

H liite nro 2

29.11.2018

Gradian tietoturva- ja tietosuojalinjaukset**Sisällysluettelo**

Yleistä tietoturvallisuudesta ja tietosuojasta.....	1
Tietoturva- ja tietosuojalinjausten velvoittavuus.....	2
Tietoturva- ja tietosuojalinjauksia.....	3
Tietoturvan ja tietosuojan osa-alueet	4
Tietoturvan ja tietosuojan hallinta ja organisointi	4
Lait, asetukset ja muu ulkoinen hallinta	4
Tietoturvan ja tietosuojan tavoitteet ja sisäinen hallinta	5
Organisointi ja vastuut.....	6
Seuranta.....	7
Rikkomukset ja seuraamukset.....	8
Voimaantulo ja allekirjoitukset	8

Yleistä tietoturvallisuudesta ja tietosuojasta

Tietoturva- ja tietosuojalinjaukset sisältävät ne periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Jyväskylän koulutuskuntayhtymässä tietoturvan ja tietosuojan toteuttamisessa ja kehittämisessä. Tietosuoja on olennainen osa tietoturvallisuutta, joka puolestaan on osa organisaation riskienhallintaa, sisäistä valvontaa ja turvallisuusjohtamista. Tietoturvallisuus ja tietosuoja lisäävät kuntayhtymän toiminnan laadukkuutta ja kokonaisturvallisuutta.

Yksityiskohtaisemmat ohjeet sisältyvät muihin kuntayhtymän antamiin ohjeisiin ja määräyksiin. Nämä annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmien käyttäjille.

Tietoturva- ja tietosuojalinjausten periaatteet perustuvat eurooppalaisiin, kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, tietosuojaa, henkilötietoja, rekistereitä, hyvää tiedonhallintapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin.

Tietoturvallisuus ja tietosuoja on juuri niin hyvä kuin sen heikoin lenkki. Tämä ei koske vain tekniikkaa, vaan myös jokapäiväiset toimintatapamme ja asenteemme vaikuttavat – ***vahvin lenkki on oikealla tavalla toimiva yksilö.*** Jyväskylän koulutuskuntayhtymän henkilökunta ja luottamushenkilöt sitoutuvat tietoturvan ja -suojan huomioivaan toimintaan ja toimivat tässä julkaistujen periaatteiden mukaisesti.

Mikä on tietoturvallisuus?

Tietoturvallisuus on luottamusta, eheyttä ja saatavuutta. *Luottamuksellisuus* takaa, että tieto on vain siihen oikeutettujen henkilöiden ja organisaatioiden saatavilla, eikä sitä paljasteta muille. *Eheydellä* tarkoitetaan tietojen säilymistä sellaisina kuin ne on alun perin tarkoitettu eli että tiedot eivät muutu tai tuhoudu järjestelmävian tai inhimillisen toiminnan vuoksi. *Saatavuus* takaa sen, että tietoon pääsevät käsiksi aina tarvittaessa ne henkilöt ja tahot, joilla siihen on oikeus. Lisäksi on pystyttävä *todentamaan* tietojen käsittelijöiden henkilöllisyys (esim. käyttäjätunnuksen ja salasanan avulla) sekä todistettava *kiistämättömästi* käyttäjien tapahtumat järjestelmässä (esim. lokitiedot).

Tietoturvallisuuden tarkoituksena on suojata sähköinen ja paperinen tietoaaineisto sekä tietojärjestelmät niiden koko elinkaaren ajan. Tietoturvallisuuteen vaikuttavia tekijöitä ovat käytetyt tekniikat, annetut ohjeistukset ja johtaminen.

Tietoturvatoinnin päämääriä ovat:

- turvata kuntayhtymälle tärkeiden tietoaaineistojen, tietojärjestelmien, tietoverkkojen sekä palveluiden toiminta sekä normaali- että poikkeusoloissa,
- estää tietojen luvaton käyttö ja luottamuksellisiin tietoihin pääsy henkilöiltä, joilla ei ole niihin riittäviä valtuuksia,
- estää tahaton tai tahallinen tiedon tuhoaminen tai vääristyminen,
- varmistaa, että tietoja käsitellään lakien, asetusten ja sopimusten mukaisesti sekä
- varmistaa henkilöstön riittävä tietoturvaosaaminen ja sitouttaa henkilökunta hyvän tietoturvan toteuttamiseen.

