Kammeri Kooli infoturbe põhimõtted

1. Infoturbe eesmärk

1.1. Infoturbe põhimõtted määratlevad Kammeri Kooli (edaspidi Kool) suunised oma infovarade turvalisuse tagamisel. Kool püüab piisavate turvameetmete rakendamisega kõige tõenäolisemate ohtude tingimustes vältida oma infovarade ja maine kahjustamist ning tagada katkestusteta tegevuse oma ülesannete saavutamiseks. Valitud turvameetmed (organisatsioonilised, füüsilised ja infotehnilised) aitavad täita õigusaktidest tulenevaid turvanõudeid ning olema majanduslikult õigustatud ning nende häiriv toime kooliperel tegevusele peab olema võimalikult väike.

2. Rakendusala

2.1. Infoturbe põhimõtted kehtivad Kammeri Kooli füüsilistes asukohtades ning muus kohas kaugtöö korral.

2.2. Infoturbe põhimõtteid on kohustatud järgima ja täitma kõik koolipere liikmed, praktikandid ning kooli lepingulised partnerid, kes on volitatud töötleja rollis.

3. Infoturbe tagamise põhimõtted

3.1. Infoturbe põhimõtted sõnastavad turbe eesmärgid, nende saavutamise suunised, üldise turbe korralduse ja -strateegia ning peamiste turvamehhanismide rakendamise poliitikad. Kool lähtub oma infoturbe korraldamisel:

3.1.1. IT-halduse headest tavadest,

3.1.2. Otstarbekuse piires kolmeastmelisest etalonturbe standardi ISKE juhistest, mis on leitavad veebiaadressilt https://www.ria.ee/et/kuberturvalisus/iske/juhendid-ja-materjalid.html

3.2. Infoturbe põhieesmärgiks on kaitsta andmeid ohtude eest, tagada andmete väärtuste ja omaduste säilimine, tagada talituse jätkuvus, minimeerida talitusriski, tagada õigusaktidele vastavus ja säilitada asutuse kuvand.

3.3. Infoturbe valdkonda reguleeriv sisemine regulatsioon on kirjeldatud Kooli infosüsteemi kasutamise eeskirjas.

4. Infoturbe korraldamine

4.1. Infoturbealast tööd korraldab ja koordineerib IT-tugi.

4.2. Infovara kasutaja vastutab infoturbe meetmete rakendamise eest, täidab infoturbe nõudeid ja rakendab asjakohaseid turvameetmeid.

5. Infoturve ja riskianalüüs ning riskihaldus

5.1. Kooli infovarade ja neile rakenduvate turvameetmete rakendatus vaadatakse läbi vähemalt kord aastas või suuremate muutuste ja turvaintsidentide korral. Läbivaatust koordineerib ja

analüüsib IT-tugi. Sellest tulenevalt tehakse ettepanekud koolijuhile infoturbealaste otsuste tegemiseks.

6. Infovarad

6.1. Varade üle peab arvestust IT-tugi koostöös haridustehnoloogiga.

7. Turvarisk

7.1. Ohuallikaks infosüsteemile võib olla:

7.1.1. puudus infrastruktuuris – ebapiisav kaitse füüsilise ohu eest (nt elektrikatkestus, kuum, külm, vesi) või turbe füüsilise meetme osaline rakendamine;

7.1.2. puudus infotehnoloogias – süsteemi või seadme tõrge (nt serveririke või võrguühenduse katkestus); seadme paigutus; süsteemi jõudlus; ülepingutatud turvameede;

7.1.3. puudus töös − viga, mida töötaja teeb turvanõuete järgimisel (nt annab edasi ligipääsuõiguse või taotleb tarbetu ligipääsuõiguse, ei järgi töö- ja eraasjade lahususe põhimõtet);

7.1.4. puudus töökorralduses – juhtum, kus järgitakse turvanõuete täitmise reegleid puudulikult või ei täideta neid; kasutusjuhend või süsteemikirjeldus on ebaselged või puudub; süsteemile juurdepääsu reguleerimise vahend ehk parool on nõrk või ebapiisav; arvutisse on paigaldatud volitamata tarkvara;

7.1.5. turvaründed;

7.1.6. vääramatu jõud.

