ALGTEKST-TERVIKTEKST

Kinnitatud rektori 21.12.2017 käskkirjaga nr 117

Redaktsiooni jõustumise kuupäev: 01.01.2018

Infoturbe poliitika

1. **Sissejuhatus**
   1. Infoturbe poliitikaga sätestatakse infoturbe aluspõhimõtted Tallinna Tehnikaülikoolis (edaspidi *ülikool*).
   2. Infoturbe poliitika eesmärk on määratleda ülikooli strateegiline lähenemine infoturbe tagamisel.
2. **Mõisted**
   1. Infovara on informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid.
   2. Informatsioon on mis tahes viisil kogutud, jäädvustatud ja töödeldud andmete kogum mistahes andmekandjal, sh paberkandjal.
   3. Infoturve on turvameetmete loomise, valimise ja rakendamise protsesside kogum.
   4. Infoturve tähendab andmete kolme põhiomaduse – käideldavuse, tervikluse ja konfidentsiaalsuse tagamist, sh:
      1. käideldavus – andmed peavad olema õigel ajal kättesaadavad ja kasutuskõlblikud;
      2. terviklus – andmed peavad olema usaldusväärsed ja autentsed ning volitamata muudatused peavad olema tuvastatavad ja kõrvaldatavad;
      3. konfidentsiaalsus – andmetele võimaldatakse juurdepääs ainult tõendatud teadmisvajaduse alusel.
   5. Infoturbeintsidendiks on juhtumid, mille läbi on sündinud või võib sündida kahju andmete põhiomadustele või andmesubjektile, samuti toimingud, mis ei ole kooskõlas infoturbe valdkonda reguleerivate õigusaktidega.
   6. Infovara peakasutaja on isik, kes on vastutusala juhi poolt määratud ja vastutab infovara eest. Kuni peakasutaja määramiseni vastutab infovara eest selle tekitanud isik.
   7. Infovara haldur (teenusehaldur) on isik, kes on infovara peakasutaja poolt määratud ja tegeleb infovara majandamisega, tagades infoturbe põhimõtete rakendamise.
   8. Infovara kasutaja on töötaja, üliõpilane või muu ülikooliga seotud isik, kellele infovara peakasutaja on andnud infovara kasutamise õigused.
3. **Infoturbe eesmärgid**

Infoturbe eesmärkideks on tagada:

* 1. ülikooli toimimine, hea maine ja teenuste jätkusuutlik pakkumine;
  2. infosüsteemide ja andmekogude pidamine ning arendamine vastavalt õigusaktidest tulenevatele infoturbe nõuetele.

