ALGTEKST-TERVIKTEKST

Kinnitatud rektori 04.03.2024 käskkirjaga nr 7

Redaktsiooni jõustumise kuupäev: 04.03.2024

Infoturbe poliitika

Sisukord

[1 Üldine 2](#_Toc159837374)

[2 Mõisted 2](#_Toc159837375)

[3 Käsitlusala 3](#_Toc159837376)

[4 Põhimõtted 3](#_Toc159837377)

[5 Eesmärgid 3](#_Toc159837378)

[6 Infoturbe organisatsioon ja juhtimine 4](#_Toc159837379)

[6.1 Rektor 4](#_Toc159837380)

[6.2 Rektoraat 4](#_Toc159837381)

[6.3 Infoturbejuht 4](#_Toc159837382)

[6.4 Isikuandmete ja riigisaladuse kaitset korraldav isik 5](#_Toc159837383)

[6.5 Valdkonnajuht (struktuuriüksuse juht) 5](#_Toc159837384)

[6.6 Protsessijuht 5](#_Toc159837385)

[6.7 Organisatsiooni liikmed 5](#_Toc159837386)

[7 Infoturbeintsidendi lahendamisest 5](#_Toc159837387)

[8 Vastavused ja mittevastavused 5](#_Toc159837388)

[9 Rektoraadi ülevaade 6](#_Toc159837389)

[10 Rakendamine 6](#_Toc159837390)

[Lisa 1 8](#_Toc159837391)

# Üldine

Infoturbe poliitikaga sätestatakse infoturbe aluspõhimõtted Tallinna Tehnikaülikoolis (edaspidi ülikool), mis lähtuvad ISO 27001 standardi nõuetest ning annavad täpsemad tingimused, alused ja põhimõtted strateegiliseks infoturbe tagamiseks. Infoturbe poliitika eesmärk on määratleda ülikooli strateegiline lähenemine infoturbe tagamisel.

Ülikool käivitab infoturbe halduse süsteemi (ISMS), mis koosneb poliitikatest, protseduuridest, juhistest ning nendega seotud ressurssidest ja tegevustest, mida organisatsioon kollektiivselt haldab, püüdes kaitsta oma infovarasid. ISMS on suunatud organisatsiooni eesmärkide saavutamisele ning kujutab endast süstemaatilist lähenemist infoturbe rajamisele, käigushoiule, seirele, hooldamisele ja täiustamisele. See põhineb riski kaalutlemisel ja selle aktsepteerimisel tasemetele, mis tagavad riskide toimiva käsitluse ja halduse.

Infoturbe poliitika on tugevalt seotud ülikooli riskihalduse korralduse ja andmekaitse regulatsioonidega. Infoturve on eesmärgistatud tegevus ülikooli põhiprotsesside toetamiseks, infoturbealaste eesmärkide täitmiseks ning infovarade käideldavuse, tervikluse ja konfidentsiaalsuse tagamiseks.

# Mõisted

**Infoturve** tähendab andmete kolme põhiomaduse – käideldavuse, tervikluse ja konfidentsiaalsuse tagamist, sh:

* käideldavus – andmed peavad olema õigel ajal kättesaadavad ja kasutuskõlblikud;
* terviklus – andmed peavad olema usaldusväärsed ja autentsed ning volitamata muudatused peavad olema tuvastatavad ja kõrvaldatavad;
* konfidentsiaalsus – andmetele võimaldatakse juurdepääs ainult tõendatud teadmisvajaduse alusel.

**Infoturbe halduse süsteem** on infoturbe alane organisatsiooni sisene korraldus tagamaks infoturbe eesmärkide saavutamise. Infoturbehaldus süsteem koosneb poliitikatest, protseduuridest, juhistest ning nendega seotud ressurssidest ja tegevustest, mida organisatsioon kollektiivselt haldab, püüdes kaitsta oma infovarasid. ISMS on suunatud organisatsiooni eesmärkide saavutamisele ning kujutab endast süstemaatilist lähenemist infoturbe rajamisele, käigushoiule, seirele, hooldamisele ja täiustamisele. See põhineb riski kaalutlemisel ja selle aktsepteerimisel tasemetele, mis tagavad riskide toimiva käsitluse ja halduse.

**Vara** on miski, millel on omaniku jaoks väärtus. Varad on näiteks: teave, andmed, tarkvara, füüsiline vara (taristu, hoone, riistvara, sisseseade), rahaline vara, teenus, inimressurss (inimesed, kvalifikatsioon, oskused, kogemused), oskusteave, mitteaineline vara (maine, kuvand).

