KINNITATUD
19.11.2026 direktori käskkirjaga nr 1-2/26/57

Infoturbe poliitika

Tallinna Muusika- ja Balletikool

Sisukord

1. Sissejuhatus....2
2. Infoturbe eesmärgid....3
3. Infoturbe organisatsioon ja juhtimine....4
4. Dokumentatsiooni halduse korraldus ja infoturbega seotud dokumendid....5
5. Riskihaldus....6
6. Infoturbemeetmete rakendamine....13
7. Infoturbe käigushoid....14
8. Infoturbeprotsessi täiustamine....14
9. Turvateadlikkus ja -koolitus....15
10. Infoturbeintsident....15
11. Infoturbe juhtimine partnerite juures....165

1. Sissejuhatus

1.1. Kooli infoturbeprotsess on algatatud käesoleva poliitika kehtestamisega.

1.2. Infoturbe poliitika on Tallinna Muusika- ja Balletikooli (edaspidi kool) infoturbe keskne dokument ning on osa üldisest juhtimissüsteemist, mille laiem eesmärk on tagada koolile pandud ülesannete täitmine.

1.3. Infoturbe poliitika eesmärk on määratleda põhimõtted ja korraldus kooli infoturbe tagamisel ning mille abil tagatakse nõuetekohane infovarade kaitse. Poliitika kehtib kõikidele asutuse töötajatele ja õpilastele, samuti puudutab see asutuse suhtlust ja seoseid teiste riigiasutuste, partnerite ning kolmandate isikutega. Infoturbe käsitlusala hõlmab kõiki asutuse omandis, valduses või kasutuses olevaid varasid ja infovarasid, sealhulgas infosüsteeme, andmeid, infotehnoloogilist taristut ning muid asutuse ülesannete täitmiseks ja tegevuse järjepidevuse tagamiseks vajalikke ressursse. Infosüsteemi turbeviisiks on valitud põhiturve, mille rakendamisel lähtutakse infosüsteemi turbevajadustest ning tagatakse asjakohaste turvameetmete abil teabe ja infosüsteemi konfidentsiaalsus, terviklus ja käideldavus.

1.4. Kooli juhtkond peab infoturbe rakendamist eluliselt tähtsaks ning teeb selle järgimise kohustuslikuks kõigile töötajatele. Korraga on kohustatud tutvuma kõik kooli töötajad, samuti töövõtu või muu lepingu alusel teenust osutavad isikud ning kõik teised isikud, kes osalevad asutuse töös (edaspidi töötaja).

1.5. Infoturbejuhtimisega seotud kohustusi ja vastutust ning muudatusi ja otsuseid kommunikeeritakse järjepidevalt huvitatud osapooltele, samuti tagatakse asutuse infoturbeteadlikkus läbi töötajate koolitamise.

1.6. Kooli infoturbe korraldamisel järgitakse nii Eesti Vabariigis kehtivat regulatsiooni kui ka asutuse sisemist töökorraldust, sh:

- isikuandmete kaitse seadust;
- haridusseadust;
- põhikooli-ja gümnaasiumiseadust
- töötervishoiu ja tööohutuse seadust;
- töölepingu seadust;

- tuleohutuse seadust;
- küberturvalisuse seadust;
- keeleseadust;
- konkreetse infosüsteemi valdkonna kohta käivat seadusandlust ja standardeid;
- asutuse tegevuse iseärasust.

2. Infoturbe eesmärgid

2.1. Kooli infoturbe üldine eesmärk on toetada koolile pandud ülesannete ja eesmärkide täitmist, tagades infovarade konfidentsiaalsuse, terviklikkuse ja käideldavuse ning kaitstes kooli töötajate ja õpilaste isikuandmeid:

2.1.1. Käideldavus – tagada infosüsteemide talitluspidevus vastavalt kokkulepitud tingimustele, sh kriisiolukorras.

2.1.2. Terviklus – tagada et töödeldav informatsioon on usaldusväärne ja vigadeta kogu tarkvara elutsükli jooksul ning kontrollida regulaarselt andmete volitamata muutmise puudumist.

2.1.3. Konfidentsiaalsus – kaitsta konfidentsiaalset teavet selgelt määratletud nõuete kohaselt ja tagada üldiseks kasutamiseks mõeldud teabele avalikkuse juurdepääs.

2.1.4. Isikuandmed – kaitsta kooli õpilaste ja töötajate isikuandmeid tagades konfidentsiaalsuse reeglite järgimist.

2.2. Kooli infoturbe vahetuteks eesmärkideks on tagada:

2.2.1. Kooli igapäevane asjaajamine ja infovahetus - luua stabiilne, turvaline ja töökindel töö- ja õppekeskkond, mis vastab töötajate ja õpilaste ootustele ja tagab asutuse igapäevaste tegevuste katkematu toimimise.

2.2.2. Kooli ja koolipere vaheline infovahetus - tagada avaliku info kättesaadavus ja avalike teenuste kiire ning tulemuslik osutamine kodanikele.

2.2.3. Andmete konfidentsiaalsus, terviklus ja käideldavus - tagada asutusele töötlemiseks või hoidmiseks antud andmete kaitse volitamata juurdepääsu, muutmise ja hävitamise eest.

2.2.4. Infoturbe integreerimine asutuse tegevustesse - tagada infoturbe nõuete arvestamine kõikides asjakohastes kooli tegevustes ja otsustusprotsessides, et vähendada riske ja kaitsta infovarasid ja isikuandmeid.

