ROVANIEMEN KAUPUNGIN TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

ROVANIEMI

Sisällys

Johdanto

Tieto on keskeisessä roolissa Rovaniemen kaupungin toiminnassa ja palvelutuotannossa. Jotta tieto on tehokkaasti hyödynnettävissä, tiedonhallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa.

Lainsäädäntömuutokset, esimerkiksi EU:n yleinen tietosuoja-asetus, tietosuojalaki, EU:n saavutettavuusdirektiivi ja tiedonhallintalaki tähtäävät tietoturvan, tietosuojan, riskienarvioinnin, kokonaisarkkitehtuurin ja yhteentoimivuuden huomioimiseen suunnittelun aikaisessa vaiheessa. Suunnittelun kautta on mahdollisuus parantaa niin kustannustehokkuutta, tietojen käytettävyyttä kuin tietoturvallisuutta.

Tietoturvallisuuden toteutumiseksi organisaation tulee tunnistaa sen toiminnan kannalta elintärkeät palvelutehtävät sekä määritellä ja kuvata näiden turvaamiseksi riittävät tietoturvaperiaatteet. Tietoturvallisuuden toteutumista tukevat periaatteista johdetut käytännöt, joita ovat mm.:

- ✓ hanke ja projektisuunnittelun tietoturvan ja tietosuojan tarkastuslistat
- ✓ puite-, palvelu- ja toimitussopimukset sekä niihin liittyvät turvallisuus- tai tietoturvasopimukset
- ✓ henkilötietojen käsittelyn ehdot, käsittelytoimien kuvaukset
- ✓ dokumentit organisaation toimintaympäristön tietokriittisyydestä sekä keskeisistä palveluista, prosesseista ja toiminnoista sekä näiden jatkuvuuden ja toimintavarmuuden hallintamekanismeista.

Suunniteltujen ja kuvattujen käytäntöjen toteutumista valvotaan säännöllisesti.

Rovaniemen kaupunki määrittelee tässä politiikassa tietoturvallisuutta sekä tietosuojaa koskevat periaatteet ja linjaukset. Politiikka toimii perustana kaupungin tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tukea kaupungin toimintaan liittyvien tietojärjestelmien, palveluiden ja tietoverkkojen toiminta ja henkilötietojen asianmukainen käsittely arjen työssä.

Näitä periaatteita ja linjauksia sovelletaan kaikessa kaupungin toiminnassa, koskien koko henkilöstöä, luottamushenkilöstöä ja sidosryhmiä, joka työnsä tai toimeksiannon perusteella käsittelee Rovaniemen kaupungin omistamaa tai hallinnoimaa tietoa.

Tämä politiikka on kaupunkia sitova ja sitä tarkennetaan kaupunkitason sekä toimialojen omilla ohjeistuksilla ja määräyksillä. Tietoturvallisuudesta ja tietosuojasta ohjeistetaan myös sovellus- tai käyttötarkoituskohtaisilla ohjeilla.

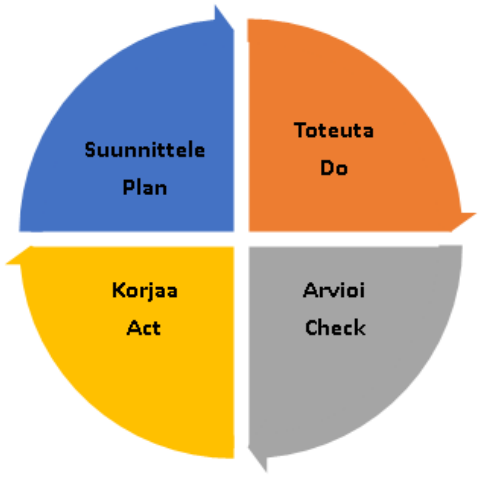
Tätä politiikkaa sovelletaan kaikkeen tietoon riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotiestä.

Politiikassa kuvataan Rovaniemen kaupungin tietoturvallisuuden ja tietosuojan periaatteet, tavoitteet, vastuut, organisoinnin ja toteutuskeinot. Lisäksi kuvataan seurannan ja tiedottamisen yleisperiaatteet.

