Metropolian tietoturvan hallintamallin kattavuuslausunto ja soveltamisala

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 25.3.2024

Metropolian tietoturvan hallintamallin kattavuuslausunto ja soveltamisala
Kattavuuslausunto

25.3.2024

Määritelmät

Saatavuus = Ominaisuus, joka tarkoittaa, että valtuutetulla taholla on tarvepohjainen pääsy- ja käyttöoikeus tieto-omaisuuden hyödyntämiseksi.

Luottamuksellisuus = Ominaisuus, joka tarkoittaa, että luvattomilla henkilöillä, tahoilla tai prosesseilla ei ole pääsyä tieto-omaisuudelle eikä tietoja luovuteta tällaisille tahoille.

Eheys = Ominaisuus, johon sisältyy tieto-omaisuuden oikeellisuus ja kattavuus.

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.

Tietoturva = Järjestelyt, joilla pyritään varmistamaan tieto-omaisuuden saatavuus, eheys ja luottamuksellisuus.

Tietoturvan hallintamalli = Tietoturvallisuuden hallintamalli koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista ja toiminnoista, joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan.

Tietoturvan hallintamallin asiantuntija = Henkilö, joka luo ja toteuttaa sekä ylläpitää ja jatkuvasti parantaa yhtä tai useampaa tietoturvallisuuden hallintamallin prosessia.

Dokumentoitu tieto = tieto, jota organisaatiolla on tarve hallita ja ylläpitää, sekä tietoväline, joka tiedon sisältää.

Kattavuuslausunto; tietoturvallisuuden hallintamallin soveltamisala = Organisaation on päätettävä tietoturvallisuuden hallintajärjestelmän rajauksista ja soveltamisesta, jotta järjestelmän soveltamisalan voi määritellä. Kattavuuslausunto kuvaa, muun muassa organisaatiota ja sen toimintaympäristöä, sidosryhmien tarpeita ja odotuksia, sekä organisaation riippuvaisuuksia suhteessa muihin toimijoihin. Soveltamisala on oltava dokumentoituna tietona.

Tietoturvallisuuden hallinta = Johtamistapa, jolla organisaation tietoturvatoimenpiteitä ohjataan ja valvotaan. Tietoturvallisuuden hallinta ohjaa tietoturvan hallintamallia.

Tietoturvallisuuden jatkuva parantaminen = Tietoturvallisuuden hallintamallin jatkuvan parantamisen tarkoituksena on lisätä sen todennäköisyyttä, että tiedon luottamuksellisuuden, saatavuuden ja eheyden säilyttämiseen liittyvät tavoitteet täyttyvät. Jatkuvan parantamisen tarkoitus on löytää parantamismahdollisuuksia eikä olettaa, että nykyiset hallintatoimenpiteet ovat riittävän hyviä tai parhaita mahdollisia. Tietoturvan hallintamallia parannetaan korkeakoulun Metropolin laadunhallinnan PDCA-ympyräprosessin mukaisesti.

25.3.2024

Asiakirjan tarkoitus

Metropolia Ammattikorkeakoulu kehittää tietoturvaansa tietoturvan hallintamallin mukaisesti. Tämän asiakirjan tarkoituksena on dokumentoida korkeakoulun tietoturvan hallintamallin soveltamisala kattavuuslausunnon mukaisesti. Tietoturvallisuuden hallintamalli on järjestelmällinen lähestymistapa Metropolian tietoturvallisuuden laatimiseen, toteuttamiseen, käyttöön, seurantaan, katselmointiin, ylläpitoon ja parantamiseen korkeakoulun asettamien tavoitteiden saavuttamiseksi. Hallintamalli perustuu riskien arviointiin ja korkeakoulun riskien hyväksyntätasoihin, jotka on suunniteltu riskien tehokasta käsittelyä ja hallintaa varten. Tieto-omaisuuden suojausvaatimuksia analysoimalla ja suojauksen varmistamiseen soveltuvat teknologiset, organisatoriset, henkilöstölliset ja fyysiset hallintakeinot toteuttamalla voidaan myötävaikuttaa tietoturvallisuuden hallintamallin onnistuneeseen toteuttamiseen. Kattavuuslausunto on suunnattu erityisesti korkeakoulun ulkopuolisille sidosryhmille, jotka arvioivat Metropolian tietoturvan tasoa ja prosesseja.