2.2.5. Kooli töötajate ja õpilaste teadlikkuse suurendamine infoturbega seotud kohustuste ja vastutuse osas - tagada kõikide töötajate ja õpilaste teadlikkus oma infoturbega seotud kohustustest ja vastutusest ning korraldada regulaarseid koolitusi ja teavitustegevusi, sealhulgas: tagades kõikidele töötajatele infoturbekoolituse vähemalt kord aastas.

2.2.6. Tõhus riskihaldus - hinnata ja vähendada kooliinfoturbe riske süsteemselt, kasutades selleks E-ITS standardeid ja parimaid praktikaid.

2.2.7. Tõhus intsidendihaldus - tagada kooli kõikidele infoturbeintsidentidele reageerimine ja lahendamine vastavalt kokkulepetele.

2.2.8. Jätkusuutlik areng ja pidev parendamine - jälgida ja parendada pidevalt kooli infoturbe meetmeid ja protsesse, et need vastaksid muutuvatele ohtudele ja tehnoloogiatele.

3. Infoturbe organisatsioon ja juhtimine

3.1. Infoturbe toimimiseks on vajalik, et organisatsioonis oleks kindlalt määratletud turbealased rollid ja vastutused. Infoturve on organisatsiooni kollektiivne tegevus ja kõikide töötajate kohustus. Iga töötaja peab teadma, milles seisneb tema panus infoturbesse.
3.2. Kooli infoturbejuhi ülesandeid täidab lepinguline partner CISOaaS teenusena .
3.3. Infoturbealane vastutus jaguneb üldiseks ja konkreetseks vastutuseks:

3.3.1. Üldine vastutus – Kõikidel asutuse töötajatel ja õpilastel on üldine infoturbealane vastutus, mis seisneb antud valdkonda reguleerivate kordade järgimises ning infoturbeintsidentidest teavitamises.
3.3.2. Konkreetne vastutus - Konkreetne, st rolli- või ametikohapõhine vastutus järgib organisatsiooni struktuurilist ülesehitust, üldist töökorraldust, tegevusvaldkondi ja kehtivaid delegeerimispõhimõtteid. Sealhulgas:

- Asutuse juht kannab lõppvastutust, vastutades mh. kooli infoturbe tagamise eest ja korraldades infoturbe poliitika kehtestamise ja kaasajastamise.
- Osakondade juhatajad korraldavad asutuse juhi delegeerimisel infoturbe juhtimist oma vastutuse piirides.
- Infoturbejuht vastutab infoturbe põhimõtete, standardite, juhiste ja muude vajalike alusdokumentide väljatöötamise, ülevaatamise ja jõustamise eest. Samuti koordineerib infoturbe meetmete rakendamist ja kontrollimist.

3.3.3. Kooli direktor ja osakondade juhatajad peavad olema kaasatud infoturbega seotud kesksetesse küsimustesse.
3.3.4. Infoturbe erandid ja jääkriskid peavad olema teada, hinnatud ja aktsepteeritud kooli juhtkonna poolt.
3.3.5. Infoturbe eest vastutav isik peab olema teadlik kõikidest IT valdkonnaga seotud projektidest.

3.4. Kooli juhi vastutus

3.4.1. Määratleb valdkonna tähtsamad eesmärgid;
3.4.2. Kehtestab asutuses antud valdkonda puudutava regulatsiooni;
3.4.3. Kinnitab infoturbe tööplaani;
3.4.4. Osaleb infoturbe olulisusest teavitamises;
3.4.5. Tellib sõltumatuid hinnanguid infoturbe valdkonnale;
3.4.6. Vajadusel aktsepteerib võimalikud jääkriskid;
3.4.7. Tagab infoturbe jätkusuutlikuks arenguks vajalikud eelarvelised vahendid.

3.5. Osakonna juhataja vastutus

3.5.1. jälgib infoturbe eeskirjade täitmist ja vastavust enda vastutusalas.

3.6. Infoturbejuhi vastutus:

3.6.1. Infoturbe poliitika, standardite, juhiste ja muude vajalike alusdokumentide väljatöötamine, ülevaatamine ja jõustamine.
3.6.2. Infoturbe meetmete rakendamine ja kontrollimine ning asjakohaste tähelepanekute, järelduste ja soovituste tegemine, säilitades objektiivsuse ja sõltumatuse kõikide infoturbejuhi ülesannete täitmisel
3.6.3. Infoturbealaste aruannete esitamine kooli juhile ja regulaarselt informatsiooni edastamine infoturbe olukorra kohta kooli juhtkonna koosolekutel.
3.6.4. infoturbealaste otsuste tegemine oma volituste piires ning infoturbe olulisusest teavitamises osalemine.
3.6.5. Infosüsteemide taasteplaanide koostamine ja testimine;
3.6.6. Koostöö töötajatega ja isikuandmete töötlemise eest vastutava isiku ja/või andmekaitse spetsialistiga;
3.6.7. Viivitamatu teavitamine Riigi Infosüsteemide Ameti küberintsidentide käsitlemise osakonda (CERT-EE) olulistest turvaintsidentidest;
3.6.8. Vastutab turvaintsidentide lahendamise ja vastavate meetmete rakendamise korraldamise eest.
3.6.9. Töötajate teavitamine turvareeglitest, nende nõustamine infoturbealaselt ning vajadusel töötajatele koolituste korraldamine üldise turvateadlikkuse tõstmiseks;
3.6.10. Uute töötajate informeerimine IT- ja infoturbe-alastes küsimustes.

