
YT-neuvosto hyväksynyt 10.2.2005

Vahvistanut: Hallintojohtaja Hannu Pietilä
Pvm: 11.2.2007

TIETOTEKNIKKARIKKOMUSTEN SEURAAMUSKÄYTÄNTÖ

1	Käyttöoikeuksien rajoittaminen selvitystyön ajaksi	1
2	Seuraamukset	2
2.1	Opiskelijat	2
2.2	Henkilökunta.....	3
2.3	Muut.....	3
3	Seuraamustaulukot.....	3
3.1	Käsitteitä	3

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

Tässä dokumentissa on kuvattu toimenpiteitä, joita henkilöön kohdistetaan, kun tietotekniikkarikkomus on havaittu tai sitä on perusteltua syytä epäillä. Toimenpiteet on jaettu käyttöoikeuksien rajoituksiin rikkomuksen *selvitystyön ajaksi* sekä mahdollisiin rikkomuksesta määrättyihin *seuraamuksiin*.

Dokumentti keskittyy ensisijaisesti yliopiston tutkinto-opiskelijoihin ja henkilökuntaan.

Yliopiston järjestelmiin voi olla käyttäjätunnuksia myös mm. OPM-rahoituksella toimivilla tutkijoilla, emerituksilla ja ulkopuolisten palveluntarjoajien työntekijöillä sekä täydennyskoulutuksen ja avoimen yliopiston opiskelijoilla. Tämän ryhmän heterogeenisuudesta johtuen sen osalta tapahtuneissa rikkomuksissa käytetään enemmän tapauskohtaista harkintaa.

Kaikki havaitut tietotekniikkarikkomukset ja niistä aiheutuneet toimenpiteet on ilmoitettava yliopiston tietoturvapäällikölle.

1 Käyttöoikeuksien rajoittaminen selvitystyön ajaksi

Käyttöoikeuksia voidaan rajoittaa joko sulkemalla kaikki tai osa rikkomuksesta epäillyn käyttäjän käyttäjätunnuksista tai muutoin estämällä hänet jonkin tietojärjestelmän käyttö (esim. poistamalla tiedon muutosoikeus).

Selvitystyön ajaksi

- *henkilökuntaan* kuuluvan käyttöoikeuksia rajoitetaan tarvittavassa määrin. Rajoituksena verkkohäiriötilanteissa voi olla myös työaseman kytkeminen irti verkosta,
- muilta (*opiskelija, muu käyttäjä*) pääsääntöisesti suljetaan käyttäjätunnukset ja heidät kutsutaan keskustelemaan tietoturvapääallikön tai järjestelmästä vastaavan henkilön kanssa.

Käyttöoikeuksia on rajoitettava aina, kun on perusteltua syytä epäillä, että käyttäjä on syyllistynyt väärinkäyttöön, ja kun on mahdollista, että käyttöoikeudesta on haittaa rikkomuksen selvittämiseksi tai vahinkojen minimoimiselle.

Käyttöoikeuksien rajoittamisesta selvitystyön ajaksi päättää tietojärjestelmän omistaja, yksikön johtaja tai muu tehtävään nimetty henkilö ja rajoittamisen toteuttaa ylläpitäjä. Kiireellisissä tapauksissa ylläpitäjä voi omalla päätöksellään rajoittaa käyttöoikeuksia enintään kolmeksi päiväksi, mistä tulee välittömästi ilmoittaa rajoituksista vastaavalle henkilölle.

2 Seuraamukset

Lievimmissä tapauksissa käyttäjälle huomautetaan virheellisestä tai asiattomasta toiminnasta.

Tietotekniikkarikkomuksen seurauksena käyttäjä on korvausvastuussa yliopistolle aiheutetuista vahingoista, väärinkäyttämistään resursseista (esim. koneaika) että väärinkäytön selvitystyöstä aiheutuneista kustannuksista.

2.1 Opiskelijat

Opiskelijalle kohdistettavia seuraamuksia voivat olla tietojärjestelmien käyttöoikeuksien rajoittaminen (käyttäjätunnusten sulkeminen)¹, yliopiston sisäiset hallinnolliset toimet (kirjallinen varoitus, määräaikainen erottaminen)² sekä rikosilmoituksen tekeminen (epäiltäessä laissa rangaistavaksi määriteltyä tekoa).