Tämä tietoturva- ja tietosuojapolitiikka korvaa kaupunginhallituksen KH 7.10.2019 326 §:n päätöksen mukaisen tietoturvapolitiikan.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi. Asiasisältöä tarkistetaan ja sitä voidaan tarvittaessa täydentää tai päivittää lainsäädännön tai muiden ohjeistusten muuttuessa.

Tietoturva- ja tietosuojapolitiikka on julkinen asiakirja. Tämä politiikka on saatavissa asianhallintajärjestelmässä ja Intranetin tietosuoja ja tietoturva -sivulla. Politiikka liitetään tarvittaessa Rovaniemen kaupungin toimeksiantosopimuksiin ja huomioidaan hankinnoissa.



Kuvio 1. PDCA – toimintamallilla ylläpidetään tietoturvallisuuden ja tietosuojan riittävän hyviä toimintakäytäntöjä yksityisyyden turvaamiseksi.

Tietoturvallisuudesta ja tietosuojasta huolehtiminen on jatkuva prosessi, jonka perustana on riskienhallintaprosessin riskikartoitus. Prosessin toteutukseen kuuluu PDCA-mallin mukaisesti myös raportointi ja seuranta vaikuttavuuden ja muutostarpeiden toteamiseksi.

Kuviossa 1 on tietoturva- ja tietosuojan prosessimalli (PDCA-malli), jossa

Suunnittelu (Plan) sisältää vaikuttavan sääntelyn selvittämisen, käytettävien tietojen ja tietoaineistojen määrittelyn, riippuvuus- ja riskienkartoituksen. Näiden perusteella määritellään vaatimustaso ja tarvittavat mittarit (määrälliset ja/tai laadulliset) halutulle tietoturvan ja tietosuojan tasolle toteutusta ja seurantaa varten.
Teknisen seurannan tarve ja taso on myös määriteltävä.

Toteuttaminen (Do) sisältää haluttuun vaatimustasoon tarvittavien hallinnollisten ja teknisten toimenpiteiden valinnan ja käyttöönoton sekä sovittujen mittareiden käyttöönoton seurantaa varten.

Seuranta (Check) sisältää sovittujen toimenpiteiden seurannan mittareiden ja auditointien (hallinnollisten ja teknisten) avulla. Lisäksi tähän kuuluu toimintaympäristön ja lainsäädännön ja muiden vaatimusten muutosten seuranta.

Ylläpito (Act) sisältää seurannan perusteella havaittujen muutostarpeiden ja kehityskohteiden toteaminen ja tarvittavien uusien toimenpiteiden suunnittelun käynnistäminen. Vaikuttavuuden arviointi on tärkeää kustannusten hallitsemiseksi.

Määritelmät

“Tietoturvallisuus”
Rovaniemen kaupungissa tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kaupungin omistamaa tai hallinnoimaa tietoa. Tietoturvallisuus huomioidaan jo suunnitteluvaiheessa ennen käyttöönottoa. Tietoturvalla tarkoitetaan kaikissa muodoissa olevan tiedon (sekä tietojärjestelmien, tietoliikenteen, palveluiden ja niiden käyttöympäristöjen) turvaamista siten, että tieto on muuttumatonta ja eheää sekä vain siihen oikeutettujen saatavilla.