3.7. **Töötajate vastutus**

3.7.1. oma töövaldkonnas infoturbe eesmärkide saavutamise ja kehtestatud kordade täitmise eest;
3.7.2. kõigi talle määratud kasutajatunnuste kasutamisel sooritatud tegude eest;
3.7.3. kõigi tema kasutusse antud infosüsteemi komponentide ja IT-seadmete säilimise ning turbe eest.
3.7.4. olema teadlikud ja järgima isikuandmete kaitse reegleid.
3.7.5. viivitamatu teavitamine infoturbejuhti infoturbeintsidentsidest.

3.8. **Õpilase vastutus**

3.8.1. kehtestatud kordade järgimise eest;
3.8.2. kõigi talle määratud kasutajatunnuste kasutamisel sooritatud tegude eest;
3.8.3. kõigi tema kasutusse antud infosüsteemi komponentide ja IT-seadmete säilimise ning turbe eest.
3.8.4. olema teadlikud ja järgima isikuandmete kaitse reegleid.
3.8.5. Viivitamatu teavitamine infoturbejuhti infoturbeintsidentidest.

4. Dokumentatsiooni halduse korraldus ja infoturbega seotud dokumendid

4.1. Infoturbeprotsessi jätkusuutlikkuse ja jälgitavuse aluseks on dokumenteerimine.
4.2. Dokumenteeritakse: a) infoturbeprotsessi alusdokumendid ja väljatöötluse kulg, b) otsused, sh infoturbe meetmete rakendusplaan, c) infoturbesündmused, d) asutuse reaktsioon sündmustele ja otsustele, e) muu teave, mida asutus peab vajalikuks säilitada infoturbe halduse toimivuse huvides.
4.3. Asutuse juht kinnitab ning avaldab asjakohased infoturbega seotud poliitikad, korrad ja juhised (edaspidi regulatsioon) kõikidele töötajatele ja õpilastele.
4.4. Kooli infoturbekontseptsiooni keskme moodustavad käesolev infoturbe kord, IT-teenuste kasutaja eeskiri ja IT-teenuste osutamise eeskiri. Vajadusel kehtestatakse nimetatud dokumentide alusel täiendavaid juhiseid. Infoturbe lähimad eesmärgid ja ülesanded fikseeritakse infoturbe tööplaanis, arvestust infovarade üle koos vajalike kaitsetarvetega peetakse infovarade registris ning riskihaldust riskiregistris

4.4.1. IT-teenuste kasutaja eeskiri kehtestab üldnõuded kooli IT-süsteemide kasutajatele, et tagada infoturbenõuete täitmine.
4.4.2. IT-teenuste osutamise eeskiri määratleb nõuded operatiivsete kontrollidele (nt varundamine, kaitse pahavara eest, tehniliste haavatavuste haldamine, krüptograafialased juhtelemendid, side turvalisus), mille alusel kehtestatakse täiendavad tehnilised protseduurid.

5. Riskihaldus

5.1. **Üldsätted**

5.1.1. Kooli riskihalduse eesmärgiks on toetada asutuse põhitegevuste eesmärkide saavutamist, vähendades või hoides ära soovimatuid riske ning tagades järjepideva infoturbe juhtimissüsteemi (ISMS) arengu.
5.1.2. Riskide haldamisel kasutab asutus E-ITS metoodikat, mis lähtub põhimõttest et infoturvaohud ja kaitstavad varad on organisatsioonide puhul tüüpsed. See võimaldab rakendada eelanalüüsitud meetmekomplekte, mis katavad tüüpsete sihtobjektide riskihalduse ja infoturvavajadused. E-ITSi etalonturbe kataloog (kättesaadav https://eits.ria.ee/) on käesoleva poliitika lahutamatu osa.
5.1.3. Riskide vähendamiseks rakendatakse E-ITS turvameetmeid vastavalt infovaradele määratud turvaklassile ja E-ITS rakendusjuhendile.
5.1.4. Kui mõnda E-ITS turvameedet ei ole võimalik või otstarbekas täita, tuleb leida alternatiivsed meetmed riski vähendamiseks või kinnitada meetme täitmata jätmisega tekkinud jääkriski aktsepteerimine asutuse juhi või tema poolt volitatud isiku poolt.
5.1.5. Riskihindamise protsessi käigus määratakse riskitasemed, millest lähtuvalt otsustatakse tuvastatud riskide edasine käsitlemisvajadus. Iga maandamistegevuse puhul tuleb määrata vastutaja, tähtaeg, lisanduv ressursivajadus ja juhtkonna otsuse või informeerimise vajadus. Oluline on mõelda, milliseid maandamistegevusi saab valdkonna enda ressurssidest ja enda vastutuse piires otsustada ning millised vajavad juhtkonna otsust või vähemalt teadlikkust.
5.1.6. Asutus määrab lähtuvalt oma tegevuse spetsiifikast kaitsetarbe määramise põhimõtted, sh kahjustsenaariumid, riski aktsepteerimise kriteeriumid, kaitsetarbe komponendid (vähemalt konfidentsiaalsus, terviklus, käideldavus ehk C-I-A) ja täpsustab kaitsetarbe määramise skaala.

5.1.7. Etalonturbe kataloogi protsessimoodulrühmade kõik moodulid kaasatakse rakendusplaani. Mooduli käsitlemata jätmine peab olema põhjendatud. Süsteemimoodulid rakendatakse vastavuses kaitseala määratlusega.

5.1.8. Riskihalduse käik ja tuvastatud või määratud meetmete rakendamise otsused dokumenteeritakse korratavuse ja võrreldavuse eesmärgil.

