilistest komponentidest koosnev süsteem arvutivõrkude turvaliseks ühendamiseks.

14.1.14. Turvaintsident - iga teenuse/protsessi mitteplaneeritud katkestus või kõrvalekalle, mis mõjutab teenuse/protsessi käideldavust ja/või terviklust ja/või konfidentsiaalsust.

14.1.15. Viirus - arvutiprogramm, mis on kirjutatud spetsiaalselt selleks, et arvutit ilma selle kasutaja teadmata kahjustada või kuritarvitada.

15. KÄESOLEVA DOKUMENDI STAATUS

15.1.1. Kinnitatud 03.07.2019 seisuga.