TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

18.12.2011

# Tietoturvapolitiikka

## Johdanto

Tietoturvapolitiikka on ammattikorkeakoulun johdon kannanotto, joka määrittelee ammattikorkeakoulun tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot.
Ammattikorkeakoululla on sidosryhmiä, jotka asettavat vaatimuksia, velvoitteita, määräyksiä ja ohjeita tietoturvallisuuden suhteen. Tällaisia ovat mm. asiakkaat, sopimuskumppanit ja lainsäätäjä.

Tietoturvauhkien huomioiminen on tärkeää, koska ammattikorkeakoulun päivittäinen toiminta perustuu pitkälle tietojärjestelmien ja tietoverkkojen turvalliseen ja luotettavaan toimintaan. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Ammattikorkeakoulu suhteuttaa tietoturvatoimensa uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

## Tavoitteet ja päämäärä

### Tavoitteet

Tietoturvaa pitää jatkuvasti kehittää vastaamaan muuttuvia toimintariskejä, vaatimuksia ja ympäristöjä. Ammattikorkeakoulun tiedot, tietojenkäsittelyjärjestelmät, tietoverkko ja sen palvelut pidetään asianmukaisesti suojattuina normaali-, häiriö- ja erityistilanteissa sekä poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla.

### Päämäärä

Ammattikorkeakoulun tietoturvallisuustyön päämäärä on turvata ammattikorkeakoulun toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot.

## Tietoturvallisuuden käsite ja merkitys

Tietoturvallisuus tarkoittaa tietojenkäsittelyn turvaamista. Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua, toteuttamista, valvontaa, seurantaa ja ohjausta. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Tietoturvallisuus rakentuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä lisäksi soveltuvilta osin pääsynvalvonnasta ja kiistämättömyydestä.
**Luottamuksellisuus** tarkoittaa, että tiedot ovat vain niiden käyttöön oikeutettujen saatavissa sovituilla tavoilla ja sovittuun aikaan eikä niitä paljasteta tai muutoin saateta sivullisten tietoon.
**Eheys** tarkoittaa, että tiedot ja tietojärjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ole muuttuneet tai vahingoittuneet laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena.
**Käytettävyys** tarkoittaa, että tiedot ja tietojenkäsittelyjärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille, toiminnan kannalta hyväksyttävän ajan kuluessa.
**Pääsynvalvonta** tarkoittaa, että tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa.
**Kiistämättömyys** tarkoittaa todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen.

Tietoturvallisuus kattaa kaikenlaiset ammattikorkeakoulun tietojenkäsittelytehtävät sisältäen myös erityyppisten dokumenttien arkistoinnin. Tietoturvallisuustoimet koskevat sähköisessä, puhutussa ja kirjallisessa muodossa olevan tiedon käsittelyä, säilyttämistä, luovutusta ja siirtoa.

## Tietoturvatoimintaa ohjaavat tekijät

Ammattikorkeakoulun tietoturvallisuutta hoidetaan kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten pohjalta sekä valtionhallinnon tietoturvallisuudesta annettuja ohjeita ja suosituksia, että CSC - Tieteen tietotekniikan keskuksen tietoturvavaatimuksia, noudattaen.

### Yhteisötilaaja

Ammattikorkeakoululla on yhteisötilaajana velvollisuus huolehtia toiminnan turvallisuuden, tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistoturvallisuuden varmistamisesta. Ammattikorkeakoulu käsittelee viestintäverkossaan luottamuksellisia viestejä, tunnistamis- ja sidosryhmätietoja sekä henkilötietoja.
Ammattikorkeakoulussa käsitellään henkilötietoja, joista osa on arkaluontoisia, kuten opiskelijoita ja heidän terveydentilaansa koskevat arvioinnit (ammattikorkeakoululaki 351/2003). Tietojen käsittely ja luovutus eri sidosryhmille tulee ohjeistaa selkeästi. Ammattikorkeakoulun opetuksen eri osa-alueilla käsitellään todellisia työelämän tietoja, jotka ovat osin salassa pidettäviä, kuten potilas-, katsastus- ja tilitiedot sekä harjoittelupaikkojen ja opinnäytetöiden toimeksiantajaorganisaatioiden liikesalaisuudet. Ammattikorkeakoulu noudattaa toiminnassaan julkisuuslain (621/1999) mukaista hyvää tiedonhallintatapaa ja henkilötie-

tolakia (523/1999). Muita tietosuojan kannalta keskeisiä säädöksiä ovat sähköisen viestinnän tietosuojalaki (516/2004) ja yksityisyyden suoja työelämässä (759/2004).