5.2. Riskihalduse protsess

5.2.1. Riskihaldus koosneb kahest põhielemendist: riskihindamine (s.o riskianalüüs) ja riskide käsitlemine.

5.2.2. Riskihalduse protsess tervikuna hõlmab järgmisi aspekte:

- infovarade tuvastamine ja klassifitseerimine,
- infovara väärtuse määramine,
- ohtude tuvastamine ja hindamine,
- varade haavatavuste tuvastamine ja hindamine konkreetsete ohtude suhtes,
- riski kindlaksmääramine (rünnaku eeldatavad tagajärjed),
- riskide vähendamise meetmete tuvastamine,
- riskide vähendamise meetmete prioriseerimine strateegiast lähtuvalt.

5.2.3. Tuvastatud riskid registreeritakse riskide registris. Iga riski kohta registreeritakse järgnev:

- riski kirjeldus (üksikasjad selle põhjuste ja mõjude kohta),
- riski elementide hinnang käideldavuse, konfidentsiaalsuse ning tervikluse lõikes,
- riski koondhinnang,
- olemasolevate riskimaandamistehnikate kirjeldus,
- riski realiseerumise tagajärgede hindamine,
- jääkriski hinnang,
- soovitus riski maandamiseks,
- tegevuskava kirjeldus,
- ülevaade tegevuskava rakendamise hetkeseisust.

5.2.4. Riskihalduse protsessi järjepideva ja regulaarse toimimise ja arengu eest vastutab asutuse juht.

5.3. Riskihindamine

5.3.1. Riskihindamise (analüüsi) eesmärk on selgitada välja infovaradele ja protsessidele suunatud võimalikud ohud ja nõrkused, hinnata ohtude realiseerumise tõenäosust ja nendega kaasnevaid kahjusid. Samuti tuleb riskianalüüsi käigus kontrollida määratletud turbe-eesmärkide vastavust

põhitegevuse vajadustele ning vajadusel eesmärke ajakohastada, uuendades infoturbe poliitikat või selle alusel antud dokumente.

5.3.2. Analüüsi lähtekohaks on sihtobjektide (nii infovara kui äriprotsessi) kaitsetarbe vajadus. Äriprotsessi kaitsetarbe hindamisel lähtutakse eelkõige selle raames töödeldava teabe kaitsetarbest, infovara kaitsetarbe hindamisel kasutatakse struktureeritud analüüsi kooskõlas E-ITS metoodikaga. Täiendavalt arvestatakse võimalikke väliseid infoturbealaseid nõudeid (nt lepingud, regulatsioon).

5.3.3. Kaitsetarbe määramise eelduseks on täielik ja ajakohane ülevaade asutuse infovaradest, mis omakorda loob arusaama kaitseala ulatusest. Seetõttu on vajalik tagada täpne ülevaade infovaradest alates arvelevõtmise hetkest kuni nende kasutusest eemaldamiseni.

5.3.4. Kaitsetarvet hinnatakse kvalitatiivselt, kasutades maatriksit kolmeastmelisest mõjuskaalast (normaalne, suur, väga suur) ning turvalisuse kolmest põhikomponendist (konfidentsiaalsus, terviklus ja käideldavus). Normaaltaset ületava kaitsetarbe korral rakendatakse E-ITS välist riskianalüüsi ja määratakse lisaturvameetmed.

5.3.5. Riskihindamise vahetuks väljundiks on riskiregister, kuhu pannakse kirja tuvastatud riskid ning kokku lepitud maandamistegevused. Protsessi teiseseks tulemiks on erinevad tööpaberid, kus on fikseeritud erinevate etappide protsess ja tulemid. Need tööpaberid selgitavad teistele osapooltele protsessi käiku ja kaalutlusi, samuti pakuvad need selgitusi asutuse juhile, kelle pädevuses on riskihinnangute lõplik aktsepteerimine.

5.3.6. Infoturbejuht vastutab kasutatava riskihindamise metoodika sobivuse ja ajakohasuse eest, koordineerib, toetab ja kontrollib analüüsiga seotud protsesside läbiviimist.

5.3.7. Asutuse juht vastutab riskihindamise protsessi toimivuse, piisavuse ja eesmärgipõhisuse ning riskide aktsepteerimise ja meetmete õigeaegse rakendamise eest.

5.4. **Riskikäsitlus**

5.4.1. Riskikäsitluse eesmärk on valida sobivad meetmed ohtude realiseerumise mõju vähendamiseks, hinnata nende tasuvust ja otsustada aktsepteeritava jääkriski suurus. Riskikäsitluse aluseks on jääkriski hinnatav suurus ning vahetuks tulemuseks meetmete rakendusplaan. Kui jääkriski tase ei ole vastuvõetav, rakendatakse täiendavaid kontrolle, et vähendada riske vastuvõetava tasemeni.

5.4.2. Riskikäsitluse käigus otsustatakse riski a) aktsepteerimine, b) maandamine kontrollimeetmete rakendamise abil, c) vältimine või d) üleandmine läbi kindlustuskaitse või lepingu abil kolmandale osapoolele.

5.4.3. Maandatavad või üleantavad riskid tuuakse välja rakendusplaanis, mis sisaldab riskide järgi prioriseeritud meetmeid koos ajakavaga. Rakendusplaanis on igale riskile määratud vastutav töötaja, nimetatud riski käsitlemiseks tegevused ja vajalikud ressursid.

5.4.4. Riskide maandamiseks rakendatakse vaikimisi E-ITS etalonturbes kirjeldatud meetmeid, neile lisanduvad etalonturbe välised meetmed (vt. „E-ITS väline riskikäsitlus“). Riskile rakendatud peamine riskikäsitlusviis tuleb dokumenteerida.

