Tallinna Tööstushariduskeskus (TTHK)

INFOTURVAPOLIITIKA 2025

Kinnitatud: 20.09.2025
Koostaja: Eduard Brindfeldt, Tehnoloogia direktor

---

1. Eesmärk ja ulatus

Infoturvapoliitika eesmärk on tagada Tallinna Tööstushariduskeskuse (TTHK) infosüsteemide, võrkude ja andmete turvaline ning järjepidev toimimine.
Poliitika määrab põhimõtted, vastutused ja eesmärgid infoturbe korraldamisel vastavalt Eesti infoturbestandardile (E-ITS ISMS), GDPR nõuetele ning Küberturvalisuse seaduse §7 ja §8 kohustustele.

Poliitika hõlmab kõiki TTHK infosüsteeme ja andmehaldust, sealhulgas:
Microsoft 365 (SharePoint, OneDrive, Teams),
Active Directory (AD),
TAHVEL, SAIS, Moodle, EHIS, Juhan, Nixor, SAP, PINAL, ERPLY, Kutseregister jt,
ning nende kasutajaid, töötajaid ja õppijaid.

---

2. Infoturbe põhimõtted

- **Konfidentsiaalsus, terviklus ja kättesaadavus** tagatakse süsteemsete ja dokumenteeritud meetmetega.
- Kõigil kasutajatel on unikaalsed kontod ning õigused antakse **piisava minimaalsuse põhimõttel**.
- Tundlikku teavet töödeldakse ainult ametlikes ja turvatud infosüsteemides.
- Lahkunud töötajate ja lõpetanud õppurite ligipääsud suletakse viivitamata.
- Infosüsteemide tegevus on **jälgitav logide kaudu**; rikkumised registreeritakse ja analüüsitakse.
- Töötajatele ja õppuritele viiakse läbi **infoturbealased koolitused** vähemalt kord igas õppeperioodis.
- Kooli infosüsteemide infrastruktuur (serverid, tööjaamad, võrguseadmed) on kaitstud füüsiliselt ja loogiliselt.
- Andmete varundused teostatakse **planeeritud graafiku alusel** ning testitakse taastevõime.

---

3. Vastutused

Roll / funktsioon	Vastutaja	Ülesanne
Infoturbe üldjuhtimine	Tehnoloogia direktor	Üldine vastutus infoturbe juhtimise ja poliitikate täitmise eest
Andmekaitse ja riskihaldus	Tehnoloogia direktor ja haridustehnoloog	GDPR nõuete järgimine, riskianalüüs ja DPIA
Tehniline turve	IT-süsteemi administraatorid ja IT abi	Tehniliste kaitsemeetmete rakendamine, logimine, ligipääsuhaldus
Andmetöötluse vastutajad	Osakondade juhid	Andmete töötlemise korrektsus ja lubatud ulatus
Kasutajad	Kõik töötajad ja õppurid	Infoturbe põhimõtete järgimine igapäevases töös

---

4. Infoturbe juhtimise põhimõtted

Infoturvet juhitakse põhimõttel **planeeri – rakenda – kontrolli – parenda** (PDCA-tsükkel):

1. **Planeerimine:** riskide hindamine ja turvameetmete kavandamine.
2. **Rakendamine:** turvameetmete ja poliitikate kasutuselevõtt.
3. **Kontroll:** sisemine auditeerimine, logianalüüs ja järelevalve.
4. **Parendamine:** tuvastatud puuduste kõrvaldamine ja süsteemi täiustamine.

Infoturbe juhtimine on pidev protsess, mis hõlmab nii tehnilisi kui organisatsioonilisi tegevusi.

---

5. Järelevalve ja koolitused

- Infoturbe olukorda hinnatakse vähemalt kord aastas või RIA/HTM järelevalve järel.
- Töötajatele ja õppuritele korraldatakse regulaarsed infoturbealased mikrokoolitused (linkjagamine, paroolid, isikuandmete kaitse).
- Koolituste eesmärk on suurendada teadlikkust turvariskidest ja ennetada andmeleket.

- Kõik rikkumised või kõrvalekalded registreeritakse, analüüsitakse ja dokumenteeritakse.
- Tulemused esitatakse direktori kinnitamiseks ning vajadusel rakendatakse parandusmeetmeid.

---

6. Poliitika kehtivus ja muutmine

Infoturvapoliitika kehtib alates 20.09.2025.
Poliitikat vaadatakse üle kord aastas või tehnoloogiliste muudatuste korral.
Muudatusettepanekud esitab IT-osakond, muudatused kinnitatakse direktori käskkirjaga.

---

7. Kinnitamine

Allkiri:

Eduard Brindfeldt
Tehnoloogia direktor
Tallinna Tööstushariduskeskus
20.09.2025
