JYVÄSKYLÄN YLIOPISTON TIETOTURVAPERIAATTEET

Tietoturvaperiaatteilla yliopiston johto täsmentää turvallisuuspolitiikassa määriteltyä tietoturvapolitiikkaa. Tietoturvapolitiikka ja -periaatteet kuvaavat tietoturvaan liittyviä yleisiä tavoitteita, keinoja, vastuita ja organisointia, joilla tietoturvallisuutta yliopistossa ohjataan ja toteutetaan.

Tietoturvaperiaatteet koskevat jokaista yliopistossa työskentelevää ja opiskelevaa. Näitä periaatteita ja vastuita on kuvattu tarkemmin yliopiston sisäiseen käyttöön tarkoitetuissa tietoturvaperiaatteissa intranetissä.

Tietoturvan tavoitteet

Tiedon hallinta ja käsittely turvallisesti on osa yliopiston toiminnan laatua ja kokonaisturvallisuutta. Tietoturvan tavoitteena on varmistaa tiedon suojaaminen (luottamuksellisuus), taata tiedon oikeellisuus (eheys) sekä mahdollistaa tiedon käytettävyys ja saatavuus siihen tarkoitukseen, johon se on luotu. Tietoturvapolitiikkaa, -periaatteita, -sääntöjä ja -ohjeita sovelletaan kaikkeen yliopiston oman ja sen sidosryhmien toimeksiannoissa saadun tiedon käsittelyyn tiedon koko elinkaaren ajan riippumatta siitä, missä muodossa ja millä välineillä tietoa käsitellään, ja kuka tietoa käsittelee.

Tietoturvallisuuden tavoite on turvata yliopiston toiminnalle tärkeiden tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tarkoituksellinen tiedon tuhoutuminen tai vääristyminen.

Tietoturvan hallintamekanismien ja riskienhallinnan keinoin varmistetaan toimintaympäristön ja -tapojen riittävä ja tarkoituksenmukainen turvallisuus ja häiriötön toiminta.

Tietoturvatoiminnalla varmistetaan toiminnan jatkuvuus normaalioloissa ja niiden häiriötilanteissa sekä valmiuslain (2011/1552) mukaisissa poikkeusoloissa. Yliopiston velvoitteista poikkeusoloissa säädetään yliopistolaissa (2009/558).

Tietoturvan toteuttamisen keinot

Tietoturvatoimintaa toteutetaan erilaisina prosesseihin sisällytettävinä kontrolleina, toimintatapoina, ohjeina ja koulutuksilla sekä tietojärjestelmissä erilaisilla teknisillä ratkaisuilla. Toiminta perustuu jatkuvaan kehittämiseen, jolla tietoturva pyritään liittämään osaksi päivittäistä operatiivista toimintaa ja toimintatapoja.

Tietoturvariskejä hallitaan säännönmukaisella ja järjestelmällisellä riskienhallinnalla. Riskiarvion avulla suunnataan kehittämistä, joka toteutetaan yliopiston normaalin vuosisuunnittelun puitteissa.

Tietoturvapoikkeamiin reagoidaan mahdollisimman nopeasti vaikutusten minimoimiseksi. Poikkeamia hallitaan määritellyn prosessin mukaisesti.

Jatkuvuus-, toipumis- ja valmiussuunnittelu kohdennetaan vähintään yliopiston kriittisiin toimintoihin ja prosesseihin ja niitä toteuttaviin tai tukeviin tietojärjestelmiin. Kyvykkyyttä

toimia häiriötilanteissa tai poikkeusoloissa kehitetään ja ylläpidetään säännöllisellä harjoittelulla.

Henkilöstön ja opiskelijoiden tietoturvaosaamista ja –tietoisuutta kehitetään koulutuksella ja tietoturvasta tiedottamalla.

Tietoturvaa ohjaavat tekijät

Yliopiston tietoturvatoiminnassa noudatetaan yliopiston johtosääntöä sekä Suomen ja EU:n lainsäädäntöä. Viitekehyksenä tietoturvan toteuttamisessa yliopistossa sovelletaan julkishallinnon tietoturvakäytänteitä ja ISO 27001 -standardia.

Tietoturvan vastuut ja organisointi

Jyväskylän yliopiston tietoturvasta vastaa yliopiston rehtori.

Jokaisen yliopistoon työ-, opiskelu- tai muussa sopimussuhteessa oleva henkilö tai yliopiston tarjoamiin palveluihin käyttöoikeuden saanut käyttäjä on velvollinen noudattamaan tietoturvaperiaatteita ja niitä täsmentäviä sääntöjä ja ohjeita sekä tietojärjestelmien, -verkkojen, -koneiden ja -välineiden käyttösääntöjä. Politiikoiden, periaatteiden, sääntöjen tai ohjeiden laiminlyöminen tai niiden vastaisesti toimiminen voi johtaa seuraamuksiin, jotka on määritelty tietoturvasäännöissä.

Seuranta ja valvonta

Hallinnollisen ja teknisen tietoturvan toteutumista yliopistossa valvotaan ulkopuolisten auditointien, sisäisen tarkastuksen ja katselmusten avulla. Teknistä tietoturvaa seurataan lisäksi jatkuvan teknisen ja osittain automaattisen valvonnan keinoin. Tietoturvapäällikkö koordinoi valvontaa ja seurantaa.

Poikkeamien valvonta

Jokaisen työntekijän, opiskelijan ja yliopiston palveluita käyttävän velvollisuus on ilmoittaa havaitsemistaan tietoturvapoikkeamista ja –puutteista sekä epäilemistään väärinkäytöksistä tietoturvapäällikölle (tietoturva@jyu.fi).

Tietoturvapolitiikan ja –periaatteiden hyväksyntä ja ylläpito

Tietoturvapolitiikan ja -periaatteiden valmistelusta ja ylläpidosta vastaa yliopiston tietoturvapäällikkö.

Tietoturvaperiaatteet päivitetään vähintään kahden vuoden välein ja ne hyväksyy vararehtori tietoturvan kehittämisryhmän puheenjohtajana.

9.1.2024 Jyväskylässä

_____

Henrik Kunttu, vararehtori, tietoturvan kehittämisryhmän puheenjohtaja

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Tämä dokumentti on allekirjoitettu sähköisesti JYU Sign-järjestelmällä
This document has been electronically signed using JYU Sign

Päiväys / Date: 10.01.2024 13:52:51 (UTC +0200)

Henrik Mikael Kunttu

Vararehtori

Organisaation varmentama (JYU käyttäjätunnus ja puhelintunnistus)
Certified by organization (JYU user account and mobile identification)