- Kohalduvad meetmed tuvastatakse määratud kaitsetarbe alusel rakenduvate E-ITS kaitsemoodulite abiga. Moodulist sihtobjekti turvameetmete tuvastamisel arvestatakse: a) turbeviisi (põhiturve, standardturve või tuumikturve); b) sihtobjekti kaitsetarvet; c) meetme seost infoturbeprotsessi elutsükliga.
- E-ITS kataloogi protsessimoodulite kõik rühmad käsitletakse väljajättudeta, st iga väljajätt peab olema põhjendatud. Süsteemimoodulid rakendatakse vastavuses kaitseala määratlusega.
- E-ITS etalonturbes kirjeldatud meetmete osas määratakse moodulite rakendamise järjekord lähtuvalt infoturbe poliitika põhimõtetest ja reaalsetest vajadustest. Tehnilised meetmed rakendatakse kõigile kaitseala sihtobjektidele. Organisatoorsed meetmed integreeritakse asutuse kõigisse protsessidesse.

5.5. Asutuse juht määratleb riskide aktsepteerimise kriteeriumid, aktsepteerib jääkriskid ning kinnitab rakendusplaani.

5.6. Vara eest vastutav töötaja vastutab õigeaegse, sisulise ja piisava riskikäsitlusprotsessi läbiviimise eest konkreetse vara osas. Osakonna juht vastutab oma haldusala piires olevate protsesside ja rakenduste riskikäsitlusprotsessi läbiviimise osas.

5.7. Infoturbejuht hindab tuvastatud ja määratud meetmete:

5.7.1. ressursside ühekordseid ja korduvaid kulusid;

5.7.2. sobivust, teostatavust, piisavust, võimalikku toime efektiivsust ja meetmete omavahelisi mõjusid.

5.8. Infoturbejuht koordineerib, toetab ja kontrollib riskikäsitlusega seotud protsesside läbiviimist ning monitoorib tegevusplaanide täitmist. Samuti tagab infoturbejuht rakendusplaani ajakohasuse tervikuna.

5.9. **E-ITS väline riskikäsitlus**

5.9.1. Etalonturbe välisesse riskikäsitlusse suunatakse sihtobjektid, mille jaoks puudub E-ITS etalonturbe kataloogis sobiv moodul. Täiendavalt suunatakse välisesse riskikäsitlusse sihtobjektid, kui sihtobjekti puhul on täidetud üks järgmistest tingimustest:

- kaitsetarve on suur või väga suur;
- kaitsetarve on määramata või ebaselge;
- kasutusviisid ei ole vastavuses etalonturbe kataloogi moodulite kirjeldustega;
- etalonturbe kataloogi meetmed osutuvad turvaeesmärkide täitmisel puudulikuks (s.o jääkrisk pole aktsepteeritav).

5.9.2. Etalonturbe väline riskihaldus määrab sihtobjektidele lisaturvameetmeid sihtobjekti kaitsetarbest ja infoturbe eesmärkidest lähtuvalt. Rakendusplaanis kajastatakse tuvastatud lisaturvameetmed.

5.9.3. Riskianalüüsi tegemisel võib kasutada kas kvalitatiivset või kvantitatiivset hindamist. Kvalitatiivsel hindamisel kasutatakse riskistsenaariumeid (vt E-ITS) ning kvantitatiivsel hindamisel varapõhiseid nõrkuseid.

5.9.4. Riskianalüüsis hinnatakse kahe faktori koosmõju - (1) riskisündmuse tagajärge ja (2) riskisündmuse võimalikkust (tõenäosust) - mille korrutise tulemusel moodustub (3) riskitase:

5.9.5. Riskisündmuse tagajärgede analüüsi käigus kirjeldab riski omanik, mis juhtub kui risk realiseerub ehk kui oht nõrkuse ära kasutab. Tagajärgede analüüsis tuleb välja tuua kõik võimalikud riski realiseerumise tagajärjed, hindamisel lähtutakse järgnevatest kategooriatest:

Tagajärg	**Vähene mõju**	**Piiratud mõju**	**Oluline mõju**	**Kriitiline mõju**
Skoor	1	2	3	4
	Tegevused on häiritud, aga eesmärkide saavutamine on võimalik ilma täiendavate ressurssideta.	Tegevused on oluliselt häiritud, aga eesmärkide saavutamine on võimalik siseste ressursside ümberjaotamise teel, mis ei mõjuta teiste eesmärkide saavutamist.	Tegevused on oluliselt häiritud ning eesmärkide saavutamiseks on vaja oluliselt lisaressursse.	Asutusele seatud eesmärke ja põhiprotsesse ei ole võimalik saavutada.
Õppe- ja loometegvuse jätkuvus				
Õilaste ja töötajate turvalisus				
Õiguslik mõju				
Finantsiline mõju				
Mainekahju				

5.9.6. Riskisündmuse võimalikkuse analüüsi käigus tuvastatakse riski realiseerumise tõenäosus. Tõenäosuse hindamiseks on võimalik saada infot erinevatest allikatest, näiteks statistika või eksperthinnang. Riskide tõenäosuse (võimalikkuse) hindamisel lähtutakse järgnevatest kategooriatest:

Tõenäosuse hinnang	**Skoor**	**Kriteeriumid**
Vähetõenäoline	1	Riski realiseerumine on pigem teoreetiline või praktikas väga harv; esineb ca 1 poliitika 10 aasta jooksul.
Võimalik	2	Riski realiseerumine on võimalik, aga praktilised näited on üksikud; võib juhtuda lähiaastatel.
Tõenäoline	3	Eksisteerivad tõendusmaterjalid selle kohta, et riski realiseerumine on tõenäoline; võib juhtuda aasta jooksul.
Kindel	4	Risk on varasemalt realiseerunud või on vältimatu; võib juhtuda päevade ja nädalate jooksul.

