Digiturvallisuuden hallinta

Kaupunginhallitus 4.12.2023

Sisällys

Digiturvallisuuden hallinta

Tämä asiakirja käsittelee digiturvallisuuden toteuttamista ja se annetaan kaupungin henkilöstölle ja luottamushenkilöille tiedoksi ja noudatettavaksi. Digiturvallisuuden hallinta on johdon hyväksymä ja se on voimassa toistaiseksi.

Digiturvallisuuden hallinta kokonaisuutena sisältää vastuiden ja roolien määrittelyt, keskeisen dokumentaation, työntekijöiden ja luottamushenkilöiden tietoturva- ja tietosuojakoulutukset sekä tietoturvan ja tietosuojan huomioimisen sopimuksissa. Lisäksi digiturvaa hallitaan erillisillä jatkuvuus-, toipumis- ja tietoturvankehittämissuunnitelmilla sekä riskienhallintasuunnitelmalla.

Käytäntöjä ohjataan tämän asiakirjan lisäksi käyttäjille suunnatuissa erillisissä tietoturvan, tietosuojan ja riskienhallinnan ohjeissa.

Turvallisuus rakentuu arjen käytänteistä, toiminnasta sekä henkilöstön asenteista. Turvallisuuskulttuuri ei ole koskaan valmis, se muokkautuu ja sitä muokataan ympäristössä tapahtuvien muutosten vuoksi ja organisaatiomme tarpeiden pohjalta. Digiturvallisuuden hallinta ottaa kantaa kaupungin sisäiseen toimintaan riskienhallinnan, henkilöstö- ja tilaturvallisuuden, varautumisen ja jatkuvuuden hallinnan, tietoturvallisuuden sekä tietosuojan osalta.

Vastuutaho	Vastuun sisältö	Tehtävät
Kaupunginhallitus	Johtaa kaupungin hallintoa.	Hyväksyy Digiturvallisuuden hallinta- asiakirjan.
Kaupunginjohtaja	Tietoturvallisuuden yleinen järjestäminen.	Nimeää kaupungin tietoturva- ja tietosuojaorganisaation. Nimeää tietosuojavastaavan.
Kaupungin henkilöstö ja luottamushenkilöt	Tietoturvallisuuden toteuttaminen jokapäiväisessä työssä.	Noudattaa kaupungin ohjeita, periaatteita ja linjauksia.

		Velvollisuus suorittaa tietoturva- ja tietosuojakoulutukset. Allekirjoittaa tietoturva- ja salassapitositoumuksen ja noudattaa sen sisältöä. Huolehtii ja vastaa työkäyttöön annetuista laitteista ja välineistä.
Tietosuoja- ja tietoturvaryhmä	Järjestää ja organisoi kaupungin digiturvallisuuden hallintaa, tietoturvaa, tietosuojaa ja riskienhallintaa.	Laatii yleisohjeet, määräykset ja suositukset digiturvallisuuden käytännön toteuttamisesta. Laatii ja toteuttaa erilaisia digiturvallisuutta vahvistavia suunnitelmia, hankkeita ja projekteja sekä vie niitä eteenpäin toimivalle johdolle.
Tietohallintojohtaja	Vastaa tietoturvallisuuden ja kyberturvallisuuden toimeenpanosta koko kaupungin tasolla ja ohjeiden ajan tasalla pysymisestä.	Toimii kaupungin tietoturvavastaavana. Avustaa palvelualueita ja tietojärjestelmän omistajia tietoturvan toteutuksessa. Vastaanottaa ilmoitukset mahdollisista tietoturvauhkista. Valvoo tietoturvan toteutumista.

		Päättää tarvittavista toimenpiteistä tietoturvauhkien torjumiseksi. Raportoi ja tiedottaa tietoturvaan liittyvistä asioista.
Tietojärjestelmän omistaja: Tietojärjestelmän omistajana toimii sen prosessin prosessinomistaja, jota tietojärjestelmällä tuetaan. Jos järjestelmä palvelee useampaa prosessia, noustaan omistajuudessa siihen tasoon organisaatiossa, että voidaan määritellä yksikäsitteinen omistaja	Vastaa tietoturvallisuuden ja tietosuojan toteutumisesta järjestelmässä.	Nimeää yksikön tietojärjestelmien vastuuhenkilöt. Huolehtii, että järjestelmän pääkäyttäjillä on riittävä tietoturva- ja tietosuojaosaaminen. Vastaa järjestelmän tietoturvallisesta käyttämisestä ja kehittämisestä.
Tietosuojavastaava	Seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita. Tietosuojavastaava on tehtävässään riippumaton ja raportoi suoraan rekisterinpitäjän ylimmälle johdolle. Tietosuojavastaava ei ole henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen rikkomisesta.	Antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille. Seuraa asetuksen noudattamista sekä tietosuojaan liittyvän tiedottamisen ja koulutuksen toteutumista. Antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo

		vaikutustenarvioinnin toteutusta. Rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa. Vastaanottaa henkilötietojen käsittelijöiden tekemät selosteet käsittelytoimista. Tekee kaupungin tieto-suojaloukkaus ilmoitukset tietosuojavaltuutetun toimistolle. Tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa.
Rekisterinpitäjä Henkilötietorekisterin vastuuhenkilö	Rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta koko käsittelyn elinkaaren ajan sekä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.	Rekisterin vastuuhenkilö tekee henkilörekisteriselosteen, toimittaa sen tietosuojavastaavalle ja julkaisee sen toiminnasta kertovilla Lahden verkkosivuilla ja vastaa kuntalaisten kyselyihin rekisterintiedoista. Vastuuhenkilö vastaa rekisteriselosteiden tietojen oikeellisuudesta ja vastaa rekisteröityjen kyselyihin ja pyyntöihin.

Turvallisuuspäällikkö	Riskienhallinnan vastuulla on tuottaa tietoa ja työkaluja riskienhallintaa toteuttaville tahoille. Riskienhallinta on koko organisaation vastuulla, eikä pelkästään erillisenä toimintona. Kaupungin johdon, tietosuoja- ja tietoturvaryhmän, työntekijöiden sekä muiden sidosryhmien on osallistuttava riskienhallintaan ja noudatettava sovittuja tietoturvaperiaatteita.	Riskienhallinta auttaa vastuutahoja riskien tunnistamisessa, arvioinnissa, luokittelussa seurannassa ja toimeenpanojen suunnittelussa.

Organisoituminen, tehtävät ja vastuut

Tietosuoja- ja tietoturvaryhmän nimeää kaupunginjohtaja. Ryhmän toiminnalla kaupunki pystyy vastaamaan tiedonhallintalain ja tietosuoja-asetuksen asettamiin tehtäviin. Jäsenten vastuulla olevien tehtäväalueiden nivoutuessa voimakkaasti yhteen, ryhmän toiminnan tuloksena syntyy kokonaiskuva kaupungin digiturvallisuuden tilanteesta.

Ryhmän tehtävänä on laatia yleisohjeet, määräykset ja suositukset digiturvallisuuden käytännön toteuttamisesta. Ryhmä laatii ja toteuttaa erilaisia digiturvallisuutta vahvistavia suunnitelmia, hankkeita ja projekteja sekä vie niitä eteenpäin toimivalle johdolle. Ryhmän puheenjohtajana toimii tietohallintojohtaja, ryhmä voi tarvittaessa kutsua kokouksiinsa asiantuntijoita.

Henkilöstö

Kaupungin henkilöstöllä sekä luottamushenkilöillä on vastuu omalta osaltaan digiturvallisuuden toteuttamisesta ja valvonnasta. Kaikilla kaupungin ympäristössä toimivilla on velvollisuus noudattaa tietosuoja- ja tietoturvaryhmän laatimia digiturvallisuuteen liittyviä sääntöjä, määräyksiä ja ohjeita.

Jokaisen tiedonkäsittelijän velvollisuus on viipymättä ilmoittaa tietoturvallisuuden puutteista, epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista esihenkilölle, tietoturvavastaavalle, tietosuojavastaavalle ja tietohallinnolle. Näiden perusteella tietohallintojohtaja voi tarvittaessa käynnistää kaupungin tietojenkäsittelyn turvallisuuteen liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi. Tietosuojavastaava tekee ilmoitusten perusteella tarvittaessa ilmoituksen tietosuojavaltuutetun toimistolle, mikäli tietoturvarikkomukseen liittyy henkilötietoja.