Tietoturvallisuus on osa jokapäiväistä toimintaa sekä työpaikalla että sen ulkopuolella. Tämä edellyttää kaikilta työntekijöiltä ja luottamushenkilöiltä vastuullista toimintaa, tietoturvan ohjauksen ja valvonnan organisointia sekä turvallista teknistä ympäristöä. Tietoturallinen toiminta on yksi tietosuojan toteuttamisen keinoista.

Mikä on tietosuoja?

Tietosuoja on osa Suomen perustuslain takaamaa yksityisyyden suojaa. Tietosuojalainsäädännössä suojan kohteena ovat yksityisyyden suojan ohella rekisteröidyn oikeudet ja vapaudet. Tietosuojan tarkoituksena on näin ollen turvata tiedon kohteen eli rekisteröidyn yksityisyys ja luottamus sekä edut, oikeudet ja vapaudet sekä oikeusturva.

Tietosuojaa toteutetaan noudattamalla tietosuoja-asetuksen tietosuojaperiaatteita. Tämän mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi sekä luottamuksellisesti ja turvallisesti. Henkilötietoja on kerättävä ja käsiteltävä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietoja on kerättävä minimimäärä henkilötietojen käsittelyn tarkoitukseen nähden. Henkilötiedot on aina tarvittaessa päivitettävä – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä. Lisäksi tiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Osa tietosuojaa on myös rekisteröidyn oikeuksien turvaaminen. Rekisteröidyllä on oikeus saada pääsy tietoon (nk. tarkastusoikeus), oikeus tietojen oikaisemiseen, oikeus tietojen poistamiseen, oikeus käsittelyn rajoittamiseen, oikeus siirtää tiedot järjestelmästä toiseen sekä vastustamisoikeus (artiklat 12-21). Osa oikeuksista on ehdollisia tai riippuvia henkilötietojen käsittelyperusteesta.

Tietosuojassa on siis kysymys rekisteröidyn oikeuksista ja vapauksista eli se suojaa ihmistä. *Tietoturvalle* puolestaan tarkoitetaan niitä teknisiä ja hallinnollisia toimenpiteitä, joilla rekisteröidyn oikeudet ja tiedot turvataan eli se suojaa tietoja.

Tietoturva- ja tietosuojalinjausten velvoittavuus

Tietoturva- ja tietosuojalinjaukset kertovat Jyväskylän koulutuskuntayhtymän tahtotilan tietoturva- ja tietosuoja-asioissa.

Koulutuskuntayhtymän strategian kriittiset menestystekijät toteutuvat noudattamalla tietoturva- ja tietosuojalinjauksia. Näitä sovelletaan kaikissa kuntayhtymän toiminnoissa. Linjaukset koskevat kaikkia organisaatiossa työskenteleviä ja se ulotetaan soveltuvin osin myös ulkopuolisiin palvelujen toimittajiin ja muihin sidosryhmiin.

Kuntayhtymässä on tietoturva- ja tietosuojalinjausten lisäksi tietoturvaan ja tietosuojaan liittyviä suunnitelmia, ohjeita ja menetelmäkuvauksia.

Tietoturva- ja tietosuojatoimenpiteitä kohdistetaan tarpeelliseksi katsottuihin kohteisiin. Tietoturva- ja tietosuojariskejä arvioidaan säännöllisesti, tunnistetuille riskeille kohdistetaan riskienhallintakeinoja ja riskienhallintatoimenpiteiden onnistumista seurataan.

Tietoturvan ja tietosuojan hallintamenetelmät kohdistuvat kaikkeen sekä manuaaliseen että sähköiseen tietojenkäsittelyyn ja pitävät sisällään myös puhutun ja kirjoitetun tiedon.

