

Voimaan: 28.10.2020	Vahvistaja: tietoturvapäällikkö Riitta Gröhn

A8 SUOJATTAVAN OMAISUUDEN HALLINTA

SISÄLTÖ

1 Suojattava omaisuus	1
2 Suojattavien kohteiden hallinta	1
3 Suojattavan omaisuuden vastuutaho	2
3.1 Suojattavan omaisuuden vastuullisen vastuut	2
3.2 Vastuiden delegointi	2
4 Kuinka suojattavia kohteita tulee käsitellä?	2
4.1 Määräysten velvoittavuus	2
4.2 Suojattavan omaisuuden hyväksyttävä käyttö	3
4.2.1 Tietojärjestelmät	3
4.2.2 Päätelaitteet	4
4.2.3 Tietoaineistot	4
4.2.4 Siirrettävät ulkoiset muistivälineet	4
4.3 Salassapito	5
5 Suojattavan omaisuuden palauttaminen	5
6 Fyysisten tietovälineiden siirtäminen	7
7 Tietovälineiden ja tietoaineistojen hävittäminen	7

1 Suojattava omaisuus

Suojattavaa omaisuutta ovat Aalto-yliopiston hallinnassa tai vastuulla oleva tieto ja tietojärjestelmät ja niihin liittyvät prosessit, järjestelmät, laitteet, palvelimet, päätelaitteet, ohjelmistot ja tietoverkot. Kyse ei ole vain Aalto-yliopiston omistamasta omaisuudesta, vaan myös omaisuudesta, joka on Aalto-yliopiston vastuulla.

Esimerkiksi työntekijöiden henkilötiedot eivät ole Aalto-yliopiston omaisuutta, koska Aalto-yliopisto on kuitenkin rekisterinpitäjänä vastuussa näiden tietojen suojaamisesta, niin ne katsotaan Aalto-yliopiston suojattavaksi omaisuudeksi.

2 Suojattavien kohteiden hallinta

Aalto-yliopiston tietojärjestelmät suojattavina kohteina on lähtökohtaisesti yksilöity ja luetteloitu konfiguraationhallintatietokantaan, CMDB:hen. CMDB:ssä ylläpidetään suojattavien kohteiden tietoja läpi suojattavan omaisuuden elinkaaren.

Aalto-yliopiston tiedonohjaussuunnitelmassa on tunnistettu yliopistossa käsiteltävät tietoaineistot.

3 Suojattavan omaisuuden vastuutaho

Suojattavalla kohteella on nimetty vastuutaho. Vastuussa suojattavasta kohteesta on toiminnosta vastaava.

3.1 Suojattavan omaisuuden vastuullisen vastuut

Suojattavan kohteen omistaja vastaa tietoturvallisuuden ja tietosuojan toteuttamisesta lakien, tietoturva- ja tietosuojasääntöjen sekä velvoittavien ohjeiden mukaisesti kohteen elinkaaren ajan sen käyttöön-otosta siitä luopumiseen. Tietoturvallisuuden hallintajärjestelmän velvoittavissa ohjeissa, säännöissä ja ohjeissa on tarkemmin kuvattu suojattavan kohteen omistajan vastuut.

3.2 Vastuiden delegointi

Vastuisiin liittyvät tehtävät voidaan delegoida muille henkilöille tai ulkoistaa nämä kolmannelle osapuolelle edellyttäen, että henkilöllä on riittävät valtuudet ja resurssit. Vastuuta ei kuitenkaan voi delegoida.

4 Kuinka suojattavia kohteita tulee käsitellä?

4.1 Määräysten velvoittavuus

Aalto-yliopistolla on tietojärjestelmien ja palveluiden omistajana ja työnjohto- ja valvontaoikeutensa perusteella oikeus antaa määräyksiä siitä, mihin ja miten sen työ- ja opiskelukäyttöön tarjoota palveluita käytetään. Määräysten velvoittavuus sisällytetään myös hankintavaatimuksiin ja yhteistyötahojen kanssa tehtäviin sopimuksiin tarvittavissa määrin.

Määräykset ovat Aalto-yliopiston IT-palveluiden tai Aalto-yliopiston yksiköiden antamia velvoittavia ohjeita. Tämän lisäksi on noudatettava lainsäädäntöä ja hyviä tapoja.

Määräykset koskevat:

- a) kaikkia yliopistoyhteisön jäseniä
- b) muita Aalto-yliopiston tietojärjestelmien käyttäjiä
- c) Aalto-yliopiston yksiköitä
- d) yliopistolla olevia yleisökäyttöisiä työasemia
- e) kaikkia yliopiston verkkoon liitettyjä laitteita

Määräysten valvonta

Valvonnasta vastaavat IT-palvelut (tietoturvaryhmä ja IT solution ownerit), suojattavien kohteiden omistajat sekä työjohtollisesti esimiehet kukin omalta osaltaan.

