NARVA TÄISKASVANUTE KOOL

Riskihalduskord

Kehtestatud direktori käskkirjaga 1-2/26/7 05.02.2026

Sisukord

1. Sissejuhatus 3
2. Mõisted 3
3. Vastutused ja rollid 4
4. IT ja infoturbe riskide halduse põhimõtted 4
5. Riskide kaalutlemise metoodika 5
6. Riskikäsitlus 6
7. E-ITS väline riskikäsitlus 6
8. Lõppsätted 7

1. Sissejuhatus

1.1 Käesoleva riskihalduse korra eesmärk on toetada Narva Täiskasvanute Kooli põhitegevuste (õppetöö ja kooli haldustegevuse) toimimist, vähendades või ennetades IT- ja infoturbega seotud riske ning tagades infoturbe juhtimissüsteemi (ISMS) järjepideva arendamise.

1.2 Riskide haldamisel kasutab kool 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.

1.3 Riskide vähendamiseks rakendatakse E-ITS turvameetmeid vastavalt infovaradele määratud kaitsetarbele ja E-ITS rakendusjuhendile.

1.4 Juhul kui mõnda E-ITS turvameedet ei ole võimalik või otstarbekas rakendada, määratakse alternatiivsed meetmed või aktsepteeritakse jääkrisk kooli juhi poolt.

1.5 Kooli peamised kaitset vajavad infovarad on: õppijate ja töötajate isikuandmed; õppeinfosüsteemid; dokumendihaldus ja e-post; kooli IT-taristu ja lõppseadmed.

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. Kooli tegevuse eripärast tulenevalt on peamised kaitset vajavad infovarad, õppijate isikuandmed, õppeinfosüsteemid, personaliandmed ning haridust toetavad IT-süsteemid. Etalonturbe kataloogi protsessimoodulrühmade kõik moodulid kaasatakse rakendusplaani. Mooduli käsitlemata jätmine peab olema põhjendatud. Süsteemimoodulid rakendatakse vastavuses kaitseala määratlusega.

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

2. Mõisted

2.1. Korras kasutatakse mõisteid järgmises tähenduses:

Mõiste	**Selgitus**
Riskihaldus	Omavahel kooskõlalised tegevused organisatsiooni suunamiseks ja juhtimiseks riski suhtes.
Riski kaalutlemine	Koondnimetus riskituvastuse, riskianalüüsi ja riski hindamise protsessidele.
Riskituvastus	Riskiallikate (ohtude), sündmuste ning nende põhjuste ja võimalike tagajärgede kindlaks määramine.
Riski hindamine	Riskianalüüsi tulemite ja riski kriteeriumide võrdlemine, eesmärgiga teha kindlaks, kas riskitase on talutav ning seeläbi aktsepteeritav.
Riskianalüüs	(Eelnevalt tuvastatud) riski iseloomu ja riskitaseme väljaselgitamine.
Riskikäsitlus	Riski muutmise või kõrvaldamise või vältimise protsess; riskihalduse protsessi viimane järk, kus eelnevalt tuvastatud ja kategoriseeritud riskidele valitakse vastavad meetmed.
Nõrkus	Vara, süsteemi või protsessi kavandi, teostuse või käituse nõrk koht või puudus, mille kaudu riskiallikas võib tekitada tagajärjega sündmuse.
Meede	Abinõu, mis muudab riski, üldjuhul eesmärgiga seda vähendada.
Oht	Võimaliku kahjustuse allikas.
Risk	Määramatuse toime organisatsiooni eesmärkidele. Väljendub sündmuse tekkimise tõenäosuse ja kahjutoime (tagajärgede) koosmõjuna. Eksisteerib relevantse ohu ning varaga seotud vastava nõrkuse olemasolul.
Riskitase	Riski või riskide ühendi suurus, väljendatuna tagajärgede ja nende võimalikkuse

	kombinatsioonina.
Jääkrisk	Pärast riskikäsitlust säiliv risk.
Riskinorm	Riskitase või tüüp, mida organisatsioon soovib järgida või säilitada.

3. Vastutused ja rollid

3.1. Koolis ei ole eraldi infoturbejuhi ametikohta. Infoturbejuhi ülesandeid täidab IT eest vastutav isik, arvestades kooli suurust, struktuuri ja tegelikke töökorralduslikke võimalusi.