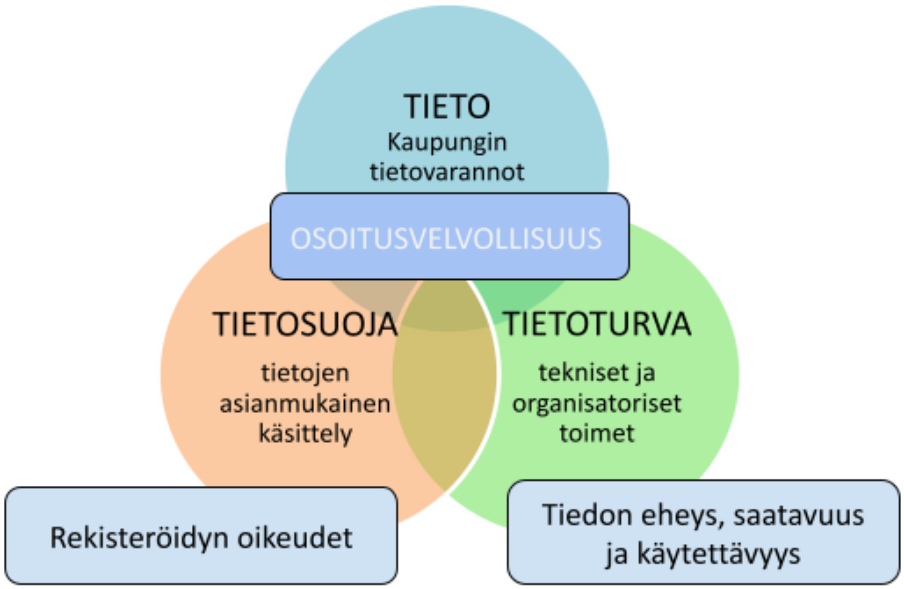
“Tietosuoja”
Tietosuojalla tarkoitetaan yksilön (rekisteröidyn) yksityisyyden suojaamista. Tietosuojalla turvataan rekisteröidyn oikeuksia, yksilön tietoja ja luottamusta. Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa sitä, että henkilötietojen suoja on otettu huomioon jo toiminnan suunnitteluvaiheessa.
Rovaniemen kaupungissa tämä tarkoittaa asiakkaiden, henkilöstön ja sidosryhmien henkilötietojen suojaamista. Tietosuoja on osa toiminnan vaatimustenmukaisuutta, tietoturvallisuutta ja riskienhallintaa.

“Kyberturvallisuus”
Kyberturvallisuudella tarkoitetaan yhteiskunnan elintärkeiden toimintojen ja kriittisen infrastruktuurin laajempaa suojaamista toimenpiteillä, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää uhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa. Kyberturvallisuudessa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja

kriisivarautumisen hallinnan näkökulmat. Kyberturvallisuus ei koske vain julkishallintoa, vaan valtaosa yhteiskuntamme kriittisistä palveluista tuotetaan yritysten toimesta.

"Tietovaranto"
Tietovarannolla tarkoitetaan viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettävä, toiminnan ja hallinnon tarpeista johdettu ja määritelty looginen tietoaineistojen kokonaisuus. Tietovaranto voi koostua tai olla osa yhden tai useamman järjestelmän tuottamista tiedoista, muista digitaalisessa muodossa olevista tiedoista ja analogisessa muodossa olevista tiedoista. Rovaniemen kaupungin tietovarannot jakautuvat kaupungin tehtävien mukaan, ja niitä ovat esimerkiksi maankäytön, talouden ja varhaiskasvatuksen tietovarannot.

"Tietoturvapoikkeama"
Tietoturvapoikkeamasta on kysymys silloin, kun henkilötietoa tai muuta luottamuksellista tietoa tuhoutuu, häviää tai muuttuu, taikka niitä luovutetaan luvattomasti tai niihin pääse käsiksi sellainen taho, jolla ei ole oikeutta käsitellä niitä tai joka estää tai häiritsee tiedon käyttämistä. Tietoturvapoikkeama voi kohdentua esim. järjestelmään tai henkilötietoihin tai molempiin samanaikaisesti.



Kuvio 2. Tietoturva ja tietosuoja osana kaupunkikonsernin tietovarantoja

Tietoturvallisuustyön periaatteet ja tavoitteet

Tietoturvalla tarkoitetaan kaikissa olomuodoissa olevan tiedon (sekä tietojärjestelmien, tietoliikenteen, palveluiden että niiden käyttöympäristöjen) turvaamista siten, että tiedon alkuperäisyys, luottamuksellisuus, eheys, saatavuus ja käytettävyys kyetään varmistamaan.

Tietoturvaperiaatteet pitävät sisällään hallinnollisen, fyysisen, tietoaineisto-, laitteisto-, ohjelmisto- ja tietoliikenneturvallisuuden lisäksi henkilöstö- ja käyttöturvallisuuden periaatteet.

Tietoturvallisuus integroidaan kiinteästi osaksi kaupungin palveluja ja toimintoja. Tietoturvaperiaatteet viedään käytäntöön ohjeistuksin, koulutuksin ja tiedottein, tavoitteena ennaltaehkäistä tietoturvallisuuteen liittyviä poikkeamia ja häiriötilanteita.