8. Turvariskide vähendamine

8.1. Riskide vähendamiseks võetakse kasutusele:

8.1.1. füüsilised meetmed ruumidele (uste, akende ja lukkudega seotud abinõud);

8.1.2. organisatsioonilised meetmed töötajatele (protseduurireeglid, korrad ja eeskirjad turvanõuete täitmiseks);

8.1.3. infotehnoloogilised meetmed infosüsteemidele ja andmekogudele (ligipääsuõiguste andmise ja kasutamisega, viirusetõrjega, krüpteerimisega, varukoopiate tegemise ja ID-kaardi kasutamisega seotud abinõud).

9. Personaliturve

9.1. Personali turbe eesmärk on tagada lojaalne ja turvateadlik koolipere. Inimeste turvateadlikkuse tõstmiseks viiakse läbi erinevaid koolitusi.

9.2. Turvateadlikkuse saavutamiseks ning oma igapäeva töös lähtub töötaja töökorraldusereeglitest, ametijuhendist, asjaajamiskorrast ja infosüsteemi kasutamise korrast.

9.3. Töötaja lahkumisega seotud tegemised on kirjeldatud infosüsteemi kasutamise korras.

10. IT-turve

10.1. Riist- ja tarkvara peab tagama vajaliku info käideldavuse, tervikluse ja konfidentsiaalsuse.
10.2. Riist- ja tarkvara haldab või seda korraldab IT-tugi, kelle ülesanne on tagada süsteemide kvaliteetne toimimine, kasutajatoe pakkumine ja jätkusuutlikkus.
10.3. Teenustaseme lepingute sõlmimisel fikseeritakse teenuse kvaliteedi tagamiseks teenustaseme käideldavus.
10.4. Arvutivõrgu kasutamist reguleerib infosüsteemi kasutamise kord.

11. Üldturve

11.1. Üldturbe eesmärk on luua tehnilised võimalused ja keskkond infoturbe korraldamiseks. Üldturvet korraldab majandusjuhataja või tema ülesandeid täitev isik. Üldturvet reguleerivad töökorralduse reeglid ja tuleohutuseeskiri.
11.2. Ligipääs ruumidele on tagatud ja korraldatud tööalase vajaduse ja vastuse alusel. Võtmete jagamisel peetakse kirjalikku arvestust juhiabi poolt.
11.3. Olulistes ruumides on paigaldatud valvesignalisatsioon.
11.4. Eraldi lukustatavas tööruumis tuleb viimasel väljujal aknad sulgeda ja uks lukustada.
11.5. Väline hoolde- ja remondipersonal lubatakse ruumidesse koos saatjaga.

12. Andmed

12.1. Andmekaitse eesmärk on tagada andmete töötlemise turvalisuse vastavus kehtivatele õigusaktidele. Kõigile andmetele on määratud omanik. Andmete omanik on isik, kes vastutab andmete loomise, klassifitseerimise, kasutamise, ligipääsude reguleerimise ja administreerimise eest. IT-tugi korraldab andmete haldamise ja administreerimise andmete omaniku eest. Andmete töötlemisel järgitakse andmekaitse reegleid.
12.2. Vajadusel kaasatakse andmetöötluse turvalisuse tagamiseks ja turbemeetmete ülevaatuseks andmekaitse- ja küberturvalisuse asutusi.
12.3. Andmete töötlemise põhimõtted on avaldatud kooli kodulehel.

13. Turvaintsident

13.1. Turvaintsidentide käsitlemise poliitika eesmärk on tagada turvaintsidentidest tuleneva kahju minimeerimine. Turvaintsident on mistahes kõrvalekalle süsteemide normaalsest talitlusest. Turvaintsidendist tuleb koheselt teatada IT-toele. IT-tugi tagab turvaintsidendile reageerimise, registreerimise ja hilisema analüüsimise.

14. Järelevalve

14.1. Infoturbe põhimõtete elluviimise aluseks on kõik ülalviidatud eeskirjad ja juhendid, mille eest vastutab IT-tugi.