Metropolia Ammattikorkeakoulun tietoturvapolitiikka

Sisällysluettelo

Hallinnolliset tiedot

Otsikko: Metropolia Ammattikorkeakoulun tietoturvapolitiikka
Versio: Ensimmäinen versio
Voimassaolopäivämäärä: 8.3.2024
Omistaja(t): Metropolia Ammattikorkeakoulun johtoryhmä
Hyväksyjä(t): Metropolia Ammattikorkeakoulun johtoryhmä
Luokitus: Julkinen
Kohdeyleisö: Metropolia korkeakouluyhteisö
Muutoshistoria:

- Ensimmäinen versio on julkaistu 13.6.2022
- Toinen versio on julkaistu 25.3.2024

Määritelmät

Tieto-omaisuus = Mikä tahansa tieto, jolla on arvoa organisaatiolle ja joka tästä syystä edellyttää suojaamista. Tieto-omaisuus olisi tunnistettava ottaen huomioon se, että tietojärjestelmä koostuu suojattavista toiminnoista, prosesseista ja tiedoista.

Tieto-omaisuuden omistaja = Henkilö tai taho, joka vastaa tieto-omaisuudesta ja määrittää sen käytöstä hallinnoijalle ja käyttäjälle. Tieto-omaisuuden omistajalla on vastuu ja valtuudet hallita tieto-omaisuuteen kohdistuvia riskejä, esimerkiksi tietosuojalainsäädännön mukaisesti.

Hallinnoija = Hallinnoijalla tarkoitetaan kaikkia korkeakoulun palveluiden teknisestä ylläpidosta vastaavia henkilöitä sekä muita henkilöitä, jotka vastaavat järjestelmien hallintaan liittyvistä toimista sekä käyttäjien tuesta ja ohjauksesta tieto-omaisuuden omistajan määrittelemien kriteerien mukaisesti. Laajasti ymmärrettynä hallinnoijalla tarkoitetaan jokaista henkilöä, jolla on laajoja oikeuksia järjestelmään riippumatta järjestelmän käyttötarkoituksesta. Hallinnoijaksi lasketaan myös opiskelija, jos hän hallinnoi korkeakoulun tietojärjestelmää tai palvelua.

Käyttäjä = Viittaa Metropolia-tunnuksen omaavaan henkilöön, jolla on pääsy tieto-omaisuuden äärelle tieto-omaisuuden omistajan määrittämien kriteerien mukaisesti. Hallinnoijat vastaavat käyttöoikeuksien myöntämisestä käyttäjille.

Tietoturva = Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.

Lievä tietoturvapoikkeama= Tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan. Lievät tietoturvapoikkeamat eivät johda jatkuvuudenhallinta- ja toipumissuunnitelmien aktivoimiseen. Esimerkkejä lievästä tietoturvapoikkeamasta ovat palvelunestohyökkäysyritykset, henkilökohtaisen tietoturvan laiminlyöminen, laitteiston tietoturvapäivityksen laiminlyöminen ja kulunvalvontasääntöjen rikkomukset.

Vakava tietoturvapoikkeama = Yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti. Vakavat tietoturvapoikkeamat johtavat jatkuvuudenhallinta- ja toipumissuunnitelmien aktivoimiseen. Esimerkkejä vakavasta poikkeamasta ovat palvelunestohyökkäys, kiristyshaittaohjelma, raju sääilmiö, sähkökatkos, tietomurto sensitiiviseen tietoon, toimitusketjuhäiriö, varastetut luottokorttitiedot ja ihmishengen vaarantuminen, esimerkiksi tieto-omaisuuden toimimattomuuden vuoksi.

Tiedon elinkaarisuunnittelu = Tietojärjestelmillä ja tietoturvallisuuteen liittyvillä tieto-omaisuudella on elinkaari, jonka aikana tieto-omaisuus perustetaan, määritellään, suunnitellaan, kehitetään, testataan ja toteutetaan, jolloin niitä käytetään ja ylläpidetään ja jonka päättyessä ne poistetaan käytöstä ja hävitetään. Tietoturvallisuutta olisi tarkasteltava kaikissa tieto-omaisuuden käytön vaiheissa.