5.9.7. Riskitase väljendab riski olulisust tagajärgede ja nende võimalikkuse kombinatsioonina. Riskitasemete skaala eesmärk on aidata riskiomanikel otsustada riski edasise käsitlemise (nt aktsepteerida, maandada) vajaduse ja meetodi üle:

Riskitase		**Tegevus**
1-4	Madal	Riski aktsepteeritakse, seiratakse vähemalt poliitika aastas.
5-8	Keskmine	Riskiga tegeletakse võimaluse korral. Juhul, kui otsustatakse aktsepteerida riski, siis on see vajalik riskiomaniku poolt kirjalikult põhjendada. Riski seiratakse vähemalt poliitika aastas.
9-12	Kõrge	Risk vajab tegelemist. Riskiomanik peab panema paika tegevuskava. Riski seiratakse vähemalt poliitika 6 kuu jooksul.
13-16	Kriitiline	Risk vajab kohest juhtkonna otsust ning tegelemist. Riski omanik peab viima riski juhtkonda, seda selgitama ning tegema ettepanekud riski käsitluseks. Riski seiratakse ja tegevusi tehakse vastavalt juhtkonna otsuses toodud tähtaegadele

5.9.8. Asutuses on riski aktsepteerimine lubatud ainult juhul, kui riskiskoor jääb alla 13 ning täiendavad meetmed riski maandamiseks ei ole võimalikud või otstarbekad.

5.9.9. Maandatavad või üleantavad riskid tuuakse välja rakendusplaanis, mis sisaldab riskide järgi prioriseeritud meetmeid koos ajakavaga. Rakendusplaanis on igale riskile määratud vastutav töötaja, nimetatud riski käsitlemiseks tegevused ja vajalikud ressursid.

5.9.10. Vara eest vastutav töötaja vastutab õigeaegse, sisulise ja piisava riskikäsitlusprotsessi läbiviimise eest. Osakonna juht vastutab oma haldusala piires olevate protsesside ja rakenduste riskikäsitlusprotsessi läbiviimise osas.

5.9.11. Infoturbejuht vastutab kasutatava E-ITS välise riskihalduse metoodika sobivuse ja ajakohasuse eest, koordineerib, toetab ja kontrollib sellega seotud protsesside läbiviimist.

6. Infoturbemeetmete rakendamine

6.1. Infoturbemeetmete rakendamise protsess

6.1.1. Tehnilised meetmed rakendatakse kõigile kaitseala sihtobjektidele. Organisatsioonilised meetmed lõimitakse organisatsiooni kõigisse protsessidesse.

6.1.2. Asutus hindab tuvastatud ja määratud meetmete: a) ressursside ühekordseid ja korduvaid kulusid; b) sobivust, teostatavust, piisavust, võimalikku toime efektiivsust ja meetmete omavahelisi mõjusid.

6.1.3. Meetmed rakendatakse vastavalt kinnitatud rakendusplaanile. Meetmete rakendatuse määr ning rakendamise etapid dokumenteeritakse ajakohase ülevaate ning hilisema kontrollitavuse eesmärgil.

6.1.4. Asutuse juht teadvustab ja aktsepteerib regulaarselt jääkriskid ning nende alusel kinnitab rakendusplaani.

6.1.5. Rakendusplaanis toodud kaitsemeetmete rakendamise ning rakendusplaani ajakohasuse eest vastutab infoturbejuht koos meetme eest vastutajaga.

6.1.6. Infoturbejuht nõustab ja koordineerib meetme rakendamist ning hindab rakendusprotsessi piisavust.

6.1.7. IT-juht vastutab meetmete tehnilise juurutamise eest.

6.2. Infoturbe rakendusplaan

6.2.1. Infoturbe rakendusplaanis tuuakse välja kõik planeeritavad infoturbe meetmed, seda nii lühi- kui pikaajalises vaates. Lisaks põhjendatakse E-ITS-is nimetatud meetmete osas mitterakendatavad meetmed. Rakendusplaaniga tagatakse meetmetes kirjeldatud korduvate ja regulaarsete tegevuste tõendatavus, võrreldavus, järjepidevus ja õigeaegsus.

6.2.2. Infoturbe meetmete rakendusplaan sisaldab vähemalt:

- rakendamisele kuuluvaid E-ITS turvameetmeid koos meetme koodi, nimetuse ja meetme teostatuse määraga;
- rakendamisele kuuluvaid etalonturbe väliseid turvameetmeid koos meetme teostatuse määraga (vajadusel);
- meetme rakendamise eest vastutajaid;
- meetme rakendamisega seotud tähtaegu;
- meetme osalise rakendamise puhul täpsustavaid selgitusi, mis osas on meede täitmata;
- meetme mitterakendamise puhul asutuse juhi aktsepteeringut meetmete mitterakendamisest tulenevatele jääkriskidele.

6.2.3. Rakendusplaani hoitakse pidevalt ajakohasena, minimaalselt vaadatakse kavandatavaid meetmeid üle kord aastas. Seejuures on infoturbe meetmete rakendusplaanist võimalik saada hetkeseisu kajastavat väljavõtet igal ajahetkel.

6.2.4. Asutuse juht tagab rakendusplaani meetmete piisavuse ning nende ajakohasuse ja õigeaegse täitmise, sealhulgas vastutab rakendusplaanis

toodud tegevustele ressursside eraldamise eest ning kinnitab rakendusplaani eelarve.