Periaate: Jos käytössä olevasta tietojärjestelmästä tai tiedon hallintatavasta on uhkaa kaupungin tietoturvallisuudelle, voi tietohallintojohtaja tietoturvavastaavan roolissa määrätä sille teknisiä tai hallinnollisia rajoituksia.

Tietoturvavastaava

Kaupungin tietoturvavastaavana toimii tietohallintojohtaja. Tietoturvavastaava huolehtii tieto- ja kyberturvallisuuden toimeenpanosta kaupungissa. Apuna työssä toimii kaupungin tietohallinto sekä tietosuoja- ja tietoturvaryhmä. Tieto- ja kyberturvallisuuteen liittyvästä sisäisestä tiedottamisesta vastaa tietoturvavastaava. Kaupungin digiturvallisuutta koskevat asiat eivät ole aktiivisen ulkoisen tiedottamisen aihe.

Periaate: Kaupungin tietojenkäsittelyä ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan omavalvonnan ja sisäisen tarkastuksen keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen, lain ja toiminnan vaatimusten mukaisuuden varmistamiseksi sekä parannettavien kohteiden havaitsemiseksi.

Tietoturvallisuus

Tietoturvan tarkoitus on suojata tietoaineisto ja tietojärjestelmät. Se tarkoittaa erilaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.

Tietojärjestelmiä hankittaessa noudatetaan Lahden kaupungin projektimallia, jossa on huomioitu tiedonhallintalaki (906/2019) ja sen määräykset, ennen projektin käynnistämistä.

Periaate: Kaupunki estää riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen valtuudettoman käytön, tahattoman tai tahallisen tiedon tuhoutumisen tai vääristymisen sekä turvaa tietojen ja oleellisten palveluiden käytön.

Tiedon luottamuksellisuudesta huolehtiminen

Tiedon luottamuksellisuudella tarkoitetaan, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Tämä tarkoittaa sitä, että käyttövaltuudet ovat vain sellaisten henkilöiden käytettävissä, joilla on oikeus niiden käyttöön. Käyttövaltuuksilla rajataan tiedonkäsittelyä siten, että tietoa pääsevät käsittelemään vain ne, joiden tehtäviin kulloinenkin tieto kuuluu.

Periaate: Kaupunki todentaa ympäristönsä käyttäjät hallinnollisin ja teknisin keinoin.

Tiedon eheydestä huolehtiminen

Tiedon eheydellä tarkoitetaan, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut. Eheydellä tarkoitetaan myös sitä, että tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia eivätkä ne muutu laitteisto- tai ohjelmistovikojen, luonnonilmiöiden tai tietojen tahattoman muuttamisen seurauksena. Se sisältää myös vaatimuksen tietojen täydellisyydestä ja tahattoman muuttamisen estämisestä.

Periaate: Työasemia ja ohjelmistoja päivitetään säännöllisesti. Laatutyöllä varmistetaan tietojen ajantasaisuutta sekä oikeellisuutta.

Tiedon käytettävyydestä huolehtiminen

Tiedon käytettävyydellä tarkoitetaan, että järjestelmien tiedot ja palvelut ovat niihin oikeutettujen henkilöiden käytettävissä määritellyissä vasteajoissa. Tiedon käytettävyydestä huolehtiminen tarkoittaa sopimuksia, suunnitelmia, toimenpiteitä ja teknisiä ratkaisuja, joilla taataan tietojen ja tietojärjestelmien saatavuus käyttäjälle.

Periaate: Tietojen käytettävyydestä huolehditaan sekä manuaalisesti, että automaattisesti järjestelmien avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan.

Tiedon todentamisesta huolehtiminen

Todentamisella eli autentikoinnilla tarkoitetaan henkilöiden ja järjestelmien luotettavaa tunnistettavuutta. Todentamisessa käytetään erilaisia teknisiä ratkaisuja kuten vahvaa tunnistautumista, salasanoja, sertifikaatteja ja avaintunnuksia.

Periaate: Henkilöiden ja järjestelmien todentamisesta huolehditaan erilaisin teknisin sekä manuaalisin ratkaisuin

Kyberturvallisuus sekä toiminnan jatkuvuus ja varautuminen

Kyberturvallisuudella tarkoitetaan teknisiä toimenpiteitä, joilla suojataan kaupungin digitaalista ympäristöä. Kaupungin ICT-palvelun tuottajan kanssa on yhteistyöllä laadittu tekninen ympäristökuvaus, jota parannetaan vuosittaisella kehittämissuunnitelmalla ja sen toteutuksella.