Kattavuuslausunto

Kattavuuslausunnon soveltamisala

Kattavuuslausunnon piirin kuuluvat kaikki metropolialaiset, kuten korkeakoulun henkilökunta ja opiskelijat. Tietoturvan hallintamalli ulotetaan koskemaan koko korkeakoulua, johon kuuluvat muun muassa kaikki innovaatiokeskittymät, osaamisalueet ja muut korkeakoulun päivittäiseen pyörittämiseen tarvittavat hallinnolliset osa-alueet. Hallintamallia ja sen periaatteita sovelletaan kaikissa korkeakoulun tietopalveluissa. Hallintamallia toimeenpanee tietohallinto, jossa tietohallinnon johtotiimi päättää korkeakoulun tietoturvan ratkaisuista ja hallintakeinoista. Tietohallinnon johtotiimin on kuultava tietoturva-asiantuntijaa sekä tietoturvasta tietäviä, jotka toimivat tietoturvan hallintamallin asiantuntijoina. Tietohallinnon johtotiimi viestii säännöllisesti hallintamallin kehityksestä johtoryhmälle, esimerkiksi kaksi kertaa vuodessa. Johtoryhmän palautteen pohjalta hallintamallia kehitetään tietoturvan jatkuvan kehittämisen mukaisesti. Johtoryhmä toimii myös hallintamallin ylätason ohjausryhmänä. Näin tietoturvan hallintamalli mahdollistaa Metropolian liiketoimintalähtöisyyden tietoturvallisesti hyviä hallintatapoja noudattaen.

Kattavuuslausunnon ulkopuolella olevat

Metropolian tietoturvan hallintamallia ei sovelleta korkeakoulun sidosryhmien tietoturvakäytänteisiin. Kuitenkin Metropolia ohjeistaa, miten korkeakoulu toivoo sidosryhmien käyttäytyvän tietoturva-asioissa korkeakoulun kanssa, esimerkiksi noudattamalla Metropolian tietoturvapolitiikan periaatteitta.

Metropolian keskeisimmät sidosryhmät

Metropolia Ammattikorkeakoulun keskeisimmät sidosryhmät ovat Metropolian opiskelijoiden opiskelijakunta METKA, yhteistyöoppilaitokset, viranomaiset, ohjelmistotoimittajat, TKI-kumppanit ja yrityskumppanit.

Metropolia Ammattikorkeakoulun maantieteellinen sijainti

Metropolia Ammattikorkeakoulu sijaitsee pääkaupunkiseudulla Etelä-Suomessa. Metropolialla on neljä kampusta: Arabian ja Myllypuron kampukset Helsingissä, Karamalmin kampus Epoossa sekä Myyrmäen kampus Vantaalla.

Metropolian tietoturvan hallintamallin tavoitteet

Termi *tietoturvallisuus* perustuu yleensä siihen, että tieto katsotaan omaisuudeksi, joka on arvokasta ja joka siksi edellyttää asianmukaista suojausta, esimerkiksi suojaamista saatavuuden, luottamuksellisuuden ja eheyden menettämiseltä. Tarkan ja täydellisen tiedon asettaminen sitä tarvitsevien tahojen saataville edistää liiketoiminnan tehokkuutta. Metropolian tietoturvan hallintamallin periaatteet johdetaan Metropolian laajemmasta strategiasta ja arvoista, Metropolian eettisistä toimintaperiaatteista ja tietohallintopalveluiden asiakkaiden tarpeista. Konkreettisesti tietoturvan hallintamallilla toimeenpannaan tietohallinnon IT-strategian mukaisesti, jossa korkeakoulun tietoturvaa kehitetään ja jalkautetaan, esimerkiksi toimeenpanemalla tietoturvan hallintamallin hallintakeinot ja kullekin vuodelle asetetut tietoturvatoimenpiteet. Ennen kaikkea tietoturvan hallintamallilla tietohallinto haluaa viestiä noudatettavista tietoturvakäytännöistä selkeästi ja käyttäjälähtöisesti.

Seuranta ja valvonta

Kattavuuslausunto katselmoidaan tietohallintojohtajan kanssa vuosittain tietoturvapolitiikan tavoin. Dokumenttia päivitetään, mikäli Metropolian ylätason strategia tai tietohallinnon IT-strategian tavoitteet muuttuvat merkittävästi. Kattavuuslausunnolle on oltava johtoryhmän hyväksyntä. Uuden kattavuuslausunnon kirjoittaminen kuuluu Metropolian tietoturva-asiantuntijalle ja IT-johdolle.