Tietoturva- ja tietosuojalinjauksia

Kuntayhtymän tietoturva- ja tietosuojatavoitteiden saavuttamiseksi asetetaan seuraavia peruslinjauksia:

- Organisaation niin paperisessa kuin sähköisessä muodossa olevat asiakirjat, työtilat ja työvälineet ovat **kuntayhtymän omaisuutta ja lähtökohtaisesti työntekoa varten**. Turvallisuutta ja organisaation etuja vaarantava toiminta on kielletty.
- **Palvelussuhteen päättyessä työntekijän on luovutettava kaikki koulutuskuntayhtymälle** kuuluva tietoaineisto ja työn suorittamiseen tarkoitetut tietovälineet (tietokone, tabletti, älypuhelin ja muut sähköisen tallentamisen välineet) työnantajalle.
- **Perehdytyksessä** käsitellään aina tietoturvallisuuden ja tietosuojan perusperiaatteet ja salassa pidettävän tiedon käsittelyyn liittyvät yleiset periaatteet. Kuntayhtymällä on lisäksi kirjalliset henkilöstön tietoturva- ja tietosuojaohjeet, jotka esimies antaa jokaiselle työntekijälle palvelussuhteen alkaessa. Ohjeet löytyvät myös intranetistä. Lisäksi jokaisen on suoritettava tietosuojan nettitesti. Testin suorittaneista pidetään kirjaa.
- **Jokainen työntekijä noudattaa** tietoturvallisuutta ja tietosuojaa koskevia ohjeita ja vastaa omalta osaltaan tietoturvallisuudesta ja tietosuojasta kuntayhtymässä.
- Organisaatiossa noudatetaan mahdollisuuksien mukaan **puhtaan pöydän ja kuvaruudun politiikkaa**. Arkaluonteiseksi luokitellut aineistot säilytetään lukituissa tiloissa tai niille kuuluvissa tietojärjestelmissä käyttäjätunnusten ja salasanojen takana silloin, kun niitä ei käsitellä.
- Organisaatiossa **käsitellään vain tarpeellisia henkilötietoja**.
- **Salassa pidettävien tietojen ja henkilötietojen käsittelyä** omilla yksityiskäyttöön tarkoitetuilla tietovälineillä tulee välttää. Näiden tietojen käsittely julkisissa tai yksityiseen käyttöön tarkoitetuissa pilvipalveluissa ei ole sallittua. Kuntayhtymän hyväksymien pilvipalveluiden käyttö on sallittua.
- **Pääsy- ja käyttöoikeudet** kuntayhtymän järjestelmiin ja tietoon annetaan vain henkilöille, joilla on työ- tai virkasuhde, opiskeluoikeus tai muu sopimussuhde koulutuskuntayhtymään tai muu erillisestä hakemuksesta myönnetty käyttöoikeus. Pääsy- ja käyttöoikeudet annetaan vain tehtävän edellyttämässä laajuudessa. Sopimussuhteen päättyessä pääsy- ja käyttöoikeudet poistetaan (tarkemmat ohjeet tietoverkon ja tietojärjestelmien käytösäännöissä). Oikeudet salassa pidettävään tietoon ja henkilötietoihin myönnetään vain tehtävän sitä edellyttäessä. Jokaisella on oikeus katsoa ja käyttää vain työn edellyttämiä tietoja.
- Tarvittavat **kriittiset toimet organisaation tietoturvallisuuden ylläpitämiseksi** toteutetaan viipymättä.
- Organisaation **tietoturva- ja tietosuoja-vaatimukset** sisällytetään soveltuvin osin **ostopalvelusopimuksissa** toimittajille. Palvelun toimittajan henkilöstön tulee noudattaa organisaation tietoturvaohjeita.
- Organisaatioon kohdistuvat **vakavat tietoturvaloukkaukset** annetaan lähtökohtaisesti **poliisin tutkittavaksi**.

Tietoturvan ja tietosuojan osa-alueet

Jyväskylän koulutuskuntayhtymän tietoturvallisuuteen ja tietosuojaan kuuluu seuraavia osa-alueita:

- Tietoturva- ja tietosuojalinjaukset.
- Tietoturva- ja tietosuojaorganisaatio.
- Henkilöstöturvallisuus, jolla varmistetaan organisaation kanssa toimivien henkilöiden sopivuus tehtäväänsä.
- Suojattavan omaisuuden hallinta, jolla varmistetaan, että omaisuus luetteloidaan, merkitään ja käsitellään oikein.
- Pääsynhallinnalla varmistetaan vain oikeutettujen henkilöiden pääsy tietoon.
- Salauksella suojataan tietojen luottamuksellisuutta, aitoutta ja eheyttä.
- Toimitilaturvallisuudella huolehditaan toimitilojen ja ympäröivien alueiden turvallisuudesta.
- Käyttöturvallisuudella huolehditaan tietojenkäsittelypalveluiden toteuttamisesta asianmukaisesti, turvallisesti ja häiriöttömästi.
- Viestintäturvallisuudella varmistetaan tietoliikenneverkkojen ja tietoliikenteen turvallisuus ja häiriöttömyys.
- Tietojärjestelmien hankinta-, kehitys- ja ylläpitokäytännöillä varmistetaan, että tietojärjestelmien turvallisuudesta huolehditaan kulloinkin oikealla tavalla niiden elinkaaren eri vaiheissa.
- Toimittajasuhteisiin liittyvät turvallisuusnäkökohdat.
- Tietoturvapoikkeamien hallinnalla varmistetaan, että toimintamalli niihin reagoimiseksi on johdonmukainen ja vaikuttava ja että loukkauksista ja häiriöistä viestitään tarvittavin tavoin.
- Jatkuvuuden hallinnalla huolehditaan tietoturvatavoitteiden huomioinnista jatkuvuussuunnittelussa.
- Vaatimustenmukaisuudella varmistetaan tietoturvallisuuden hallinnan yhdenmukaisuus säädösten ja sidosryhmävaatimusten kanssa.

Tietoturvan ja tietosuojan hallinta ja organisointi

Lait, asetukset ja muu ulkoinen hallinta

Jyväskylän koulutuskuntayhtymä on opetushallituksen sekä opetus- ja kulttuuriministeriön hallinnonalalla toimiva koulutusorganisaatio. Opetus- ja kulttuuriministeriö ja opetushallitus ohjaavat organisaation toimintaa mm. koulutuksen rahoituksella, koulutuksen järjestämisluvilla, valtakunnallisilla tutkintojen perusteilla sekä projekti- ja asiakohtaisilla valtionavustuksilla. Oman toimintansa ohjaamiseksi kuntayhtymä ylläpitää erilaisia strategisia tavoitteita.

Lisäksi Jyväskylän koulutuskuntayhtymän tietoturvan ja tietosuojan käytäntöjen tulee kaikilta osin noudattaa lakeja ja asetuksia, sopimusten velvoitteita ja turvallisuusvaatimuksia. Lainsäädäntö suojaa henkilötietoja usein tarkemmin kuin muita organisaation käytössä olevia luottamuksellisia tietoja.

Tietoturvasta, tietosuojasta ja arkaluonteisten tietojen käsittelystä on säädetty useissa eri laeissa, joista oleellisia tässä yhteydessä ovat:

- Kuntalaki (2015/410)
- Laki viranomaisten toiminnan julkisuudesta (1999/621)
- Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU:n tietosuoja-asetus, 2016/679)
- Tietosuojalaki (2018/tasavallan presidentin vahvistus puuttuu)
- Eurooppalainen sähköisen viestinnän tietosuoja-asetus (valmistelussa)
- Laki sähköisen viestinnän palveluista (ent. Tietoyhteiskuntakaari, 2014/917)
- Tiedonhallintalaki (lausuntokierroksella)
- Laki kansainvälisistä tietoturvaluotteluvelvoitteista (2004/588)
- Laki yksityisyyden suojasta työelämässä (2004/759)
- Arkistolaki (1994/831)
- Laki ammatillisesta koulutuksesta (2017/531)
- Lukiolaki (1998/629)
- Perusopetuslaki (1998/628)
- Laki taiteen perusopetuksesta (1998/633)
- Rikoslaki (1889/39)

Tietoturvaluutta ja tietosuoja ohjaavat myös hyvä tiedonhallintatapa sekä sidosryhmien kanssa laaditut sopimukset.

Koulutuskuntayhtymän tietoturvaluudessa noudatetaan salassa pidon osalta julkisuuslakia. Lähtökohtaisesti organisaatiossa syntyvä tieto on julkista. Julkisuuslain ja joidenkin erityislakien perusteella tieto voidaan määritellä salassa pidettäväksi. Salassapito voi perustua myös sopimuskumppaneiden kanssa laadittaviin sopimuksiin.

Tietosuojan osalta noudatetaan EU:n tietosuoja-asetusta sekä sitä tarkentavaa kansallista lainsäädäntöä.