**Infotehnoloogiline vara** (IT vara) on organisatsiooni jaoks väärtust loov tarkvara või riistvara komponent infotehnoloogilises keskkonnas. IT varad on organisatsiooni süsteemide ja võrgu infrastruktuuri lahutamatud osad

**Teave** ehk **infovara** on kogum teadmust või andmed, mida saab defineerida ja grupeerida üheks ühikus ning millel on väärtus, kuid ka sellega kaasnevalt riskid organisatsioonile. Teave ehk inforvarad on kirjeldatud varadena ning on seotud infosüsteemide ja protsessidega.

**Infosüsteem** on infovara säilitamiseks ja töötlemiseks mõeldud süsteem. Infosüsteem võib koosneda mitmetest omavahel seotud infotehnoloogilistest vahenditest ehk varadest (sh funktsionaalsetest moodulitest, rakendustest, veebiteenustest, võrkudest, serveritest (mh virtuaalsed), arvutitest, operatsioonisüsteemidest, tarkvaradest ja andmebaasidest), mis moodustavad kontseptuaalse tervikliku süsteemi.

**Rakendus** on erinevate programmide kogum spetsiifiliste ülesannete täitmiseks. Rakenduste kogum võib moodustada infosüsteemi.

**Tarkvara** on infosüsteemi programmid, protseduurid, reeglid ja juurdekuuluv dokumentatsioon.

**Protsess (äriprotsess)** on organisatsiooni sees aset leidev ja eesmärgi saavutamisele suunatud tegevuste, toimingute või protseduuride jada, mille tulemusena luuakse kliendile väärtust (nt tooteid või teenuseid). Igal protsessil on omanik ja protsessijuht. Protsessiga on seotud strateegilised eesmärgid, õigusaktid, olulisemad sisendid ja väljundid, teenused (sh kliendid ja seotud sihtrühmad), indikaatorid, riskid, infosüsteemid ja infovarad.

**Teenus** on kliendile või tarbijale loodav väärtus, mingi protsessi (võimalik) tulem.

**Intsident** on planeerimata sündmus, mis häirib või vähendab teenuse kvaliteeti või tekitab teenuses katkestuse (või ähvardab seda teha).

**Infoturbe intsident (küberintsident)** on intsidendi eriliik, mille raames on toimunud edukas või edutu katse või rünne mingit IT vara hävitada, muuta, blokeerida, varastada või saada lubamatu juurdepääs või kasutada seda lubamatult.

**Andmekaitse intsident** on infoturbeintsidendi eriliik, mille raames toimub edastatavate, salvestatud või muul viisil töödeldavate isikuandmete turvalisuse rikkumine, juhuslik või ebaseaduslik hävitamine, kaotsiminek, kättesaamatuks muutumine, lubamatu juurdepääs või andmete loata avalikuks saamine.

# Käsitlusala

Infoturbepoliitika ja seda toetavad kontrollmeetmed, protsessid ja protseduurid kehtivad kogu ülikoolis kasutatavale teabele. Sealhulgas hõlmab endas teavet, mida teised organisatsioonid ülikooliga suhtlemisel töötlevad.

Infoturbepoliitika ja seda toetavad kontrollimeetmed, protsessid ja protseduurid kehtivad kõigile isikutele, kellel on juurdepääs ülikooli infole ja tehnoloogiatele, sh välistele isikutele, kes pakuvad ülikoolile teenust või töötlevad informatsiooni muude koostöövormide raames.

Üksikasjalik ulatus, sealhulgas kasutajate, infovarade ja infotöötlussüsteemide jaotus, sisaldub kaasnevas infoturbe haldussüsteemi käsitlusala dokumentatsioonis.

# Põhimõtted

* Ülikool valib infovarade omanikuna nende kaitsmiseks piisavad ja asjakohased meetmed.
* Infovaradele riskihindamise käigus määratletakse olulisuse tase lähtuvalt ülikooli põhitegevusest ja eesmärkidest.
* Infovarasid tuleb kasutada ülikooli tegevusega seotud eesmärkidel.
* Infoturbe nõuete järgimine on kõikidele töötajatele kohustuslik.
* Infovaradele võimaldatakse juurdepääs tõendatud teadmisvajaduse alusel.
* Vastuolus olevad ülesanded või vastusolus olevad vastutusalad tuleb hoida lahutatuna.
* Konfidentsiaalsuskohustuse nõue kehtib konfidentsiaalse informatsiooni kohta ja seda kohaldatakse ülikooli infovara kasutavatele isikutele tulenevalt õigusaktidest ja sõlmitavatest lepingutest.

