Tallinna Tööstushariduskeskus (TTHK)

RISKIHALDUS JA DPIA 2025

Koostatud: 19.09.2025
Koostaja: Tehnoloogia direktor ja IT administraatorid
Koordineerija: Eduard Brindfeldt, Tehnoloogia direktor

---

1. Eesmärk

Riskihalduse ja andmekaitse mõjuhinnangu (DPIA) eesmärk on tuvastada ja hinnata TTHK infosüsteemidega seotud riske, et tagada isikuandmete ja tundliku teabe turvaline töötlemine vastavalt Eesti infoturbestandardile (E-ITS) ja isikuandmete kaitse üldmäärusele (GDPR).

---

2. Ulatus

Riskihaldus hõlmab kõiki infosüsteeme, mida kasutatakse kooli igapäevases tegevuses (õppetöö, haldus, personalitöö, finants, andmeanalüütika).
Mõjuhinnang tehakse süsteemidele, kus töödeldakse isikuandmeid või mis mõjutavad kooli põhitegevuse järjepidevust.

---

3. Riskihaldusprotsess

Riskide juhtimine toimub neljas etapis vastavalt E-ITS ISMS juhendile:

1. **Tuvastamine** – tuvastatakse võimalikud ohud ja nõrkused süsteemides.
2. **Hindamine** – määratakse iga riski tõenäosus ja mõju (madal / keskmine / kõrge).
3. **Leevendamine** – kirjeldatakse meetmed riski maandamiseks või kõrvaldamiseks.
4. **Jälgimine ja ülevaatus** – kontrollitakse regulaarselt meetmete tõhusust.

---

4. Peamised tuvastatud riskid ja maandamismeetmed

Nr	Risk	Tõenäosus	Mõju	Riskitase	Leevendus / meede	Vastutaja
1	Lahkunud töötaja konto jääb aktiivseks	Keskmine	Kõrge	Kõrge	Regulaarne offboarding-audit ja kontode automaatne sulgemine	IT admin
2	Failide jagamine väljaspool organisatsiooni	Keskmine	Kõrge	Kõrge	Avalike linkide keeld, DLP poliitika, koolitused	IT admin
3	Tundlike andmete salvestamine isiklikul OneDrive'il	Madal	Kõrge	Keskmine	Dokumendihaldus SharePointis, juhised töötajatele	IT + osakonnajuhid
4	Andmeleke läbi välise teenuse (nt kolmandad partnerid)	Madal	Kõrge	Keskmine	Lepingulised andmetöötlusklauslid, juurdepääsu kontroll	Direktsioon + jurist
5	Paroolide jagamine kolleegide vahel	Keskmine	Keskmine	Keskmine	MFA, paroolipoliitika, mikrokoolitused	IT
6	Ebapiisav varundamine või taastetesti puudumine	Madal	Kõrge	Keskmine	Planeeritud varundused, taastekatsetused	IT admin
7	Õpilaste isikuandmete kasutamine mitteametlikes keskkondades	Keskmine	Kõrge	Kõrge	Koolitus ja tehniline piirang (ainult SAIS, TAHVEL)	Õppeosakond
8	Phishing ja kasutajaeksimused	Kõrge	Keskmine	Kõrge	MFA, teavitused, simulatsiooniharjutused	IT admin
9	Leevendusmeede - Võrgusegmenteerimine, ligipääsu	Madal	Kõrge	Keskmine	Eraldatud tööstusvõrk (VLAN, SCALANCE)	Tehnikaosakond

	piiramine ainult laborisiseseks kasutamiseks.					
10	Isikuandmete leke füüsiliste dokumentide kaudu	Madal	Keskmine	Madal	Paberandmete hävitamise kord, lukustatud kapid	Kõik osakonnad

5. DPIA – Andmekaitse mõjuhinnang

Tuvastatud töötlustoimingud, mille puhul hinnatakse mõju isikuandmetele:

- õppijate vastuvõtt SAIS süsteemis;
- töötajate andmete säilitamine Active Directory keskkonnas;
- õppijate õppetulemuste ja hinnete haldus TAHVELIS;
- õppetöö jälgimine ja hindamine Moodle'is;
- töötajate andmete töötlemine Riigitöötaja süsteemis;
- töötajate ja õppurite andmete säilitamine M365 keskkonnas.

Riskid andmekaitse seisukohalt:

- isikuandmete liigne kogumine;
- andmete töötlemine väljaspool ametlikku süsteemi;
- ebapiisavad juurdepääsupiirangud;
- andmete säilitamine üle kehtestatud tähtaja;
- ligipääsu andmine kolmandatele osapooltele.

Rakendatud meetmed:

- piiratud ligipääs (õigused rollipõhiselt),
- mitmeastmeline autentimine (MFA),
- DLP (Data Loss Prevention) poliitikad,
- andmete krüpteerimine edastamisel ja puhkeolekus,
- töötajate ja õppurite regulaarne koolitus.

---

6. Riskide järelevalve ja aruandlus

- Riskihaldusdokument vaadatakse üle kord aastas või suurema intsidenti järgselt.
- Jälgimine toimub IT administraatorite ja haridustehnoloogi koostöös.
- Rikkumiste ja kõrvalekallete korral teavitatakse tehnoloogia direktorit ja vajadusel HTM infoturbejuhti.
- Vajadusel koostab kool GDPR artikli 33 kohase rikkumisteavituse Andmekaitse Inspektsioonile.