6.2.5. Infoturbe meetmete rakendusplaani täitmise eest vastutab meetme rakendamise eest määratud töötaja.

6.2.6. Infoturbejuht vastutab rakendusplaani haldamise eest.

7. Infoturbe käigushoid

7.1. Asutus tagab infoturbeprotsessi ning -meetmete pideva ja jätkusuutliku toimimise ning arendamise. Jälgitakse ja mõõdetakse:

7.1.1. infoturbe eesmärkide ning -meetmete sobivust ja tõhusust;

7.1.2. ressursside kasutamist.

7.2. Asutus reageerib muutustele oma eesmärkides, regulatsioonide nõuetes, lepingulistes kohustustes ning ümbritsevas infoturbeolukorras.

7.3. Tulemusi ning järeldusi kasutab asutus infoturbeprotsessi ja -meetmete täiustamise ning muutmise ettepanekute koostamisel.

8. Infoturbeprotsessi täiustamine

8.1. Asutus tagab sissejuhatava- ja täiendjuhendamise, mille käigus selgitatakse uutele ja olemasolevatele töötajatele infoturbealaseid nõudeid teadlikkuse suurendamiseks.

8.2. Asutus kontrollib perioodiliselt vähemalt poliitika aastas infoturbeprotsessi, infoturbe poliitika ja infoturbe eesmärkide sobivust ja asjakohasust.

8.3. Rakendatud turvameetmete järjepideva täitmise, vastavuse ning asjakohasuse tagamiseks viiakse läbi regulaarseid tegevusi, sealhulgas a) turvameetmete hooldamine, b) välistele nõuetele vastavuse kontrollimine, c) sisemiste regulatsioonide läbivaatused ja uuendamine, d) töökeskkonna igapäevane seiramine, e) infoturbe perioodilise vastavuskontrolli läbiviimine, f) muudatustele reageerimine, g) riskide hindamine ja maandamistegevuste rakendamine, ja h) infoturbeintsidentide käsitlemine ja neist õppimine.

8.4. Asutus korraldab regulaarselt infoturbeprotsessi tulemite ja seisundi sõltumatu läbivaatuse. Läbivaatusel hinnatakse asutuse infoturbehalduse vastavust a) E-ITS nõuetele); b) asutuses kehtivale infoturbe korrale.

8.4.1. Läbivaatuse läbiviijaks on kas sise- või välisaudiitor või käsitlusala suhtes asjakohase pädevusega sõltumatu töötaja. Väline turvanõuete audit tellitakse vastavalt vajadusele, kuid mitte harvemini E-ITSis kehtestatud korras. Läbivaatusel välditakse rakendaja ning kontrollija rollide huvide konflikti.

8.4.2. Asutus määrab sõltumatu läbivaatuse käsitlusala ja eesmärgid. Läbivaatuse läbiviimisel arvestatakse:

- asutuse eesmärke;
- regulatsioonide nõudeid ning lepingulisi kohustusi;
- asutuse infoturbe poliitikat ja eesmärke;

- varasemate läbivaatuste tulemusi.

8.4.3. Audiitori hinnang on tõend asutuse infoturbe toimivuse kohta kooskõlas E-ITS nõuetega

8.4.4. Läbivaatuse tulemused ja ettepanekud dokumenteeritakse täiustamise ja jälitatavuse eesmärgil. Tulemusi arvestatakse organisatsiooni protsesside täiustamisel.

8.5. Infoturbejuhi vastutusel on infoturbe protsessi käigushoidmine ja täiustamisega seotud tegevuste korraldamine, sh turvameetmete haldus, regulatsioonide regulaarne läbivaatus, vastavusauditite tellimine (minimaalselt 1x 3a jooksul) ja läbiviimise koordineerimine, töökeskkonna igapäevase seire koordineerimine, infoturbe perioodiline vastavuskontroll, infoturbe intsidentide käsitlemise koordineerimine, töötajate koolitamine (koostöös personaliosakonnaga) ning muudatusvajaduste tuvastamine ja nendele reageerimine.

8.6. Asutuse juht vastutab infoturbe protsessi käigushoidmise ja täiustamise eest tervikuna.

9. Turvateadlikkus ja -koolitus

9.1. Ajakohase turvalisuse tagamiseks ja infoturbe tundmise parandamiseks on vajalikud infoturbekoolitused ja teadlikkus infoturbe alal. Selleks on kool välja töötanud infoturbe koolituste kava, mille täitmine on töötajatele kohustuslik. Täitmist jälgib kooli juhtkond.

9.2. Dokumentatsiooni läbiviidud koolituste ja seal osalenud töötajate kohta säilitatakse personaliosakonna poolt vähemalt 2 aastat, pädevustõendeid kuni nende aegumiseni.

9.3. Kooli IT personal on kohustatud hoidma ennast kursis tema valdkonnas ametikohal aktuaalse infoturbealase teabega. Juhul kui selleks on vajalik koolitusel osalemine, annab töötaja sellest teada kooli juhile.

9.4. Lisaks asutuses tehtavatele koolitustele peaks võimaluse korral IT-osakond osalema erihuvigruppides või foorumites, et:

- parandada teadmisi parimate tavade kohta ja olla kursis asjakohase turvateabega;
- tagada infoturbekeskkonna mõistmine aktuaalne ja täielik;
- saada varakult hoiatusi rünnakute ja haavatavustega seotud hoiatuste, nõuannete ja plaastrite kohta;
- juurdepääs infoturbe erinõuannetele;
- jagada ja vahetada teavet uute tehnoloogiate, toodete, ohtude või haavatavuste kohta;
- pakkuda infoturbe intsidentidega tegelemisel sobivaid kontaktpunkte.