1. **Põhimõtted**
   1. Ülikool valib infovarade omanikuna nende kaitsmiseks piisavad ja asjakohased meetmed.
   2. Infovarasid tuleb kasutada ülikooli tegevusega seotud eesmärkidel.
   3. Infoturbe nõuete järgimine on kõikidele töötajatele kohustuslik.
   4. Infovaradele võimaldatakse juurdepääs tõendatud teadmisvajaduse alusel.
   5. Konfidentsiaalsuskohustuse nõue kehtib konfidentsiaalse informatsiooni kohta ja seda kohaldatakse ülikooli infovara kasutavatele isikutele tulenevalt õigusaktidest ja sõlmitavatest lepingutest.
2. **Infoturbe organisatsioon ja juhtimine**
   1. Infoturbe poliitika juurutamine hõlmab turvameetmete kavandamist, loomist, evitamist, haldamist ja vastutusalade määramist.
   2. Infoturbe toimimiseks on alapunktides 5.6 -5.12 määratletud infoturbealased rollid.
   3. Infoturve on organisatsiooni kollektiivne tegevus ja kõikide infovara kasutajate kohustus.
   4. Ülikool peab eraldama infoturbe tagamiseks vajalikud vahendid.
   5. Infoturbealane vastutus jaguneb üldiseks ja konkreetseks vastutuseks:
      1. üldine infoturbealane vastutus on infovara kasutajatel, mis seisneb valdkonna regulatsioonide järgimises ja infoturbeintsidentidest teavitamises.
      2. konkreetne infoturbealane vastutus tuleneb ametikohast ülikooli struktuuris ja tööülesannetest. Nii rektor, struktuuriüksused kui iga töötaja vastutavad individuaalselt enda kohustuste nõuetekohase täitmise eest.
   6. **Rektor:**
      1. kinnitab ülikooli infoturbe strateegia jt regulatsioonid;
      2. määrab infoturbe eest vastutavad ametikohad;
      3. korraldab infoturbe valdkonna regulaarse auditeerimise;
      4. viib läbi lõpliku jääkriskide aktsepteerimise.
   7. **Infoturvet korraldav isik:**
      1. koordineerib infoturbe valdkonda ja täidab sellega seotud ülesandeid;
      2. tagab infoturbe regulatsioonide olemasolu ja täiendamise;
      3. kontrollib turvameetmete tõhusust;
      4. teavitab, nõustab ja koolitab töötajaid turvameetmete rakendamisel;
      5. teeb koostööd töötajate ja ülikooliväliste isikutega.
   8. **Isikuandmete ja riigisaladuse kaitset korraldav isik:**
      1. korraldab isikuandmete kaitset vastavalt valdkonna õigusaktidele;
      2. korraldab riigisaladuse ja salastatud välisteabe kaitset vastavalt valdkonna õigusaktidele.
   9. **Vastutusala juht:**
      1. arvestab oma valdkonda juhtides infoturbe nõuetega;
      2. määrab infovara peakasutaja;
      3. planeerib finantsressursid infoturbeks oma valdkonnas;
      4. tagab infovara toimimiseks vajaliku ressursi ja jätkusuutlikkuse.
   10. **Infovara peakasutaja:**
       1. määratleb infovara kaitstuse vajaduse ja turvameetmed (nt kasutades turvaklassi);
       2. jälgib turvameetmete vastavust ja kontrollib nõuete täitmist.
   11. **Infovara haldur** tagab peakasutaja poolt kavandatud turvameetmete rakendamise.
   12. **Infovara kasutaja** toetab ja järgib ülikoolis infovarade kasutamist ja kaitset reguleerivaid kordasid, täites turvaalast funktsiooni vastavalt oma ametiülesannetele, lepingule või infoturbealasele regulatsioonile.
3. **Riskihaldus**
   1. Ülikoolis määratakse minimaalsed turvameetmed, lähtudes õigusaktides tulenevatest nõuetest ja standarditest, mida tuleb rakendada infovaradele ettenähtud turvataseme saavutamiseks ja säilitamiseks.
   2. Riskide leevendamiseks rakendatakse turvameetmeid vastavalt infovaradele määratud kaitstuse vajadusele ja heale tavale.
   3. Kui turvameedet ei ole võimalik või otstarbekas täita, peab leidma alternatiivsed meetmed riski leevendamiseks või peab rektor aktsepteerima meetme täitmata jätmisest tuleneva jääkriski.
   4. Kui infosüsteemi peakasutaja leiab, et minimaalsetest turvameetmetest ei piisa, koostatakse lisaks detailne riskianalüüs, kus vaadatakse eraldi iga infovarale mõjuvat ohtu, hinnatakse selle realiseerumise tõenäosust, määratakse suuremad riskid ja võetakse vajadusel kasutusele spetsiifilised meetmed nende leevendamiseks.
4. **Infoturbe halduse protsess**
   1. Turvameetmete pideva ajakohasuse tagamiseks on vajalik turvameetmete ja regulatsioonide perioodiline läbivaatus, töökeskkonna igapäevane seire, muudatustele reageerimine ning infoturbeintsidentide lahendamine.
   2. Infosüsteemi muudatusi ja uuendusi tuleb enne nende läbiviimist kaaluda infoturbe seisukohast. Muutunud nõuete või uute ohtude korral tuleb turvameetmed ümber hinnata.
   3. Infoturbe seisukohast olulised muudatused tuleb kooskõlastada infoturvet korraldava isikuga.
   4. Ülikoolis on infoturbe koolituste kava. Infoturbe koolitustel osalemine on töötajale kohustuslik.
   5. Väline organisatsiooni turvaaudit viiakse läbi vastavalt vajadusele, kuid mitte harvemini kui kord 3 aasta jooksul. Infosüsteemide turvaaudit viiakse läbi vastavalt infosüsteemi kaitstuse vajadusele.
5. **Infoturbeintsident ja kontrolljäljed**
   1. Infoturbeintsidendist peab iga infovara kasutaja esimesel võimalusel teavitama IT kasutajatoeüksust.
   2. Infoturbeintsidentide lahendamine toimub infoturvet korraldava isikuga kooskõlastatud põhimõtete alusel.
   3. Infoturbeintsidendi lahendamiseks peab infosüsteemi peakasutaja tagama infoturvet korraldavale isikule ja volitatud isikutele juurdepääsuõiguse informatsioonile, mis on intsidendi lahendamiseks vajalik.
   4. Intsidendi lahendamise käigus kogutud informatsioon dokumenteeritakse, analüüsitakse ja kasutatakse eesmärgiga ennetada sarnaste intsidentide kordumist tulevikus.
   5. Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo või distsiplinaarsüüteo tunnused, antakse juhtum edasi menetlemiseks vastava menetluse läbiviimise õigust omavale organile.