# Eesmärgid

Ülikooli infoturbealased eesmärgid on:

* Pakkuda ülikooli liikmeskonnale (töötajatele, üliõpilastele ja vilistlastele) ning koostööpartneritele kindlustunnet, et ülikool hoiab ja töötleb nendega seotud infovara (andmed, teave) lähtuvalt seaduslikest alustest ning tagab teabe turvalisuse (konfidentsiaalsuse, terviklikkuse ja käideldavuse).
* Infoturve on integreeritud ülikooli põhi- ja tugitegevuste lahutamatuks osaks.
* Infovaraga seotud riskid tuvastatakse, analüüsitakse, hinnatakse ning käsitletakse vastavalt kokkulepitud riskitaluvusele.
* Infosüsteemide ja rakenduste arendamisel või hankimisel võetakse arvesse infoturbe standardistest tulenevaid nõudeid.
* Ülikooli infovaradega toimetavad isikud on teadlikud infoturbega seotud vastutusest ja kohustusest. Infoturbega seotud lepingulisi ja juriidilisi kohustusi mõistetakse ja täidetakse.
* Infoturbeks vajalikud organisatsioonilised, füüsilised, protseduurilised ja tehnilised kontrollid tasakaalustavad kasutajakogemust.
* Volitatud kasutajad saavad oma tööülesannete täitmiseks turvaliselt ligi infovaradele ja vajadusel seda jagada.
* Infovaradega seotud intsidentide arv on minimaalne, nendest järjepidevalt õpitakse ja sellest tulenevalt täiendatakse erinevaid infoturbe meetmeid.

Infovara turvalisuse tagamiseks ja infoturbe eesmärkide saavutamiseks rakendatakse erinevaid infoturbe haldussüsteemi osasid (kontrollid, poliitikad, reeglid, juhised, protsessid, struktuurid, ressursid, tegevused, tarkvaralised kui ka riistvaralised lahendused) lähtudes infoturbe standardist ja regulatsioonidest.

# Infoturbe organisatsioon ja juhtimine

Infoturbe poliitika juurutamine hõlmab turvameetmete kavandamist, loomist, evitamist, haldamist ja vastutusalade määramist. Infoturbe toimimiseks on määratletud infoturbealased rollid. Infoturve on organisatsiooni kollektiivne tegevus ja kõikide infovara kasutajate kohustus.

Infoturbealane vastutus jaguneb üldiseks ja konkreetseks vastutuseks:

* üldine infoturbealane vastutus on infovara kasutajatel, mis seisneb valdkonna regulatsioonide järgimises ja infoturbeintsidentidest teavitamises.
* konkreetne infoturbealane vastutus tuleneb ametikohast ülikooli struktuuris ja tööülesannetest. Nii rektor, struktuuriüksused kui iga töötaja vastutavad individuaalselt enda kohustuste nõuetekohase täitmise eest.

## Rektor

* Kinnitab ülikooli infoturbe poliitika;
* Kinnitab ülikooli infoturbejuhi.

## Rektoraat

* Näitab üles pühendumust ja eestvedamist seoses infoturbe haldussüsteemiga;
* Tagab et infoturbe poliitika on ajakohane ning infoturbe eesmärgid on kooskõlas ülikooli eesmärkidega;
* Tagab, et infoturbe nõuded oleksid integreeritud ülikooli erinevatesse protsessidesse;
* Tagab lähtuvalt riskihaldusest vajalikud vahendid infoturbe haldussüsteemile;
* Tagab vastavuse infoturbe haldussüsteemi nõuetele;
* Tagab, et infoturbe haldussüsteem saavutab oma kavandatud tulemused ja hindab eesmärkide saavutamist;
* Nõuab organisatsiooni liikmetelt infoturbe poliitika kui ka infoturbe haldussüsteemi raames välja töötatud kordade, juhiste ja regulatsioonide täitmist;
* Suunab ja toetab organisatsiooni liikmeid panustama tagamaks tõhusat infoturbe haldussüsteemi;
* Edendab pidevat täiustamist;
* Toetab teisi asjakohaseid juhtimisrolle näidates üles oma eestvedamist nende vastutusvaldkondades;
* Vaatab planeeritud ajavahemike järel üle organisatsiooni infoturbe haldussüsteemi, et tagada selle jätkuv sobivus, adekvaatsus ja tõhusus.