Tietosuojapoikkeama = Henkilötietoihin kohdistunut oikeudeton puuttuminen, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittely- ja katseluoikeutta. Tietosuojapoikkeamasta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Aihe

Metropolian tietoturvapolitiikka on jatkuvasti ylläpidettävä ja päivitettävä kokonaisuus, joka sisältää korkeakoulun ydintoiminnan tarpeista lähtevän pelkistetyn politiikan (= tämä dokumentti) sekä siihen liitettävät ohjeet ja kaaviot. Tietoturvapolitiikka johdetaan Metropolian kokonaisriskienhallintapolitiikasta, jonka hyväksyy Metropolian hallitus. Tietoturvapolitiikkaa määrittää, miten tietoturva-asioita toteutetaan Metropoliassa sekä, millaiset roolit ja vastuut tietoturvaan sisältyy (Liite 1). Tietoturvapolitiikkaa ohjaa muun muassa Metropolian strategia, tietohallinnon strategia, lainsäädäntö, oppaat ja standardit (Liite 2). Tietoturvapolitiikan avulla Metropolia edistää toivotunlaista tietoturvakäyttäytymistä korkeakoulun kanssa asioidessa, jolloin niin metropolialaiset kuin sidosryhmät noudattavat tietoturvapolitiikan periaatteita. Tietoturvapolitiikassa välittyy Metropolian johtoryhmän visio tietoturvan hallintamallille.

Tavoitteet

Tietoturvan johtamisessa korostetaan ylimmän johdon vastuuta siten, että johdolla on oltava selkeä näkemys tietoturvan roolista ydintoiminnoille, ja että noudatettava tietohallintostrategia on riittävän liiketoimintalähtöinen. Tietoturvallisuuspolitiikan avulla Metropolian johtoryhmä ilmaisee tahtonsa ja näkemyksensä tietoturvasta. Metropolian toimintojen riippuvuus tietotekniikasta kasvaa jatkuvasti koko toiminnassa. Metropolian elintärkeitä toimintoja ovat oppimistoiminta, TKI-toiminta ja liiketoiminta. Metropolian IT-strategian yhtenä painopisteenä on tietoturvallisen kulttuurin luominen Metropolialle. Tieto-omaisuuden elinkaarisuunnittelulla varmistetaan omaisuuden asianmukainen käyttö ja tietoturva omaisuuden kaikissa käyttövaiheissa. Tietoturvaa toteutetaan koulutuksilla, ohjeistuksilla sekä laite- ja ohjelmistohankinnoilla. Tietoturvan kontrollitoimenpiteet muodostuvat Metropolian valitsemista teknisistä, organisatorisista, fyysistä ja henkilöllisistä hallintakeinoista. Metropolialla on korkeakouluna vastuu ylläpitää henkilöstön ja opiskelijoiden tietoturvaosaamista. Tietoturvallisuudesta on tulossa tärkeä kansalaistaito, joka koskettaa jokaista metropolialaista. Metropolia tavoittelee tietoturvassa ennakoivaan riskienhallintaan perustuvaa lähestymistapaa, jossa Metropolian riskinottohalukkuus on organisaatiotasolla matala. Metropolian riskinottohalukkuus on matala esimerkiksi lain- ja vaatimustenmukaisuuden sekä turvallisuuden osalta. Tietoturvan riskienhallinta sisältää riskien tunnistamisen, arvioimisen sekä käsittelemisen Metropolian johtoryhmän hyväksymän tietoturvan hallintamallin ja Metropolian hallituksen puoltaman riskienhallintapolitiikan mukaisesti. Tiedon käsittely perustuu tiedon luonteen tunnistamiseen ja riskiarviointiin sekä lainsäädännön asettamiin vaatimuksiin. Tietoturvapolitiikan, tietoturvan toimintaperiaatteiden ja riskikartoituksien avulla kehitetään korkeakoulun tietoturvan hallintamallia tieto-omaisuuden suojelemiseksi.

Vastuut

Opiskelijat, henkilöstö, yhteistyökumppanit ja sidosryhmät ovat vastuussa sääntöjen noudattamisesta. Sen lisäksi jokaisen opiskelijan ja henkilökuntaan kuuluvan on ilmoitettava esimiehelleen/tietohallinnolle havaitsemistaan tietoturvallisuusriskeistä, poikkeama- tai vaaratilanteista, kuten vakavista tietoturvapoikkeamista. Jokaisen työntekijän ja opiskelijan vastuulla on suorittaa korkeakoulun perustasoinen tietoturvakurssi. Niin opiskelijoille kuin henkilökunnalle tarjotaan säännöllistä tietoturvakoulutusta. Tieto-omaisuuden omistaja vastaa tieto-omaisuudestaan ja sen käytöstä. Hallinnoija, kuten pääkäyttäjä, hallinnoi tieto-omaisuutta tieto-omistajan asettamien kriteerien mukaisesti, esimerkiksi kontrolloimalla tieto-omaisuuden

käyttöoikeuksia. Käyttäjän velvollisuus on työskennellä tieto-omaisuudella tieto-omistajan määrittämien sääntöjen mukaisesti. Tietohallinnon vastuulla on kehittää Metropolian tietoturvaa.