Liite 1: Tietoturvan hallintamallin vastuutahot ja vastuut

Vastuutaho	Vastuu
Metropolian hallitus	Vastaa organisaation riskienhallinnan asianmukaisesta järjestämisestä kulloinkin voimassa olevan Metropolian riskienhallintapolitiikan mukaisesti. Lisäksi hallitus vahvistaa organisaation riskienhallintapolitiikan ja niihin liittyvät muutokset sekä käsittelee organisaation toimintaan liittyvät merkittävät riskit ja epävarmuustekijät.
Metropolian johtoryhmä	Toimii ylätason ohjausryhmänä tietoturvan hallintamallille ja ohjaa tietoturvallisuuden hallinnan tavoitteita. Johtoryhmä osoittaa sitoutumista tietoturvan hallintamallin asioihin, esimerkiksi katselmoimalla hallintamallin asioita säännöllisin väliajoin. Johtoryhmä toimii rehtorin tukena päätöksenteossa, linjaa laajemmat koko Metropoliaa koskevat riskienhallintakysymykset sekä päättää kriittisistä, merkittävistä tai muutoin keskeisistä riskien hallintakeinoista ja toimenpiteistä sekä niitä koskevista vastuista, aikatauluista, resursseista ja seurannasta.
Tietoturvan hallintamallin toimeenpanoryhmä	Toimeenpanee tietoturvan hallintamallia tietoturvan hallintamallin tavoitteiden mukaisesti. Hallintamallin toimeenpanemisesta vastaa tietohallinto, jossa päävastuu kuuluu tietohallinnon johtotiimille ja tietoturvan hallintamallin asiantuntijoille, kuten tietoturva-asiantuntijalle.
Tietohallinnon johtotiimi	Johtotiimin vastuulla on määrittää tietoturvan hallintamallin tavoitteet ja hallintakeinot. Tietohallinnon johtotiimi vastaa hallintamallin kokonaisratkaisuista.

Liite 2: Tietoturvan hallintamallin turvallisuuden osa-alueet ja vastuutahon rooli

Tehtävä	Vastuutaho
Fyysiset hallintakeinot	Tietoturvan hallintamallin fyysisestä turvallisuudesta vastaavat toimitilapalvelut. Riskienhallintapalveluilla ja tietohallinnolla on neuvoantava rooli fyysisten ja henkilöstöllisten hallintakeinojen toimeenpanemiseksi.
Henkilöstöön liittyvät hallintakeinot	Tietoturvan hallintamallin henkilöstöllisistä hallintakeinosta vastaa henkilöstöpalvelut. Riskienhallintapalveluilla ja tietohallinnolla on neuvoantava rooli fyysisten ja henkilöstöllisten hallintakeinojen toimeenpanemiseksi.
Teknologiset hallintakeinot	Tietoturvan hallintamallin teknologisten hallintakeinojen turvallisuudesta vastaa tietohallinto. Tietohallinto valvoo ja toteuttaa tietoturvan tekniset hallintakeinot.
Organisaatioon liittyvät hallintakeinot	Tietoturvan organisatorisista ja hallinnollisista hallintakeinoista vastaa tietohallinto, turvallisuus- ja riskienhallintapalvelut sekä Metropolian Johtoryhmä. Hallinnollisen turvallisuuden osa-alueessa käsitellään niitä menetelmiä, joilla tietoturvallisuuden hallinta jalkautetaan osaksi koko organisaation toimintaa. Hallinnollisen turvallisuuden kriteereillä pyritään siihen, että organisaatiolla on riittävän hyvin toimiva tietoturvan hallintamalli sekä menettelyt sen varmistamiseksi, että tietoja käsittelevä henkilöstö toimii asianmukaisesti.
Varautuminen ja jatkuvuudenhallinta	Tarpeen mukaan voidaan tapauskohtaisesti muodostaa koordinaatioryhmiä johtamaan tietyn ajallisesti tai toiminnallisesti rajautuvan kokonaisuuden riskienhallintaa. Tällaisen koordinaatioryhmän puheenjohtajana toimii toimitusjohtaja-rehtori tai hänen määräämänsä. Tietohallinto kehittää tietoturvan varautumista ja jatkuvuutta Metropolian tietoturvan hallintamallin mukaisesti normaalioloissa. Keskeisiä kriteereitä osa-alueella ovat varautumistoimenpiteet erilaisiin vakaviin häiriötilanteisiin, toiminnan jatkuvuussuunnitelmat sekä tietojärjestelmien toipumissuunnitelmat ja niiden harjoittelu. Jatkuvuudenhallinta liittyy läheisesti häiriöiden ja poikkeamatilanteiden hallintaprosesseihin.

Tietosuoja	Tietohallinnon vastuulla on huolehtia tietosuoja-asioiden toteutuminen Metropolian tietopalveluissa. Laki- ja arkistointipalveluilla sekä tietosuojavastaavalla on neuvoantava rooli tietosuoja-asioissa.
Riskienhallinta	Turvallisuusriskejä arvioidaan ja analysoidaan Metropoliassa käytössä olevan riskienarviointijärjestelmän mukaisesti, sekä tarvittaessa erillisten riskianalyysien avulla. Riskien kokonaisvaltaisella arvioinnilla pyritään jatkuvaan turvallisuustason paranemiseen. Riskienhallintapalvelut vastaavat Metropolian riskienhallinnasta. Tietoturvariskienhallinnassa tietohallinnolla on neuvoa-antava rooli.