Tietoturvan ja tietosuojan tavoitteet ja sisäinen hallinta

Tietoturva- ja tietosuojalinjausten tarkoituksena on ylläpitää organisaation tietoturvaluutta sekä suojata organisaation ja sen opiskelijoiden ja asiakkaiden tietoja.

Koulutuskuntayhtymän tietoturvaluudella ja tietosuojaalla varmistetaan tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien tavoitteiden täyttyminen, täytetään organisaatioon viranomaisena kohdistuvat vaatimukset, lisätään luottamusta kuntayhtymään yhteistyökumppanina sekä edesautetaan organisaation tavoitteiden saavuttamista.

Hyvin hallittu tietoturvaluutus ja tietosuoja mahdollistaa:

- organisaation strategioiden mukaisten tavoitteiden saavuttamisen
- luotettavien sähköisen asioinnin palveluiden ja viestinnän toteuttamisen organisaation henkilökunnalle, opiskelijoille, asiakkaille ja muille sidosryhmille
- nykyaikaisia joustavia etä-, matka- ja toimistotyöskentelyn tapoja tukevat työvälineet
- nopean toipumisen ja työskentelyn jatkumisen häiriöistä huolimatta

Organisaation tietoturva- ja tietosuoja-toimenpiteillä taataan häiriötön tietojenkäsittely, suojataan organisaation, opiskelijoiden ja asiakkaiden salassa pidettäviä tietoja sekä varmistetaan, että organisaation toiminnan kannalta keskeiset tiedot, tietojärjestelmät ja palvelut ovat aina saatavissa.

Jyväskylän koulutuskuntayhtymän tietoturvallisuuden ja tietosuojan hallinta- ja johtamisjärjestelmän tarkoituksena on tukea organisaation tietoturva- ja tietosuojalinjausten mukaisten tavoitteiden saavuttamista. Hallintajärjestelmä on kokoelma prosesseja, toimintatapoja, välineitä ja ohjeita, joilla varmistetaan, että tietoturvatöimenpiteet ja tietosuoja ovat kulloinkin oikein mitoitettu ja kohdistettu. Hallintajärjestelmän toimintaa parannetaan poikkeamien, auditointien, saatujen palautteiden, innovaatioiden ja muiden havaintojen kautta.

Tietoturvallisuuden ja tietosuojan hallintatavoitteista ylläpidetään dokumentoitua tietoa. Dokumentaatio voi olla asiakirjamuotoista, tietokannassa tai muussa muodossa, jossa tehdyt muutokset ovat hallittuja. Olennaiset hallintatavoitteita tai niiden saavuttamista koskevat muutokset käsitellään kuntayhtymän johtoryhmässä sekä yhteistoimintalain mukaisesti yhteistoimintamenettelyssä, jos muutos koskee henkilökuntaa. Kuntayhtymän johtaja voi tehdä vähäisiä täydennyksiä ja korjauksia hallintakeinoja koskeviin kuvailuihin tietosuojaryhmän esityksestä.

Organisointi ja vastuut

Tietoturvallisuus ja tietosuoja ovat osa organisaation riskienhallintaa. Jyväskylän koulutuskuntayhtymä noudattaa lakeja ja asetuksia sekä kehittää toimintaansa vastaamaan voimaan tulevia toimialan viranomaisuus suosituksia.

Organisaatiossa on seuraavat roolit ja vastuut tietoturvaluuteen ja tietosuojaan liittyen:

Kuntayhtymän hallituksella on ylin vastuu tietoturva- ja tietosuojalinjauksista. Sen tehtävänä on valvoa kokonaisturvallisuutta, riskienhallinnan ja sisäisen valvonnan toteutusta.

Kuntayhtymän johtaja vastaa tietoturvaluusasioiden ja tietosuojan johtamisesta sekä organisaatioon kohdistuvien vaatimusten säädösten mukaisuudesta. Kuntayhtymän johtaja päättää tietoturvaluuden ja tietosuojan operatiivisista linjauksista, organisoinnista, tehtävistä ja vastuista sekä nimeää turvaryhmän ja tietosuojaryhmän sekä tietosuoja- ja tietoturvaluavastaavat.