Viestintä

Mikäli julkista tiedottamista tarvitaan, siitä päättää Metropolian johtoryhmä yhdessä viestinnän kanssa. Sisäisestä viestinnästä vastaa tietohallinto. Huoltotöistä tiedotetaan tietohallinnon Wiki-sivulla ja tarpeen mukaan kohdennetulla tiedotteella OMA-intranetissä. Palvelun tai tietojärjestelmän hallinnoija vastaa palvelukohtaisten erityispiirteiden viestinnästä tietohallinnolle.

Seuraamukset ja vaatimustenmukaisuus

Tietotekniikkarikkomukseksi katsotaan sellainen toiminta, joka rikkoo Metropolian asettamia sääntöjä tietopalveluiden käyttämiseksi, tietoturvan toimintaperiaatteita tai sellainen toiminta, joka on Suomen lakien vastaista. Tietohallinnossa käydään kerran vuodessa läpi tietoturvaan liittyvät toimintaperiaatteet ja ohjeistukset. Toimintaperiaatteita ja ohjeistuksia päivitetään kerran vuodessa tilanteen niin edellyttäessä. Tietoturvakartoituksia ja auditointeja teetetään ulkopuolisilla toimijoilla tarvittaessa. Tämä dokumentti katselmoidaan ja päivitetään tarpeen mukaan kerran vuodessa. Vastuu tietoturvapolitiikan katselmoinnista on tietohallintojohtajalla, jolla on mandaatti tehdä pieniä muutoksia politiikan sisällölle tarvittaessa. Mikäli tietoturvapolitiikka tai sen sisällölliset toimintaperiaatteet poikkeavat merkittävästi, esimerkiksi korkeakoulun uudesta strategiasta, niin päivitetylle tietoturvapolitiikalle on saatava johtoryhmän puolto. Tietohallintojohtaja raportoi tietoturvatilanteesta johdolle normaalin toiminnan arvioinnin ja suunnittelun yhteydessä sekä aina silloin, kun on aiheellista, kuten vakavassa tietoturvapoikkeamassa.

Liite 1 Tietoturvaroolit

Rooli	Vastuut
Metropolian hallitus	1. Vastaa organisaation riskienhallinnan asianmukaisesta järjestämisestä korkeakoulun riskienhallinnan toimintaperiaatteiden mukaisesti. 2. Käsittelee organisaation toimintaan liittyvät merkittävät riski ja epävarmuustekijät.
Johtoryhmä	1. Ymmärtää tietoturvallisuuden roolin ydintoiminnalle sekä osana kokonaisturvallisuutta. 2. Huolehtii, että korkeakoululla on tietoturvapolitiikka. 3. Avustaa toimitusjohtaja-rehtoria riskienhallinnassa ja turvallisuusasioissa. 4. Toimii Metropolian ylimpänä operatiivisena riskienhallintaelementtinä. 5. Vastaa organisaatiotason riskien tunnistamisesta ja ajantasaisen riskitiedon hyödyntämisestä jokapäiväisessä johtamisessa.
Tietohallintojohtaja	1. Vastaa tietohallintotoiminnon johtamisesta osana Metropolian toimintaa, lähtökohtana ammattikorkeakoulun toiminnan ja käyttäjien tarpeet. 2. Vastaa tietohallinnon prosesseista ja niiden kehittämisestä sekä IT-palvelutuotannon strategisesta johtamisesta ja organisoinnista. 3. Korkeakoulun tietoturvallisuuden kokonaisvaltainen kehittäminen, ohjaaminen, seuranta ja johtaminen. 4. Määrittelee korkeakoulun tietohallintostrategian.
Johtajat, päälliköt ja esihenkilöt	1. Vastaavat oman organisaatioyksikkönsä (osastonsa, ryhmänsä, vastuualueensa) tietoriskeistä ja niiden hallinnasta. 2. Ilmoittavat ja raportoivat tietoriskeistä, joiden hallintaan tarvitaan lisätoimenpiteitä.