## Infoturbejuht

* Vastutab, et infoturbepoliitika, standardite, juhiste ja kontrollide väljatöötamise, ülevaatamise ja jõustamise eest, et tagada vastavus asjakohastele seadustele ja määrustele.
* Tagab, et infoturbe alased meetmed saaksid rakendatud ning kontrollib nende täitmist vähemalt kord aastas.
* Korraldab ülikooli infoturbe alast seiret ja intsidentidele reageerimist;
* Vastutab, et ülikooli infoturbe alane teadlikkus kasvab;
* Teavitab, nõustab ja koolitab töötajaid turvameetmete rakendamisel;
* Jälgib kontrollide täitmist ning annab ülevaateid vastavatele osapooltele;
* Annab ülevaate rektoraadile infoturbe alasest seisukorrast vähemalt kord aastas;
* Vastutab infoturbe haldussüsteemiga seotud kommunikatsiooni korraldamise eest ülikoolis;
* Määratleb ja mõtestab infoturbe haldussüsteemiga seotud osapooli ja nendega seotud vajadusi ning nõudeid;
* On kontaktisikuks infoturbe alasel suhtlusel ametivõimudega;
* Tagab asjakohase infoturbalase teabevoolu ülikooli (kontaktiks erihuvirühmadega või spetsialiste turvafoorumitega, jne)
* Korraldab riskide halduseks sisendi teabe infoturvaohtudest;
* Tagab ISMSi järjepideva parendamise.

## Isikuandmete ja riigisaladuse kaitset korraldav isik

* korraldab isikuandmete kaitset vastavalt valdkonna õigusaktidele;
* korraldab riigisaladuse ja salastatud välisteabe kaitset vastavalt valdkonna õigusaktidele.

## Valdkonnajuht (struktuuriüksuse juht)

* Vastutab oma valdkonnas infoturbe haldussüsteemi osade rakendamise eest;
* Täidab oma vastusalas paiknevate infosüsteemi või rakenduste osas omaniku rolli;
* Määrab oma vastusalas olevatele infosüsteemidele või rakendustele äriprojektijuhi ja peakasutaja;
* Tagab tema vastusalas olevate tööd tegevate isikute vajalikud pädevus, mis mõjutavad tema vastusalas olevat infoturbe toimimist
* Planeerib ja tagab ressursid infoturbeks oma valdkonnas.

## Protsessijuht

* Vastutab oma protsessis infoturbe haldussüsteemi osade rakendamise eest;
* Tuvastab, analüüsib ja hindab koostöös äriprojektijuhi, peakasutaja, IT projektijuhi ja süsteemihalduriga oma protsessiga seotud infosüsteemide ja rakendustega seotud riske.
* On protsessi jooksul tekkinud andmete või teabe omanik.

## Organisatsiooni liikmed

* On teadlikud infoturbe poliitikast ja talle kohalduvatest infoturbe alastest kordadest ja regulatsioonidest;
* Mõistavad oma rolli infoturbe haldussüsteemis ja järgivad oma töös sellest tulenevaid poliitikaid, reegleid, juhiseid, kontrolle, struktuure ja protsesse ning mõistavad kasu, mis tulenevad infoturbe tulemuslikkuse parandamisest;
* On teadlikud infoturbe haldussüsteemi nõuete mittejärgmise tagajärgedest;
* Panustavad infoturbe tegevuste pidevasse täiustamisse.

# Infoturbeintsidendi lahendamisest

* Infoturbeintsidendist peab iga infovara kasutaja esimesel võimalusel teavitama IT kasutajatuge.
* Infoturbeintsidentide lahendamine toimub lähtuvalt intsidendi lahendamise korrale.
* Infoturbeintsidendi lahendamiseks peavad infovaraga seotud osapooled andma infoturbejuhile ja volitatud isikutele juurdepääsuõiguse informatsioonile, mis on intsidendi lahendamiseks vajalik.
* Infoturbeintsidentidest teavitab infoturbejuht regulatsioonidest tulenevaid osapooli (sh välised osapooled).
* Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo või distsiplinaarsüüteo tunnused, antakse juhtum edasi menetlemiseks vastava menetluse läbiviimise õigust omavale organile.
* Intsidendi lahendamise käigus kogutud informatsioon dokumenteeritakse, analüüsitakse ja kasutatakse eesmärgiga ennetada sarnaste intsidentide kordumist tulevikus.

# Vastavused ja mittevastavused

Ülikoolis kontrollitakse infoturbepoliitika ja infoturbe haldussüsteemi vastavust läbi regulaarse aruandluse, infovarade omanike tagasisidestamise, riskide hindamise ning sise- ja välisauditite tulemuste põhjal.