Kuntayhtymän johtaja on vastuussa kriisiviestinnästä ja nimittää kriisiviestinnän operatiivisen vastuuhenkilön. Linjausten hyväksymishetkellä operatiivisena vastuuhenkilönä toimii turvaryhmän puheenjohtaja (turvaluuspäällikkö), joka tarpeen mukaan konsultoi viestintäasiantuntijoita ja kutakin kriisiä koskevia asiantuntijoita. Kriisiviestinnän vastuut määritellään tarkemmin osana kuntayhtymän viestinnän (yhteyspalveluiden) tehtävien kuvausta.

Kuntayhtymän johtoryhmä käsittelee organisaation turvallisuuteen sekä valmius- ja varautumistoimintaan liittyvät suunnitelmat, raportit, kehityskohteet, politiikat, linjaukset ja ohjeet sekä sisäisen turvallisuuden organisaatiotasoiset asiat.

Turvaryhmä vastaa kuntayhtymän kokonaisturvallisuudesta yhdessä kuntayhtymän ja oppilaitosten johdon, Gradia Kiinteistöjen ja työsuojelutoimikunnan kanssa. Turvaryhmän vastuulla ovat erityisesti kriisitilanteiden hallinta sekä kiinteistö-, palo-, henkilö- ja ympäristöturvallisuus.

Tietosuojaryhmä vastaa tietoturvaluuden ja tietosuojan suunnittelusta, ohjeistuksesta ja valvonnasta yhdessä asiantuntijoiden kanssa sekä raportoi johdolle tietoturvalu poikkeamista.

Tulosaluejohtajat, yksikönjohtajat, koulutuspäälliköt ja muut esimiehet vastaavat tietoturvallisuudesta, tietosuojasta ja niistä tiedottamisesta oman yksikkönsä toiminnassa.

Digipalvelut vastaa operatiivisen tietoturvan kehittämisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta omassa toimintayksikössä ja sen ostamissa palveluissa sekä raportoinnista johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Digipalvelut vastaa myös yleisistä tietoturva-asioista tiedottamisesta yksikkönsä sisällä ja yksikkönsä ulkopuolelle. Tiedottaminen tehdään osin yhdessä tietosuojaryhmän sekä tietosuoja- ja tietoturvavastaavan kanssa.

Tietosuojavastaava seuraa ja valvoo yhdessä mm. tietosuojaryhmän ja tietoturvavastaavan kanssa, että tietosuoja-asetusta ja muita tietosuojalainsäädäntöä ja organisaation toimintamenettelyjä noudatetaan sekä on mukana tietosuojan kehittämisessä ja tietosuojatietouden edistämisessä.

Tietoturvavastaava seuraa ja ohjaa tietoturvallisuuden kartoittamista ja edistämistä yhdessä mm. Digipalveluiden, tietosuojaryhmän ja tietosuojavastaavan kanssa.

Jokainen kuntayhtymän henkilökuntaan kuuluva vastaa oman lähiympäristönsä ja tehtäviensä tietoturvallisuudesta ja tietosuojasta sekä annettujen ohjeiden noudattamisesta. Henkilökunta ilmoittaa havaitsemistaan puutteista, poikkeamista tai läheltä piti -tilanteista palveluportaalin tietoturvapoikkeamailmoituksella, intran Läheltä piti -lomakkeella tai kiireellisissä tapauksissa esimiehelleen.

Organisaation tietojärjestelmille määritellään omistaja sekä tekniset pääkäyttäjät ja sisällön pääkäyttäjät. Omistaja vastaa siitä, että tietojärjestelmästä on tarvittavat tietosuoja- ja tietojärjestelmäselosteet. Tietosuoja-asetuksen myötä on myös laadittava kuvaukset organisaation toteuttamasta henkilötietojen käsittelystä (seloste käsittelytoimista).

Seuranta

Jyväskylän koulutuskuntayhtymän tietoturvallisuuden ja tietosuojan hallintaa seurataan ja parannetaan jatkuvasti. Tietoturva- ja tietosuojalinjausten ja niitä tukevien ohjeiden valvonta on tärkeä osa organisaation sisäistä valvontaa.

Kuntayhtymässä tehdään tarvittaessa laajempia tietoturvan ja -suojan kartoituksia ja toimeenpannaan kehittämistoimia havaittujen heikkouksien parantamiseksi. Tarvittaessa voidaan käyttää asiantuntija-apua tietoturvallisuuden ja tietosuojan toteuttamisen varmistamiseksi. Päivittäisestä, operatiivisesta seurannasta, raportoinnista ja kehittämistoimista vastaa Digipalvelut johdolta saamiensa resurssien puitteissa.