Käyttäjätunnusten sulkemisesta päättää yliopiston nimeämä henkilö. Käytön rajoitusaikaan ei lasketa mukaan tunnusten sulkemista selvitystyön ajaksi.

Kirjallisen varoituksen antamisesta opiskelijalle päättää yliopiston rehtori ja määräaikaisesta erottamisesta yliopiston hallitus. Käyttöoikeudet perutaan erottamisen ajaksi. Käyttöoikeuksien rajoittamisen kokonaiskesto on kuitenkin vähintään liitteenä olevassa taulukossa esitetyn mittainen.

¹ Oulun yliopiston tietojärjestelmien käyttösäännöt

² Yliopistolaki 645/1997, 19§ ja Yliopistoasetus 115/1998, 20§

2.2 Henkilökunta

Henkilökuntaa koskevia seuraamuksia voivat olla yliopiston työ- ja virkamiesoikeudelliset toimet (kirjallinen varoitus, irtisanominen, palvelusuhteen purku) ³ sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot). Varoituksen antamisesta, irtisanomisesta tai palvelusuhteen purkamisesta päättää rehtori tai hallintojohtaja. ⁴ Käyttöoikeudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä johtuvan luottamuspulan synnyttyä evätä määräajaksi tai pysyvästi.

2.3 Muut

Muulle käyttäjälle kohdistettavia seuraamuksia ovat huomautus ja käyttöoikeuden rajoitus, käyttöoikeuden peruminen ja rikosta epäiltäessä rikosilmoituksen tekeminen.

3 Seuraamustaulukot

Liitteen taulukoissa annetaan suositukset tietotekniikkarikkomusten seuraamuksista yliopiston tutkinto-opiskelijoille, henkilökunnalle ja muille.

Taulukoissa on esimerkkejä tyypillisistä tietojärjestelmien käytön yhteydessä esiintyvistä rikkomuksista luokiteltuina rikkomuksen vakavuusasteen mukaan. Seuraamukseen vaikuttaa rikkomuksen vakavuuden lisäksi teon tahallisuuden aste.

Taulukon seuraamusruuduissa esitetään tahallisuuden ja vakavuuden perustella tapauskohtaisesti harkittavat seuraamustyytit: rikosilmoitus, hallinnolliset toimet ja tietohallinnon / muun yksikön toteuttamat toimet.

Jos käyttäjä on sekä opiskelija että henkilökuntaa, sovelletaan häneen henkilökunnan taulukkoa.

3.1 Käsitteitä

Rikoslain alaisen materiaalin oikeudeton käsittely:

- *rikoslain alaista materiaalia* ovat esimerkiksi lapsipornoa, eläimiin sekaantumista, raakaa väkivaltaa, rasismia tai kansankiihottamista sisältävä aineisto
- *käsittelyä* ovat mm. materiaalin levittäminen ja hallussapito

Tekijänoikeuslain alaista materiaalia on esimerkiksi musiikki, videot, sarjakuvat, elokuvat, pelit ja ohjelmistot.

Palvelu on toiminto, jota voidaan käyttää koneen ulkopuolelta. Esimerkiksi

- sähköpostipalvelu (liikenneprotokollat smtp, imaps, ...)
- tiedostonsiirtopalvelu (liikenneprotokollat ftp, http, scp, ...)

³ Virkamieslaki 750/1994, 24§, 33-34§, 40§ ja Työsopimuslaki 55/2001, 7 luku 2§, 8 luku

⁴ Oulun yliopiston henkilöstöpolitiikka: Toimivalta henkilöstöasioissa

-
- vertaisverkkopalvelu (liikenneprotokollat Kazaa, eDonkey, p2p, ...)

Tunnuksen luovuttamista on esim. salasanan kertominen toiselle käyttäjälle tai istunnon auki jättäminen niin, että joku toinen pääsee valvottomasti käyttämään järjestelmää toisen tunnuksella.

Tiedon luottamuksellisuuden vaarantamista ovat esim.

- ei-julkiseksi luokitellun tiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä, esim. palvelinten käyttäjätietojen luovutus
- ei-julkiseksi luokitellun tiedon tietoturvan laiminlyönti, esim. puutteelliset suojaukset järjestelmässä, jossa tietoa käsitellään
- salassapitorikokset
- henkilötietolain rikkominen

Henkilökohtaisen tietoturvan laiminlyöntiä on esimerkiksi salasanan jättäminen näkyviin.