Kyberturvallisuuden osa-alueeseen kuuluu kaupungin toiminnan jatkuvuuden ja varautumisen varmistaminen. Tätä toteutetaan mm:

- Vastaamalla vuosittain valtakunnallisesti kerättävään digiturvallisuuden kokonaiskuva tiedon kartoitukseen.
- Osallistumalla vuosittain valtakunnallisesti järjestettävään tietosuoja- ja tietoturvaloukkausten hallinnan harjoitukseen.
- Vuosittaisilla varautumisen ja riskienhallinnan dokumenttien katselmoinneilla.

Kaupungin jatkuvuussuunnittelua tehdään vuosittain palvelualueiden johtoryhmissä. Tässä yhteydessä tunnistetaan erilaisia tietojärjestelmiin liittyviä riskejä. Tietojen turvallisesta käsittelystä sovitaan myös kaupungin tietoja käsittelevien organisaatioiden sekä muiden yhteistyökumppaneiden kanssa. ICT-palvelut tuotetaan tämän asiakirjan ja muiden tietoturvaan liittyvien ohjeiden ja määräysten mukaan. ICT-palvelujen tuotantoon liittyvistä teknisistä tietoturvatoimenpiteistä vastaa palvelujen tuottaja.

Tietojärjestelmän omistaja

Tietojärjestelmän omistajana toimii sen prosessin prosessinomistaja, jota tietojärjestelmällä tuetaan. Jos järjestelmä palvelee useampaa prosessia, noustaan omistajuudessa siihen tasoon organisaatiossa, että voidaan määritellä yksikäsitteinen omistaja.

Tietojärjestelmän omistajan vastuita ja tehtäviä:

- Omistaja vastaa tietoturvallisuuden ja tietosuojan toteutumisesta järjestelmässä.
- Omistaja nimeää yksikön tietojärjestelmien pääkäyttäjät.
- Omistaja huolehtii, että järjestelmän pääkäyttäjillä on riittävä tietoturva- ja tietosuojaosaaminen.
- Omistaja vastaa tietojärjestelmäselosteiden olemassaolosta, ajantasaisuudesta ja saatavuudesta.

Tietoturvavastaava ja tietosuojavastaava avustavat tarvittaessa hallinnollisten ja teknisten keinojen määrittelyssä.

Tietosuojavastaava

Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa. Tietosuojavastaava raportoi suoraan johdolle ja tietoturva- ja tietosuojaryhmälle.

Tietosuojavastaavaa tulee kuulla kaikkien tietosuojakysymysten käsittelyyn liittyvässä tekemisessä ja tehtäessä tietosuojaan vaikuttavia päätöksiä. Kaikki olennaiset tiedot tulee toimittaa tietosuojavastaavalle viipymättä, jotta hän voi antaa asianmukaisia neuvoja. Tällaisia tilanteita ovat mm. henkilötietojen käsittelyä sisältävien uusien toimintaprosessien luonti, hankkeiden ja projektien aloitus tai tietojärjestelmien uudistaminen ja hankinta. Mahdollisissa erimielisyystilanteissa toiminnasta vastaava dokumentoi perusteet, joiden vuoksi tietosuojavastaavaa ei kuulla tai hänen neuvojansa ei noudateta. Dokumentti toimitetaan tiedoksi tietosuojavastaavalle.

Jos tietoturvaloukkaus tai muu tietosuojaan liittyvä ongelma ilmenee, tietosuojavastaavaa kuullaan mahdollisimman nopeasti. Henkilöstö on velvollinen ilmoittamaan esihenkilölle ja tietosuojavastaavalle, henkilörekisterin vastuuhenkilö suoraan tietosuojavastaavalle. Sopimuksilla rekisterinpitäjän lukuun toimivat henkilötietojen käsittelijät velvoitetaan tekemään ilmoitus rekisterinpitäjälle ja tietosuojavastaavalle ilman aiheetonta viivytystä saatuaan niistä itse tiedon.

Lahden kaupungin henkilöstölle on käytössä tietosuojan intrasivu, jonka tiedoista ja päivittämisestä vastaa tietosuojavastaava. Kaupunkilaisille vastaava sivusto löytyy verkkosivuilta. Yhteydenottoja varten on osoite: tietosuoja@lahti.fi

Rekisterinpitäjä, henkilötietorekisterin vastuuhenkilö ja henkilötietojen käsittelijä

Rekisterinpitäjä on Lahden kaupunki, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään.