Jokainen tietoja käsittelevä työntekijä, tietojärjestelmien ja sovellusten ylläpitäjä ja käyttäjä on vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan. Henkilöstön tietoturva- ja tietosuojaosaamista ylläpidetään ja lisätään tiedottein ja koulutuksin. Yksikön esimiesten tehtävänä on valvoa tietoturvallisuuden ja tietosuojan toteutumista omassa yksikössään. Esimiesten tehtävänä on vastata siitä, että työntekijöillä on oikeudet tehtävän edellyttämässä laajuudessa tarvittaviin tietojärjestelmiin ja tietoihin. Esimiehet myös huolehtivat siitä, että muutokset työtehtävissä huomioidaan käyttöoikeuksissa ja työ- tai virkasuhteen päättyessä käyttöoikeudet järjestelmistä poistetaan.

Jokaisen työntekijän velvollisuus on ilmoittaa havaitsemistaan tietoturvapoikkeamista ja -puutteista sekä epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista tietoturvapoikkeamailmoituksella (palveluportaali.gradia.fi) ja omalle esimiehelleen. Tietoturvapoikkeaminen käsittely ja hallinta kuvataan erillisessä ohjeessa. Havaittuja poikkeamia hyödynnetään tietoturvallisten toimintatapojen, prosessien ja teknisten ympäristöjen kehittämisen tukena. Mikäli poikkeamiin liittyy rikosepäily, hallintosäännön mukainen toimivaltainen viranhaltija päättää tutkintapyyntöön tekemisestä poliisille (yleensä kuntayhtymän johtaja tai talous- ja hallintojohtaja, opiskelijoihin liittyen rehtorit).

Tietoturvaan liittyvissä uhkatilanteissa digipalvelupäälliköllä on oikeus sulkea tiedossa oleva tietoliikenneyhteys, järjestelmä, tunnus tai laite (asiantuntijoiden avustuksella). Asianosaisia on viipymättä informoitava tehdyistä toimenpiteistä ja mahdollisista jatkotoimista.

Rikkomukset ja seuraamukset

Jyväskylän koulutuskuntayhtymän tietoturva- ja tietosuojatoiminnassa noudatetaan lakeja, asetuksia ja viranomaismääräyksiä sekä kuntayhtymän sisäisiä periaatteita ja ohjeita.

Kuntayhtymän tietoturva- ja tietosuojalinjauksia sekä niihin liittyviä ohjeita vastaan havaitut rikkomukset raportoidaan organisaation johdolle. Rikkomuksen tekijä saatetaan edesvastuuseen teostaan ja häntä vastaan ryhdytään rikkomuksen vaatimiin toimenpiteisiin. Tarkoituksellinen ohjeiden vastainen toiminta voi johtaa tapauksesta riippuen esim. viranhaltijalain, työsopimuslain tai rikoslain mukaisiin rangaistusseuraamuksiin (esim. puhuttelu, suullinen huomautus, kirjallinen varoitus, irtisanominen, palvelussuhteen purkaminen) sekä vahingonkorvauksiin asianomistajille.

Voimaantulo ja allekirjoitukset

Tietoturva- ja tietosuojalinjausten valmistelusta ja ylläpidosta vastaa kuntayhtymän tietosuojaryhmä. Kuntayhtymän johtaja voi tehdä linjauksiin vähäisiä täydennyksiä ja korjauksia tietosuojaryhmän esityksestä.

Nämä kuntayhtymän tietoturva- ja tietosuojalinjaukset on valmistellut tietosuojaryhmä yhdessä Digipalveluiden kanssa. Linjaukset on käsitelty:

- Gradian tietosuojaryhmässä 21.5.2018 ja 1.10.2018
- Kuntayhtymän yhteistyötoimikunnassa 31.5.2018 ja 12.10.2018

Hyväksytty Jyväskylän koulutuskuntayhtymän hallituksessa 29.11.2018.

Tietoturva- ja tietosuojalinjaukset tulevat voimaan heti ja korvaavat aiemmat versiot. Tämä ohje on voimassa toistaiseksi. Linjaukset tarkistetaan tarvittaessa niiden ajantasaisuuden varmistamiseksi. Asiakirja on julkinen.