Tietoturvan ja tietosuojan vastaisen toiminnan seuraamukset

Henkilö vastaa itse toimintansa kaikista seurauksista ja vahingoista (ks. tietotekniikkarikkomuskäytäntö Aalto-yliopistossa).

Jos kyse on tilanteesta, jossa henkilöön ei voida soveltaa seuraamus-käytäntöä, niin tämä huomioidaan tarvittavilta osin sopimuksissa. Jos kyse on siviilipalvelusta suorittavasta henkilöstä, niin seuraamuksien määräämisessä noudatetaan valtionhallinnon ohjeistusta.

4.2 Suojattavan omaisuuden hyväksyttävä käyttö

4.2.1 Tietojärjestelmät

Yliopiston tietojärjestelmät on tarkoitettu työvälineeksi tehtäviin, jotka liittyvät opiskeluun, opetukseen, tutkimukseen, taiteen tekemiseen tai hallintoon Aalto-yliopistossa.

Yksityinen käyttö on sallittu kohtuullisessa määrin ja vain siltä osin kuin se:

- a) ei haittaa muuta järjestelmän käyttöä
- b) ei aiheuta muutostarpeita yliopiston tietojärjestelmissä
- c) ei ole ristiriidassa yksittäistä järjestelmää koskevien tai yleisten velvoittavien ohjeiden tai muun tietoturvadokumentaation kanssa
- d) ei ole laitonta tai hyvien tapojen vastaista

Sallittua kohtuullista yksityistä käyttöä ovat mm. yksityiset sähköposti-keskustelut ja muiden tehtäviin liittymättömien verkkopalveluiden käyttäminen.

Muu kuin yllä mainittu käyttö edellyttää kirjallista lupaa IT-johtajalta. Lupa myönnetään vain perustellusta syystä.

Erityisesti:

- a) kaupallinen käyttö muun kuin yliopiston lukuun on kielletty, mutta voidaan sallia nimenomaisella luvalla
- b) käyttö poliittiseen toimintaan (kuten vaalimainontaan) on kielletty, poikkeuksena ovat yliopistovaalit, ylioppilaskunnan toimintaan liittyvien poliittisten opiskelijajärjestöjen / alayhdistysten ja henkilökunnan ammattiyhdistysten yms. toiminta sekä ammatillinen yhteiskunnallinen vuorovaikutus
- c) käyttö uskonnolliseen tai vastaavaan vakaumukselliseen julistavaan toimintaan on kielletty
- d) laittoman tai hyvän tavan vastaisen materiaalin julkaiseminen, välittäminen tai jakelu on kielletty
- e) järjestelmän resurssien tarpeeton kuormittaminen on kielletty
- f) pääsyoikeuksia ei saa käyttää tietoturva-aukkojen etsimiseen ja hyödyntämiseen eikä tunnuksia saa antaa toisen henkilön käyttöön
- g) tietoliikennettä ei saa kopioida tai muuttaa
- h) järjestelmiin, hakemistoihin tai palveluihin ei saa tunkeutua
- i) tietojärjestelmissä olevien tietojen oikeudeton hankkiminen tai sen yrittäminen on kielletty
- j) vahingossa saatujen, muille osoitettujen tai kuuluvien tietojen hyväksikäyttö, talteenotto ja levittäminen on kielletty

- k) havaituista tai epäilyistä tietoturvallisuuden puutteista ja väärinkäytöksistä tulee ilmoittaa viipymättä (tietoturvapoikkeamat)
- l) työaseman tai palvelimen ulkopuolelle näkyvien palveluprosessien pystyttäminen edellyttää toiminnosta vastaavan lupaa
- m) yliopiston langalliseen tietoliikenneverkkoon saa kytkeä vain yliopiston omistamia tai hallinnoimia laitteita

4.2.2 Päätelaitteet

Päätelaitteiden hyväksyttävästä käytöstä on ohjeistettu Aalto-yliopiston päätelaitesäännössä. Pääperiaatteena on kuitenkin se, että vain Aalto-yliopiston yhteishallinnassa olevilla päätelaitteilla tulisi käsitellä Aalto-yliopiston tietoja, esimerkiksi hoitaa työtehtäviä.

Käyttäessään päätelaitteita, joilla käsitellään Aalto-yliopiston tietoja, on käyttäjä velvollinen huolehtimaan fyysisestä tietoturvallisuudesta (esimerkiksi laitteiden lukitseminen, kun ne jätetään valvomatta ks. A11) kuin myös tietoteknisestä tietoturvasta (esim. haittaohjelmia sisältävien sähköpostien tunnistaminen).