Henkilörekisterin vastuuhenkilö vastaa rekisterin tietosuojaperiaatteiden toteutumisesta, tiedon oikeellisuudesta, eheydestä ja hävittämisestä, kun tieto on tarpeetonta tietojen käsittelyn toteuttamista varten. Vastuuhenkilö tekee rekisteristä selosteen käsittelytoimista, julkaisee sen verkkosivuille toiminnasta kertovalle sivustolle sekä toimittaa yhden kappaleen tietosuojavastaavalle. Vastuuhenkilö vastaa rekisteröityjen kysymyksiin ja tiedusteluihin. Ilmoittaa tietosuojavastaavalle tietoturvaloukkauksesta tai sen epäilystä mahdollisimman nopeasti, kuitenkin viimeistään 48 h kuluessa.

Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun. Tällainen toiminta edellyttää sopimusta tai sopimuksen tietosuojaliitettä rekisterinpitäjän ja henkilötietojen käsittelijän välille.

Riskienhallinta

Kaikkiin edellä kuvattuihin digiturvan osa-alueisiin liittyy riskienhallinta. Organisaation jokapäiväisen toiminnan toteuttaminen ei voi tapahtua tarkoituksenmukaisesti, taloudellisesti ja turvallisesti ilman toimivaa riskien hallitsemista. Sen avulla organisaatio pystyy paremmin varmistamaan sille asetettujen strategisten tavoitteiden saavuttamisen sekä turvaamaan jokapäiväisen toiminnan niin fyysisessä kuin digitaalisessa toimintaympäristössä.

Lisäksi riskienhallinnan avulla organisaatio pystyy kustannustehokkaasti kohdistamaan digitaalisen turvallisuuden kehittämistoimet sen toimintaa eniten uhkaaviin kohteisiin ja osa-alueisiin. Ilman jatkuvaa riskienhallintaprosessia turvallisuuden kehittäminen tapahtuu pistemäisesti, osin hallitsemattomasti ja ilmeisiä toimintaa uhkaavia tekijöitä saattaa jäädä tunnistamatta.

Vastuualueet (palveluyksiköt) tarkastelevat vuosikellon mukaisesti riskejään. Vuosittain riskienhallintaa tehdään riskianalyysilla, joka on osa kaupunkitasoista riskienhallintaa. Riskit, niiden

analyysit ja hallintatoimet kirjataan yhteiseen riskienhallintadokumenttiin. Riskienhallinta on myös osa hankintoja.

Tietosuoja ja tietoturvallisuus nivoutuvat yhteen muun turvallisuuden kanssa. Toimitilaturvallisuus yhteiskäyttötiloineen ja kulunhallinta, monipaikkatyö, matkustaminen ja ulkopuoliset henkilöt sekä laitteistojen käyttäminen ja säilyttäminen joko tukevat tai heikentävät tietosuojaa ja tietoturvallisuutta.

Tietoturvatoimien riittävä ja oikea taso varmistetaan tietoturvallisuuden riskienhallinnan keinoin. Toimintaan, palveluihin ja järjestelmiin kohdistuva riskienarviointi toteutetaan säännöllisin väliajoin ja merkittävien muutosten yhteydessä. Tunnistettujen puutteiden korjaamiseen ja riskien pienentämiseen tarvittavat toimenpiteet kootaan tietoturvallisuuden kehittämisohjelmaksi. Korjaavien ja ehkäisevien toimenpiteiden suorittamisesta vastaavat tietojen ja tietojärjestelmien omistajat. Toimialojen ja muiden yksiköiden tietoturvatoteutukset kuvataan tarvittaessa erillisissä suunnitelmissa.

Toiminnan muutoksiin ja palveluiden tai järjestelmien hankintoihin sisällytetään riskien arviointi ja tietosuoja- ja tietoturvavaatimusten määrittely jo suunnitteluvaiheessa. Lisäksi valvotaan vaatimusten täyttymistä ennen hankkeen toteutuksen hyväksyntää. Keskeisiin hankkeisiin otetaan tietoturvallisuuden asiantuntija mukaan suunnittelun alkuvaiheista lähtien.