

IT-palvelujen väärinkäytön seuraamukset

Tietotekniikkarikkomuksina pidetään yliopiston tietojärjestelmien käytöstä annettujen sääntöjen tai määräysten vastaista toimintaa tai tietojärjestelmien käyttöä Suomen lakien vastaisesti.

Tämä toimintaohje kuvaa toimenpiteitä, joita henkilöön kohdistetaan, kun tietotekniikkarikkomus on havaittu tai sitä on perustellusti syytä epäillä. Toimenpiteet on jaettu käyttövaltuuksien rajoituksiin rikkomuksen selvitystyön ajaksi sekä mahdollisiin rikkomuksesta määriteltyihin seuraamuksiin.

Yliopisto voi rajoittaa IT-palveluiden käyttövaltuuksia selvitystyön ajaksi

Rajoituksista päätetään, kun tietotekniikkarikkomus on havaittu tai sitä epäillään. Valtuuksia rajoitetaan aina, kun perustelluista syistä epäillään, että käyttäjä on syyllistynyt väärinkäyttöön, ja on mahdollista, että käyttövaltuudesta on haittaa rikkomuksen selvittämiseksi tai vahinkojen minimoimiselle. Tarvittaessa käyttäjä kutsutaan kuultavaksi.

Käyttövaltuuksien rajoittamisesta päättää esimies ja henkilöstön kehittämisjohtaja. Rajoittamisen toteuttaa palvelun pääkäyttäjä.

Kiireellisissä tapauksissa pääkäyttäjä voi omalla päätöksellään rajoittaa käyttövaltuuksia enintään kolmeksi päiväksi, mistä tulee välittömästi ilmoittaa tietohallintojohtajalle.

Tarvittaessa käyttäjän työasema voidaan kytkeä irti verkosta.

Rajoitukset voidaan purkaa selvitystyön päätyttyä, jos käyttövaltuuksien palauttamisesta ei ole ilmeistä haittaa.

Seuraamukset

Lievisissä tapauksissa käyttäjälle huomautetaan asiattomasta toiminnasta.

Tietotekniikkarikkomuksen seurauksena käyttäjä voi olla korvausvastuussa aiheuttamistaan vahingoista ja väärinkäytön selvitystyön aiheuttamista kustannuksista.

Seuraamukset opiskelijalle

Opiskelijalle kohdistettavia seuraamuksia voivat olla määräaikainen käyttövaltuuksien menettäminen tai rajoittaminen, yliopiston hallinnolliset toimet (kirjallinen varoitus, määräaikainen erottaminen) ja rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttövaltuuksiin kohdistuvista toimista päättää tietohallintojohtaja. Käytön rajoitusaikaan ei lasketa mukaan selvitystyöhön kulunutta aikaa. Kirjallisen varoituksen antamisesta opiskelijalle päättää yliopiston rehtori ja määräaikaisesta erottamisesta yliopiston hallitus. Henkilön käyttövaltuudet perutaan erottamisen ajaksi.

Seuraamukset henkilökuntaan kuuluvalle

Henkilökuntaa koskevia seuraamuksia voivat olla yliopiston työoikeudelliset toimet (suullinen huomautus, kirjallinen varoitus, irtisanominen, palvelussuhteen purku) sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttövaltuudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä johtuvan luottamuspuolan synnyttyä evätä määräajaksi tai pysyvästi. Käyttövaltuuksiin kohdistuvista toimista päättää esimies ja henkilöstön kehittämisjohtaja.

Seuraamukset muille käyttäjille

Yliopiston henkilökuntaan tai tutkinto-opiskelijoihin kuulumattomia käyttäjiä koskevat seuraamukset voivat olla käyttövaltuuksien poistaminen tai rajoittaminen sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttövaltuudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä johtuvan luottamuspuolan synnyttyä evätä määräajaksi tai pysyvästi. Käyttövaltuuksiin kohdistuvista toimista päättää yksikön esimies ja tietohallintojohtaja.

Esimerkkejä IT-palvelujen väärinkäytöksistä

- Rikoslain ja tekijänoikeuslain alaisen materiaalin oikeudeton käsittely
 - o Rikoslain alaista materiaalia ovat esimerkiksi lapsiporno, eläimiin sekaantuminen, raaka väkivalta, rasistinen aineisto ja kansankiihottamismateriaali
 - o käsittelyä ovat mm. materiaalin levittäminen ja hallussapito.
 - o Tekijänoikeuslain alaista materiaalia ovat esimerkiksi musiikki, videot, sarjakuvat, elokuvat, pelit ja ohjelmistot.
- Tunnuksen luovuttamista on esimerkiksi
 - o salasanan kertominen toiselle käyttäjälle
 - o tietokoneen auki jättäminen niin, että toinen henkilö pääsee käyttämään toisen tunnusta.
- Tiedon luottamuksellisuuden vaarantamista on esimerkiksi
 - o Salassa pidettävän tai muutoin lain suojaa nauttivan tiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä (esimerkiksi palvelinten käyttäjätietojen luovutus)
 - o salassa pidettävän tiedon tietoturvan laiminlyönti (passiivista toimimattomuutta)
 - o tahalliset salassapitorikokset (aktiivista toimintaa)
 - o henkilötietolain rikkominen.
- Henkilökohtaisen tietoturvan laiminlyöntiä on esimerkiksi
 - o salasanan jättäminen näkyviin
 - o yliopiston varmuuskopiointikäytäntöjen laiminlyöminen