10. Infoturbeintsident

10.1. Iga töötaja on kohustatud temale teatavaks saanud infoturbeintsidendist ja selle ohust esimesel võimalusel teavitama infoturbejuhti. Infoturbeintsidentide lahendamine toimub infoturbejuhiga kooskõlastatud põhimõtete alusel.
10.2. Infoturbeintsidendiks loetakse sündmus või olukord, mis ohustab või kahjustab infovara konfidentsiaalsust, terviklust või kättesaadavust.
10.3. Intsidentide lahendamine toimub infoturbejuhi koordineerimisel, kes korraldab asjakohase reageerimise. Turvaintsidente käsitletakse viisil, mis võimaldab minimeerida ja/või piirata turvaintsidentidest tekkida võivaid kahjusid ning taastada rakenduste ja süsteemide töö aktsepteeritava aja jooksul.
10.4. Infoturbeintsidendi lahendamiseks on selleks määratud isikul juurdepääsuõigus sellistele kontrolljälgedele ja muule infosüsteemides olevale informatsioonile, mis on situatsiooni lahendamiseks vajalik, välja arvatud sõnumisaladusena käsitletavale informatsioonile.
10.5. Intsidendi lahendamise käigus kogutud informatsioon dokumenteeritakse ja analüüsitakse eesmärgiga vältida sarnaste intsidentide aset leidmist tulevikus ning otsustamaks täiendavate turvameetmete rakendamise vajaduse üle.
10.6. Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo-, distsiplinaarsüüteo või töölepingu rikkumise tunnused, antakse juhtum edasi menetlemiseks vastava menetluse läbiviimise õigust omavale asutusele või isikule. Olulise mõjuga intsidentide korral tuleb teavitada lepingupartnereid vastavalt kokkulepetele.

Teema	**Asutuse nimi**	**Millal on kohustuslik teavitada**	**Kes peab teavitama**
Andmekaitsealane intsident	Andmekaitse inspektsioon	72 tunni jooksul pärast tuvastatud vahejuhtumit	Andmekaitse-ametnik
Infoturbe intsident	Riigi Infosüsteemide Amet	Esimesel võimalusel, kuid mitte hiljem kui 24h jooksul	Infoturbejuht
Juriidiline või lepinguline küsimus	Huvitatud isikud	Vastavalt lepingule	Jurist

10.7. Varaomanikud vastutavad oma valdkonnas olulise teabe kirjeldamise eest kontaktide kohta teiste asutustega, sealhulgas kommunaalteenused, hädaabiteenused, elektritarnijad ning tervishoid ja ohutus, telekommunikatsiooniteenuste ja veekäitlejad.

11. Infoturbe juhtimine partnerite juures

11.1. Kooli infoturbe juhtimissüsteemiga seotud asutuseväliste partnerite poolt asutusele pakutavad protsessid, tooted või teenused peavad olema kontrollitud ja aktsepteeritava kvaliteediga. Selleks kool:

11.1.1. tuvastab kõik väliste partnerite poolt pakutavad protsessid, tooted või teenused, mis on ISMS-i jaoks olulised, sh millised infoturbe aspektid sõltuvad välistest osapooltest või mida need seesmiselt mõjutavad;
11.1.2. kehtestab kontrollid, mis tagavad, et väliselt pakutavad protsessid, tooted või teenused vastavad kooli teabe turvalisuse nõuetele, et hallata ja maandada seotud riske;

11.1.3. viib läbi riskianalüüsi, et a) tuvastada võimalikud turvariskid, mis on seotud väliselt pakutavate protsesside, toodete või teenustega, ning b) hinnata nende mõju kooli infoturbe eesmärkidele;
11.1.4. sõlmib selged ja kõikehõlmavad lepingulised kokkulepped väliste pakkujatega, määratledes kooli infoturbe nõuded ja ootused;
11.1.5. rakendab regulaarset monitoorimis- ja ülevaatusprotsessi, et tagada väliste pakkujate vastavus kokkulepitud turbenõuetele;
11.1.6. määratleb konkreetsed turbekriteeriumid, millele välised pakkujad peavad vastama;
11.1.7. töötab välja situatsiooniplaanid, et kõrvaldada võimalikud häired väliste protsesside, toodete või teenuste pakkumisel. Situatsiooniplaanide eesmärk on tagada teabeturbeprobleemide lahendamise mehhanismide olemasolu väliste pakkujate tegevuste probleemide korral;
11.1.8. loob tõhusad sidekanalid väliste pakkujate vahel infoturbe küsimustes, et teha koostööd turbeprobleemide lahendamiseks ning tagada vastavus kooli infoturbe eesmärkidega.

11.2. Nimetatud eesmärkide täitmiseks tuleb iga koostööpartneri osas viia läbi vähemalt järgmised tegevused:

11.2.1. lepingueelselt hinnata potentsiaalse pakkuja turbetaset;
11.2.2. lepingus ja SLA-des selgelt määratleda infoturbe nõuded;
11.2.3. paika panna regulaarne turbenõuete vastavuse kontrolli protsess;
11.2.4. kokku leppida intsidentidele reageerimise plaan nende tõhusaks lahendamiseks;
11.2.5. paika panna pakkujate tulemuslikkuse ja turvanõuete järgimise monitoorimise protsess;
11.2.6. tagada kirjalik ülevaade kõikidest kehtivatest kontrollimeetmetest.

11.3. Partneritega seotud reeglid täpsustakse vajadusel IT valdkonna korralduse eeskirjaga, täpsemad reeglid tuleb sätestada partnerlepingutes.