Kõik erisused ja erandjuhtumid infoturbe meetmete rakendamisel dokumenteeritakse ning enne nende rakendamist tuleb need infoturbejuhi poolt kinnitada.

Mittevastavuse ilmnemisel tuleb:

* reageerida ning tuleb võtta kasutusele meetmed selle kontrollimiseks ja parandamiseks või sealhulgas tagajärgedega tegelemiseks;
* hinnata olukorda, et kas mittevastavus võib esineda ka mujalgi ning vajadusel tegeleda juurpõhjuse kõrvaldamisega;
* vaadata üle parandusmeetmete tõhusus;
* vajadusel teha muudatusi infoturbe haldussüsteemis (nt täiendades kordasid, reegleid, juhiseid, jne)
* dokumenteerida mittevastavused (sh mittevastavuse olemus, edasised sammud ja meetmed ning parandusmeetmete tulemused)

Mittevastavuste dokumenteerimise eest vastutab infoturbejuht.

Organisatsiooni liikmetele, kes on rikkunud infoturbepoliitika põhimõtteid, kohaldatakse vastavalt kehtivatele kordadele distsiplinaarseid meetmeid.

# Rektoraadi ülevaade

Vaatab planeeritud ajavahemike järel üle organisatsiooni infoturbe haldussüsteemi, et tagada selle jätkuv sobivus, adekvaatsus ja tõhusus.

Rektoraadi ülevaade peab hõlmama vähemalt järgnevat

* Tegevuste staatus varasemate juhtkonna ülevaatuste põhjal;
* Muudatused infoturbe haldussüsteemi jaoks olulistes välis- ja siseküsimustes;
* Muudatused seoses huvitatud osapoolte vajaduste ja ootustega infoturbe haldussüsteemile;
* Tagasiside infoturbe toimimise kohta, sealhulgas suundumused (mittevastavused ja parandusmeetmed, seire- ja mõõtmistulemused, auditi tulemused, infoturbe eesmärkide täitmine).
* Tagasiside huvitatud isikutelt;
* Riskide tuvastamise, analüüsi ja hindamise tulemused ja riskikäsitluse plaan;
* Võimalused pidevaks täiustamiseks.

Rektoraadi ülevaate ISMS’ist valmistab ette infoturbejuht. Rektoraadi ülevaatuse tulemused peavad sisaldama otsuseid, mis on seotud infoturbe juhtimissüsteemi pideva täiustamise võimaluste ja muudatuste vajadusega.

# Rakendamine

Infoturbe poliitika on avalik dokument, mis avaldatakse ülikooli veebilehel oigusaktid.taltech.ee. Infoturbe poliitika tehakse teatavaks kõigile ISMSi kohaldamisalasse kuuluvatele isikutele.

Infoturbe poliitika ja infoturbe haldussüsteemi lisadeks on alljärgnevad väljatöötavad korrad ja juhised, mis kinnitatakse eraldisseisvalt infoturbe poliitikast. Oluline on tagada kogu infoturbe haldussüsteemi kooskõla erinevate poliitikate, regulatsioonide, kordade ja juhiste vahel. Infoturbe haldussüsteemi korrad ja juhised kinnitab kantsler oma korraldusega.

* Infoturbe käsitlusala ulatus
* Administratiiv tegevuste haldus
* Andmekaitse ja teabevahetus
* Arendustööde eeskiri (kinnitatud)
* Füüsiline turvalisuse korraldus
* Infotehnoloogiliste varade haldus
* Juurdepääsuhaldus
* Kaugtöö ja mobiilsed seadmed
* Kriisihaldus
* Krüptograafilised protseduurid
* Logimise poliitika
* Lõppkasutajate seadmete haldamise ja kasutamise põhimõtted
* Muudatuste haldus
* Partnersuhted ja kokkulepped
* Personali haldus
* Pöördumiste, intsidendi, sündmuste ja probleemide haldus
* Riskihaldus
* Serverite ja võrguhalduse põhimõtted
* Siseaudit ja vastavus
* Talituspidevus

Infoturbe poliitikaid kui ka täiendavaid kordasid ja juhiseid vaadatakse läbi vähemalt üks kord aastas ning vajadusel korrigeeritakse lähtuvalt erinevatest mõjuteguritest (nt eesmärkide muutused, väline keskkond, infoturvalisusega seotud riskid, jne) kui ka rektoraadi ülevaate või auditite tulemustest.

#  Lisa 1

Joonis Infoturbe haldussüsteemi kirjeldav joonis