4.2.3 Tietoaineistot

Tietoaineiston käsittelystä on annettu ohje, jota tulee noudattaa. Henkilötietojen osalta tulee lisäksi noudattaa Aalto-yliopiston antamaa tarkempaa ohjeistusta henkilötietojen käsittelystä, joka löytyy Aalto.fistä.

Lisäksi TOS asettaa tietoon liittyviä velvollisuuksia. Tietyt tietoaineistot on esimerkiksi lähetettävä arkistoitavaksi sähköiseen asianhallintajärjestelmään. Lähtökohtaisesti esimerkiksi sopimukset on toimitettava kirjaamoon.

Yksityisen ja työhön liittyvän materiaalin erottaminen

Opiskelijan kotihakemistossa oleva aineisto tulkitaan aina yksityiseksi. Henkilökunnan tulee kuitenkin pitää yksityinen aineisto (esim. yksityiset sähköpostiviestit ja tiedostot) selkeästi erillään työhön liittyvästä aineistosta.

Jos henkilöllä on samanaikaisesti kaksi tai useampia rooleja, siten että henkilöllä on jokin toinen rooli työntekijäroolin lisäksi (esim. Aalto-yliopiston opiskelija), niin on huomattava, että häntä sitovat ensisijaisesti työntekijää koskevat määräykset hänen työskennellessään Aalto-yliopistolle (esim. salassapitovelvollisuus).

4.2.4 Siirrettävät ulkoiset muistivälineet

Siirrettäviä ulkoisia muistivälineitä hallitaan Aalto-yliopiston tietoaineistojen luokittelu- ja käsittelysääntöjen mukaisesti. Siirrettävän tietovälineen haltija on vastuussa sääntöjen noudattamisesta. Suojattavaa tietoaineistoa saa tallettaa siirrettävälle tietovälineelle vain poikkeuksellisesti ja vain kryptattuna velvoittavan ohjeen A10 mukaisesti.

Siirrettävän ulkoisen muistivälineen katoamisesta on viipymättä ilmoitettava tietoturvaryhmälle (security(at)aalto.fi).

Aalto-yliopiston tietojen käytössä tulee huomioida salassapitovelvollisuudet sekä hyödyntämiskiellot. Edellä mainitut voivat tapauksesta riippuen olla joko lakisääteisiä velvollisuuksia tai perustua Aalto-yliopiston tekemiin sopimuksiin.

Työntekijöiden ollessa kyseessä tulee erityisesti huomioida työntekijän lojaliteettivelvollisuus, jonka mukaan työntekijä ei saa toimia työnantajansa edun vastaisesti.

4.3 Salassapito

Työntekijöillä on salassapitovelvollisuus työssään tietoonsa saamistaan salassa pidettävistä tiedoista.

Opiskelijoilla ei ole yleistä salassapitovelvollisuutta. Opiskelijalla on kuitenkin salassapitovelvollisuus esimerkiksi sellaisista salassa pidettävistä tiedoista, jotka he saavat yliopiston luottamustehtävässä toimessaan tietää. Lisäksi opiskelijalta saatetaan edellyttää yksittäisessä opintoprojektissa salassapitositoumusta. Viestintäsalaisuutta koskevan lainsäädännön nojalla opiskelijallakin on salassapitovelvollisuus erehdyksessä saamastaan, toiselle henkilölle tarkoitettua viestistä.

Muiden tahojen osalta Aalto-yliopisto huolehtii salassapidosta huomioimalla sen tarvittaessa sopimuksissa, ellei kyseisellä taholla muun syyn nojalla ole salassapitovelvollisuutta.

5 Suojattavan omaisuuden palauttaminen

Kaikkien työntekijöiden, opiskelijoiden ja Aalto-yliopiston ulkopuolisten käyttäjien on lähtökohtaisesti palautettava kaikki hallussaan oleva Aalto-yliopiston suojattava omaisuus työtehtävän, työ- tai opiskelusuhteen tai sopimuksen päättyessä. Lainalaitteet tulee kuitenkin palauttaa jo ennen Aalto-yliopistosta poistumista sen mukaisesti, mitä lainalaitteista on ohjeistettu. Jos suojattavaa omaisuutta ei palauteta, niin käsitellään tätä tietoturvapoikkeamana Aalto-yliopistossa.

Tarpeellisilta osin suojattavan omaisuuden palauttamiseen liittyviä velvollisuuksia on tarkennettu ohjeistuksella.