3.2. Riskihalduse protsess viiakse läbi koostöös kooli juhtkonna, vara ja protsesside omanike ning IT eest vastutava isiku vahel. Detailsemad IT ja infoturbe riskide halduse protsessi rollid ja vastutused on esitatud allpool RACI maatriksis:

	IT eest vastutav isik	**Vara/ Protsessi omanik**	**Juhtkond**
Riskihaldusprotsessi korraldamine	R	I	A
Riskikaalutlemise korraldamine	R	C	I
Riskide tuvastamine	R	C	I
Nõrkuste ja rakendatud meetmete tuvastamine	R	C	I
Riskide hindamine	R	C	I
Riskianalüüsi teostamine	R	C	A
Riskikäsitlusplaani koostamine ja teostamine	R	C	A
Riskikäsitlusplaani kinnitamine	I	I	A
Jääkriski aktsepteerimine	I	I	A
Riskiregistri pidamine ja haldamine	R	I	A
Riskidest raporteerimine	R	I	A

***Tabel 1**. Rollid ja vastutused, RACI maatriks*

- **Teostaja (*responsible – R*)** – täidab tööülesandeid. Igale ülesandele määratakse vähemalt üks isik.
- **Vastutaja (*accountable – A*)** – vastutab tegevuste täitmise eest. Ülesanne on juhtida ja kontrollida teostaja(te) tööd. Ühe ülesande jaoks ei tohiks olla rohkem kui üks vastutaja.
- **Nõustaja (*consulted – C*)** – jagab teavet ja/või annab nõu vastutajatele ja teostajatele. Nõustajaid võivad töö tulemused mõjutada ning nendega suheldakse kogu protsessi vältel.
- **Informeeritav (*informed – I*)** – teavitatakse otsustest ja töötulemustest kas teostaja või vastutaja poolt üldjuhul peale tegevuse lõpetamist.

4. IT ja infoturbe riskide halduse põhimõtted

4.1. Riskihaldus koosneb: riskide tuvastamine, riskianalüüs, riskide hindamine ja riskide käsitlemine.

4.2. Riskianalüüsi eesmärk on hinnata: ohtude realiseerumise tõenäosust; võimalikke mõjusid kooli tegevusele; olemasolevate meetmete piisavust.

4.3. Analüüsi lähtekohaks on sihtobjektide kaitsetarbe vajadus. Kaitsetarvet hinnatakse kvalitatiivselt, lähtudes: konfidentsiaalsusest, terviklusest, käideldavusest (CIA).

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

4.5. Riskihalduse väljundiks on riskiregister, mida uuendatakse vähemalt kord aastas või oluliste muudatuste korral.

4.6. Infoturbejuht või vastutav isik vastutab kasutatava riskihindamise metoodika sobivuse ja ajakohasuse eest, koordineerib, toetab ja kontrollib analüüsiga seotud protsesside läbiviimist.

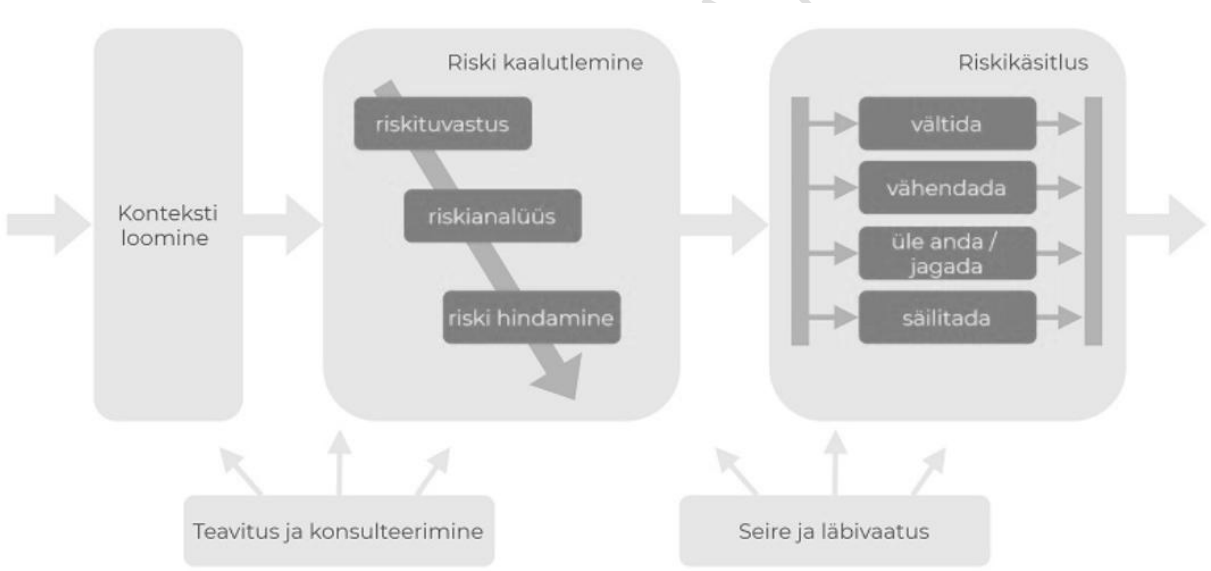
4.7. Asutuse juht vastutab riskihindamise protsessi toimivuse, piisavuse ja eesmärgipõhisuse ning riskide aktsepteerimise ja meetmete õigeaegse rakendamise eest.