Hyvä ylläpitotapa

Tietoturvallisuustyö omalta osaltaan toteuttaa tietojärjestelmien ja -verkkojen hyvää ylläpitotapaa, joka tarkoittaa suunnitelmallista, vastuuntuntoista ja ammattitaitoista ylläpitoa sekä, jossa otetaan huomioon julkisuuslaissa ja -asetuksessa säädetty hyvä tiedonhallintatapa.

## Vastuut

Vararehtori ja AMK:n hallitus

Tietoturvallisuutta johtaa ammattikorkeakoulun vararehtori. Hänen kanssaan ylin vastuu tietoturvallisuudesta on ammattikorkeakoulun hallituksella, joka vastaa tietoturvallisuuden toteutumisesta ja tarvittavien edellytyksien luomisesta.

AMK:n tietoturvaryhmä

Vararehtori nimittää tietoturvaryhmään kuuluvat henkilöt niin, että kaikki tietoturvaan liittyvät toiminnot ja vaatimukset tulee katettua. Tietoturvaryhmä edustaa ammattikorkeakoulun eri tahojen tietoturvanäkemyksiä, sovittaa yhteen tietoturvatoimenpiteet ja turvallisuustason sekä ohjaa tietoturvatoimenpiteitä.

Tietoturvaryhmän keskeisiä tehtäviä ovat riskianalyysin toteuttaminen, tietoturvallisuuden kehittämissuunnitelman laadinta ja sen toteutuksen seuranta, auditoinnin järjestäminen sekä johdon katselmuksen valmistelu.

AMK:n tietoturvavastaava

Ammattikorkeakoulussa on rehtorin päätöksellä nimetty tai toimintasäännössä määritelty ammattikorkeakoulun tietoturvavastaava. Ammattikorkeakoulun tietoturvavastaava vastaa tietoturvallisuuden seurannasta, raportoinnista, toteutuksen valvonnasta sekä kehittämishankkeiden toteutuksesta ja tietoturvatietouden edistämisestä. Ammattikorkeakoulun tietoturvavastaava toimii saamiensa resurssien ja toimintavaltuuksien puitteissa apunaan säännöllisesti kokoontuva tietoturvaryhmä, jonka puheenjohtajana toimii tietoturvavastaava.

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

18.12.2011

Toimipisteen tietoturvayhteyshenkilö

Tietoturvallisuuden toteuttamista ammattikorkeakoulun toimipisteissä ja niiden tietojenkäsittelyjärjestelmissä ohjaa ja valvoo nimetty toimipisteen tietoturvayhteyshenkilö.

Esimiehet

Esimiehet vastaavat siitä, että oma henkilökunta on selvillä tietoturvan vaatimuksista ja säännöistä sekä noudattaa niitä. Esimies vastaa uusien työntekijöiden ja sijaisten perehdytyksestä yksikössä noudatettaviin tietoturva- ja tietosuojaperiaatteisiin. Esimies käsittelee vähäpätöiset ja tahattomat tietoturvarikkomukset. Kaikki merkittävät, törkeät ja tuottamukselliset tietoturva- ja tietosuojarikkomukset on saatettava tietoturvavastaavan tietoon.

Tietojärjestelmien ja -verkkojen ylläpitäjä ja käyttäjä

Jokainen ammattikorkeakoulun tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on viime kädessä vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan.

Tietojärjestelmien ja tietojen omistaja

Tietojärjestelmän omistaja (haltija) vastaa mm. henkilötietolaissa mainitun rekisterinpitäjän velvollisuuksista sekä oman tietojärjestelmänsä tietoturvallisuudesta dokumentoinnin, turvaluokittelun, käyttäjäoikeusrekisterin ylläpidon, käyttöoikeuksien, käytön, varmistusten, tuen, koulutuksen, ylläpidon, kehittämisen ja jatkuvuussuunnittelun osalta sekä varautumisesta poikkeustilanteisiin. Vastuiden tunnettavuutta edistetään säännöllisin koulutuksin ja harjoituksin.

AMK:n yksiköt

Ammattikorkeakoulun yksiköt varautuvat oman ympäristönsä tietoturvallisuuden toteuttamisen kustannuksiin.

Alihankintasuhteet ja ulkoistaminen

Ammattikorkeakoulun tietoturvaa koskevasta vastuusta ja tietoturvavaatimuksista johdetut menettelyt ulotetaan alihankintasuhteisiin ja ulkoistettujen palvelujen toimittajaan.

**Toteutuskeinot**

Tietoturvallisuuden toteuttamisen perusta on tämä ammattikorkeakoulun johdon hyväksymä kirjallinen tietoturvapolitiikka, joka annetaan tie-

doksi ammattikorkeakoulun WWW-sivuilla ja intranetissä jokaiselle ammattikorkeakoulun henkilökunnan jäsenelle, opiskelijalle ja tietojärjestelmien käyttäjälle.