Palauttaminen tarkoittaa aina kuitenkin vähintäänkin seuraavia asioita:

- Henkilön lähtiessä organisaatiosta hänen tulee palauttaa kulkuluvat ja laitteet
- Tieto-omaisuus tulee palauttaa. Tieto-omaisuus on palautettava myös henkilön henkilökohtaiselta laitteelta.

- Henkilön tulee poistaa yksityiset sähköpostit ja tiedostot ennen tietojärjestelmän käyttöoikeuden loppumista.
- Henkilön tulee poistaa yliopiston kotikäyttöön tarjoamat, yliopistoyhteisön jäsenyyteen perustuvat ohjelmistot opinto-oikeuden tai palvelussuhteen päättyessä, ellei ohjelmiston lisenssiehdoissa toisin mainita.
- Muiden lisenssien osalta on huolehdittava lisenssien palauttamisesta Aalto-yliopistolle tai lisenssien poistamisesta. Sama koskee lisensoituja käyttäjätunnuksia, jotka tulee poistaa järjestelmistä. Suojattavan kohteen omistajalla on velvollisuus vuosittain katselmoida lisenssit.
- Henkilökunnan tulee siirtää tarvittavassa määrin työhön liittyneet viestit ja tiedostot esimiehen kanssa sovitulle henkilölle. On huolehdittava toiminnan jatkumisen kannalta olennaisen tiedon siirtämisestä. Tämä pätee soveltuvin osin myös opiskelijaan, joka on toiminut esim. tutkimusryhmissä. On varmistettava, että kaikki olennainen tieto-omaisuus siirtyy Aalto-yliopistolle ja poistetaan henkilön omilta laitteilta.

Palautusvelvollisuus ei ole täysin absoluuttinen, mutta siitä ei voida poiketa kuin lainsäädännön tai lisenssiehtojen niin salliessa tai muusta perustellusta syystä.

Poikkeuksen yllä esitetystä säännöstä voivat muodostaa:

- lisenssit; Henkilön tulee poistaa yliopiston kotikäyttöön tarjoamat, yliopistoyhteisön jäsenyyteen perustuvat ohjelmistot opinto-oikeuden tai palvelussuhteen päättyessä, *ellei ohjelmiston lisenssiehdoissa toisin mainita*.
- Opiskelijoiden opintojensa aikana saamiin kurssimateriaaleihin, kuten luentodioihin, ei lähtökohtaisesti sovelleta palautus- tai poistamisvelvoitetta.

Jos kyse on niin sanotusta kolmannesta osapuolesta, niin kolmannen osapuolen (esim. toimittajan edustajan) tulee siirtää tai tuhota hankkeen toteuttamiseksi annettuun käyttäjätunnukseen liittyvät tiedot hankkeesta solmitun sopimuksen mukaisesti. Aalto-yliopiston sopijaosapuolen tulee informoida relevantteja toiminnoista vastaavia sopimussuhteen päättymisestä.

Suojattavan omaisuuden palauttamisessa huomioidaan myös salassapito sekä muut työsuhteen tai muun suhteen (esim. opiskelusuhteen) jälkeen voimaan jäävistä velvoitteista on tarvittavilta osin sovitava ja tiedotettava (ks. velvoittava ohje A7).

6 Fyysisten tietovälineiden siirtäminen

Tietoa sisältävät tietovälineet (esim. kannettavat tietokoneet ja älypuhelimet, palvelimet, muistitikut ja varmistusmediat) on suojattava luvattomalta pääsylvä, väärinkäytöltä ja turmeltumiselta siirron aikana Aalto-yliopiston tietoaineistojen luokittelu- ja käsittelyohjeiden sekä tarvittavilta osin muun tietoturvallisuusdokumentaation huomioiden (esim. etätyöohje) mukaisesti.

Osana normaalia yliopiston toimintaa tietovälineiden käyttöä valvotaan mm. tietoturvan osalta. Tietovälineen haltija vastaa kuitenkin siitä, että hän omassa käytössään noudattaa Aalto-yliopiston tietoturva- ja tietosuojadokumentaatiota.

7 Tietovälineiden ja tietoaineistojen hävittäminen

Tarpeettomat ja/tai käyttöikänsä loppuun tulleet tietovälineet on hävitettävä noudattaen Aalto-yliopiston tietoaineistojen luokittelu- ja käsittelysääntöjä ottaen huomioon lain viranomaisten toiminnan julkisuudesta (621/1999) ja arkistolain (831/1994) vaatimukset. Järjestelmän omistaja (suojattavan kohteen omistaja) ja siirrettävän tietovälineen haltija ovat vastuussa sääntöjen noudattamisesta.

Tietoaineistojen hävittämisessä noudatetaan TOS:sia.