5. Riskide kaalutlemise metoodika

5.1. Kool viib läbi IT ja infoturbe riskide kaalutlemist lähtudes E-ITS riskihaldusjuhendis ning ISO/IEC 27005 kirjeldatud metoodikast.

5.2. Kool teostab IT ja infoturbe riskide kaalutlemist vähemalt kord aastas või oluliste muudatuste korral (sh uute infosüsteemide kasutuselevõtt, uute lepingute sõlmimine ning lepingumuudatuste teostamine, uute projektide alustamine), tagamaks, et kõik riskid on tuvastatud, analüüsitud ja tehtud teatavaks juhtimistasandile (juhtkonnale) vastavalt organisatsiooni struktuurile.

5.3. Asutuse IT ja infoturbe riskide kaalutlemise protsess koosneb kolmest sammust, milleks on 1) riskide tuvastamine, 2) analüüs ja 3) hindamine.



***Joonis 1**. E-ITS riskihalduse protsess*[1]

Risk eksisteerib kui on olemas asjakohase ohu ja seotud nõrkuse koosesinemine.

RISK = OHT x NÕRKUS

5.4. Kool viib läbi riskianalüüsi, võttes arvesse teavet infovarade kriitilisusest, protsesside ja varade teadaolevatest nõrkustest.

5.5. Kool analüüsib tuvastatud riske, kasutades kvalitatiivset meetodit. Tõenäosuse hinnang välja toodud skaaladest, hindab asutus iga tuvastatud riski realiseerumise mõju (tagajärge) ning tõenäosust.

[1] https://eits.ria.ee/et/abimaterjalid/riskihaldusjuhend

5.6. Tuvastatud riski realiseerumise tõenäosuse ja mõju alusel määratakse igale tuvastatud riskile riskiklass. Riskiklassi arvutamiseks kasutab asutus järgmist valemit:

RISKIKLASS = TÕENÄOSUS x MÕJU

6. Riskikäsitlus

6.1 Riskikäsitluse eesmärk on valida sobivad meetmed ohtude realiseerumise mõju vähendamiseks ning vähendada riskid vastuvõetava tasemeni.

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

6.3 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.

6.4 Riskide maandamisel kasutatakse vaikimisi E-ITS etalonturbe meetmeid.

6.5 Kooli direktor: määrab riskide aktsepteerimise kriteeriumid; kinnitab riskikäsitlusplaani; aktsepteerib jääkriskid.

7. E-ITS väline riskikäsitlus

7.1 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:

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

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

7.3 Kool kasutab riskisündmuse mõju hindamisel järgmisi kategooriaid:

Tagajärg	**Vähene mõju**	**Piiratud mõju**	**Oluline mõju**	**Kriitiline mõju**
Skoor	1	2	3	4
Õppetöö	Vähene häire, aga eesmärkide saavutamine on võimalik ilma täiendavate ressurssideta.	Tegevused on 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.

Mainekahju	Sisemine rahulolematus	Kaebused	Avalik kriitika	Usalduse kaotus
Rahaline kahju	Puudub	Väike kulu	Märkimisväärne kulu	Eelarveoht
Andmeleke	Üksik viga	Väike leke	Ulatuslik leke	GDPR rikkumine

***Tabel 2**. Riski realiseerumisega kaasneva mõju skaala*

7.4 Riskisündmuse võimalikkuse analüüsi käigus tuvastatakse riski realiseerumise tõenäosus. 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 kord 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.

***Tabel 3**. Tõenäosuse hinnang*

7.5 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 kord aastas.
5-8	Keskmine	Riskiga tegeletakse võimaluse korral. Juhul, kui otsustatakse aktsepteerida riski, siis on see vajalik riskiomaniku poolt kirjalikult põhjendada. Riski seiratakse vähemalt kord aastas.
9-12	Kõrge	Risk vajab tegelemist. Riskiomanik peab panema paika tegevuskava. Riski seiratakse vähemalt kord 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

***Tabel 4**. Riskitaseme skaala*

8. Lõppsätted

8.1 Käesolev riskihalduse kord vaadatakse üle vähemalt üks kord aastas.

8.2 Dokument jõustub kooli direktori kinnitamisel.