Riskikartoitus

Tietoturvallisuuden tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja teknisten ratkaisujen avulla. Ammattikorkeakoulun tietoturvallisuuden kehittämistarpeiden ja tavoitteiden määrittelemiseksi tietoturvaryhmä kartoittaa ammattikorkeakoulun tietoturvallisuusriskit säännöllisin väliajoin. Kartoituksen tavoitteena on tunnistaa toimintaa vaarantavat uhat, kartoittaa tietojenkäsittelyn haavoittuvat kohdat ja arvioida menetykset uhan toteutuessa sekä arvioida tietoturvallisuuden rakentamisen kustannukset riskien vähentämiseksi.

Tietoturvasuunnitelma

Tietoturvaperiaatteiden ja riskikartoituksen pohjalta tietoturvaryhmä laatii ammattikorkeakoulun tietoturvasuunnitelman, jota tarkistetaan säännöllisesti. Tietoturvaperiaatteet sisällytetään ammattikorkeakoulun kokonaisarkkitehtuuriin ja ne otetaan sitä kautta huomioon mm. tietojärjestelmähankinnoissa.

Tietoaineistojen ja tietojärjestelmien luokittelu

Tietoturvaryhmä huolehtii asiantuntijoita käyttäen ammattikorkeakoulun tietoaineistojen ja tietojärjestelmien luokittelusta tietoaineistojen luottamuksellisuuden ja tietojärjestelmien tärkeyden mukaan. Kullekin turvallisuusluokalle määritellään vaadittava tietoturvallisuustaso ja sen mukaiset tietoturvatoimenpiteet.

Tietojärjestelmän omistaja

Vararehtori nimeää jokaiselle tietojärjestelmälle tai sen osalle yksikäsitteisen omistajan. Järjestelmien perehdyttämisvastuu on järjestelmän omistajalla.

IT-toiminta

Perustietotekniikkaan liittyvästä teknisestä tietoturvasta vastaa IT-toiminta. IT-toiminnan yhtenä asiantuntijuusalueena on tietoturvallisuus. IT-toiminta osallistuu aktiivisesti tietoturvan suunnitteluun ja tietoturvatyön toteuttamiseen. IT-toiminta ylläpitää tietoturvaosaamistaan, joka on kaikkien yksikköjen käytettävissä. IT-toiminta järjestää tietoturvaan liittyviä asiantuntija- ja konsultointipalveluja. Tietoturvakoulutusta järjestetään yhteistyössä henkilöstökoulutuksesta vastaavien kanssa.

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

18.12.2011

Dokumentit

Tietoturvallisuuden toteuttamista ohjaavat dokumentit ovat vahvistettuja ja asianomaisten kohderyhmien saatavissa.

**Tiedottaminen**

Ammattikorkeakoulun tietoturva-asioista tiedottamisesta ammattikorkeakoulun ulkopuolelle ja ammattikorkeakoulun sisällä yleisellä tasolla vastaa ammattikorkeakoulun tietoturvavastaava. Toimipisteiden sisäiseen tiedottamiseen osallistuvat myös toimipisteiden tietoturvayhteyshenkilöt.

Tietoturvaryhmä tiedottaa ammattikorkeakoulun opiskelijoille ja henkilökunnalle tietoturvallisuudesta ja heitä koskevista säännöistä ja ohjeista.

**Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely**

Tietoturvallisuuden toteutumisen valvonta

Tietoturvasta vastaamaan nimetyillä henkilöillä on ammattikorkeakoulun valtuutus ja velvollisuus tehdä ammattikorkeakoulun tietojärjestelmien tietoturvallisuuden kartoituksia ja ryhtyä toimenpiteisiin havaittujen tietoturvallisuuden heikkouksien parantamiseksi.

Jokainen ammattikorkeakoulun tietojenkäsittelyjärjestelmien käyttäjä on velvollinen noudattamaan hyväksyttyjä käyttösääntöjä ja tietoturvaohjeita.

Toiminta häiriötilanteissa ja raportointi

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista toimipisteensä tietoturvayhteyshenkilölle tai suoraan ammattikorkeakoulun tietoturvavastaavalle.

Ammattikorkeakoulun tietoturvavastaava raportoi ammattikorkeakoulun ylimmälle johdolle ja tarvittaessa johtoryhmälle vakavista tietoturvallisuuden rikkomisista tai sellaisten epäilyistä.

Tietoturvapolitiikka tulee voimaan hyväksymispäivänä.
Turussa 18.12.2012

Juha Kettunen
rehtori