Hankkeen tai projektin omistaja, hanke/projektipäällikkö, työryhmän vetäjät sekä tutkimus- ja tietoaineistojen käsittelijät	1. Vastaa tietoturvasta ja tietoriskienhallinnasta osana hanke-/projekti/työryhmähallintoa. Tutkimus- ja tietoaineiston käsittelijä vastaa oman työnsä asianmukaisesta tietoturvan toteutumisesta. Hankkeiden, projektien ja työryhmien riskienhallinta sisältää erityisesti työn läpiviemiseen ja tavoitteiden saavuttamiseen liittyvien tietoriskien tunnistamisen, analysoinnin, käsittelyn ja raportoinnin.
Käyttäjätuki	1. Vastaa tietokoneiden ja mobiililaitteiden hankinnoista ja asennuksesta sekä ohjelmistojen ylläpidosta, asennuksesta ja henkilöstön ohjeistamisesta.
Järjestelmäylläpito	1. Vastaa tietoteknisen infran toiminnasta ja kehittämisestä pääalueinaan Windows- ja Linux-palvelinympäristöt, data- ja konesalit.
Tiedonhallinta- ja järjestelmäpalvelut	1. Kehittää, hankkii ja toteuttaa yhteisiä prosesseja tukevia tietojärjestelmiä. 2. Vastaa tiedon oikeellisuudesta ja ajantasaisuudesta järjestelmissä.
Tietoturva-asiantuntija	1. Tietoturvan hallintamallin ylläpitäminen ja tietoturvan jalkauttaminen Metropolian toimintaan. Samalla hän vastaa henkilöstön kouluttamisesta, neuvonnasta, ohjeiden ylläpitämisestä sekä vakavien tietoturvapoikkeamien käsittelystä. 2. Seuraa tietoriskienhallinnan tilaa, koordinoi tietoriskienhallintaa ja menettelyiden yhdenmukaisuutta. Hän on tietoturvallisuuden hallintamallin asiantuntija eli henkilö, joka luo ja toteuttaa sekä ylläpitää ja jatkuvasti parantaa yhtä tai useampaa tietoturvallisuuden hallintajärjestelmän prosessia.

Tietosuojavastaava	1. On koko Metropolian organisaation tukena tietosuojatyön neuvonnassa, kehittämisessä ja seurannassa lainsäädännön mukaisesti. 2.Neuvoo DPIA-asioissa. Tietosuojavastaava on organisaation yhteyshenkilö tietosuoja-asioissa Tietosuojavaltuutetun toimiston suuntaan. 3.Tietosuojavastaava ilmoittaa vakavat tietosuoja- ja tietoturvapoikkeamatapaukset Metropoliasta Tietosuojavaltuutetun toimistolle (yhteyshenkilö TSV:n ja rekisteröityjen välillä).
Riskienhallintapäällikkö	1. Vastaa riskienhallinnasta, työsuojelusta ja kokonaisvaltaisesta turvallisuusjohtamisesta.
Henkilöstöpalvelut	1. Vastaa työsuhdeasioista, henkilöstökoulutuksien järjestämisestä, sekä uusien työntekijän perehdyttämisestä.
Henkilökunta & opiskelijat	1. Noudattavat Metropolian tietojärjestelmien käyttösääntöjä, ohjeistuksia ja tietoturvan toimintaperiaatteita. 2. Raportoi mahdollisista tietoriskeistä tai poikkeamatilanteista tietohallintopalveluille .
Konsultit, palveluyritykset ja kumppaniorganisaatiot	1. Noudattavat Metropolian tietojärjestelmien käyttösääntöjä, ohjeistuksia, tietoturvan toimintaperiaatteita ja parhaansa mukaisesti hyviä tietoturvatapoja. 2. Valvovat ja ylläpitävät toivottua tietoturvatasoa asioidessaan Metropolian kanssa. 3. Raportoivat tietoturva-asioista ja siihen vaikuttavista seikoista tietohallinnolle. 4. Noudattavat toimeksiantajan antamia sopimusvelvoitteita.

Liite 2 tietoturvapolitiikkaa ohjaavat asiakirjat

Lainsäädäntö

- Korkeakoulua ohjaava lainsäädäntö on eritelty Metropolian tietohallinnon verkkosivulla

Standardit

- *ISO 27001:2022, Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset*.
- *ISO 27002: 2022, Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.*
- *ISO 27005:2022, Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Ohjeita tietoturvariskien hallintaan.*
- *The NIST Cybersecurity Framework*
- *ISO 31000:2018, Riskienhallinta. Ohjeet.*
- *ISO 22313:2020, Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Ohjeistusta standardin ISO 22301 käyttöön.*

Oppaat

- Turvallisuuskomitean *KYBERTURVALLISUUDEN SANASTO*.
- Kyberturvallisuuskeskuksen ohjeet ja oppaat tietoturva-ammattilaisille.

Strategiat

- Metropolian strategia 2021 - 2030.*Osaamisen rohkea uudistaja ja kestävän tulevaisuuden rakentaja.*
- Metropolian tietohallinnon oma strategia ja painopistealueet.