Tietoturvallisuuden tarkoituksena on turvata kaupungin toimintaan liittyvien tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tarkoituksellinen tiedon tuhoutuminen tai vääristyminen. Tietoturvan hallintamekanismeilla ja riskienhallinnalla varmistetaan toimintaympäristön ja -tapojen riittävä turvallisuus ja häiriötön toiminta.

Tietojärjestelmien ja –palveluiden hankinnoissa tietoturvallisuuteen liittyvät näkökulmat ja vaatimukset huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä.

Tietosuojatyön periaatteet ja tavoitteet

Tietosuoja-asetuksessa määritellään henkilötietojen käsittelyn periaatteet. Henkilötietoja tulee käsitellä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Henkilötietojen käsittelijän velvollisuus on informoida rekisteröityä tietojen keräämisestä; mitä ja miten kerätään sekä miten tietoja käytetään. Tietoja tulee kerätä vain nimenomaista, laillista käyttötarkoitusta varten eikä myöhemminkään saa tietoja käsitellä käyttötarkoituksen kanssa yhteen sopimattomalla tavalla.

Henkilötietojen käsittely tapahtuu vain sen ajan kun on tarpeen, joten säilytykselle on asetettava määräajat huomioiden pysyvästi säilytettävien ja arkistoitavien asiakirjojen ja tietojen vaatimukset. Kerättyjen tietojen tulee olla täsmällisiä ja virheettömiä. Tiedot päivitetään ja virheelliset tiedot on oikaistava tai poistettava viipymättä.

Tietosuojan periaatteiden noudattamisen tavoitteena on turvata henkilötietojen asianmukainen käsittely koko Rovaniemen kaupungin toiminnassa ja ennaltaehkäistä henkilötietojen käsittelyyn liittyviä poikkeamia.

Tietosuojalla turvataan kaupungin ja sen sidosryhmiin kuuluvien asiakkaiden eli yksilöiden oikeudet heitä koskevassa henkilötietojen käsittelyssä. Tietosuojan toteutumisessa on huomioitava vaitiolovelvollisuus ja henkilötietojen salassapitoa edellyttävät toimet.

Rekisterinpitäjä voi ulkoistaa valitsemansa osan henkilötietojen käsittelystä palveluntuottajalle, eli henkilötietojen käsittelijälle. Rovaniemen kaupunki valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla, täyttävät tietosuoja-asetuksen vaatimukset sekä pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

Hankinnoissa tietosuojaan ja henkilötietojen käsittelyyn liittyvät näkökulmat ja vaatimukset huomioidaan jo suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä. Jos henkilötietoja halutaan siirtää Euroopan talousalueen ulkopuolelle, on siirrossa noudatettava tietosuoja-asetuksessa määriteltyjä tiedonsiirron periaatteita

Organisointi, roolit ja vastuut

Kaupunginhallitus on tiedonhallintalain tarkoittama tiedonhallintayksikön johto kaupungissa. Kaupunginhallitus seuraa tietoturvallisuuden sekä tietosuojan toteutumista kaupungissa. Kaupunginhallitus hyväksyy tietoturva- ja tietosuojapolitiikan. Kaupunginhallitus vastaa rekisterinpitäjänä kaupunginhallituksen alaisten toimintojen henkilötietojen käsittelystä. Kaupunginhallitus vastaa siitä, että tiedonhallintalain 4.2 §:n vastuut, käytännöt ja valvonta on määritelty.

Lautakunta vastaa rekisterinpitäjänä toimialansa palvelujen henkilötietojen käsittelystä. Poikkeuksena jätehuoltojaosto, joka toimii rekisterinpitäjänä vastuualueensa henkilötietojen käsittelyssä.

Kaupunginjohtaja vastaa tietoturvallisuuden sekä tietosuojan toteuttamisesta kaupungin organisaatiossa ja kaupunginhallituksen esittelijänä näiden toteutumisen raportoinnista sekä edellä kaupunginhallituksen vastuulle määriteltyjen tehtävien valmistelun johtamisesta. Kaupunginjohtaja nimeää tietoturva- ja tietosuojatyöryhmän.

Henkilöstö- ja hallintojohtaja hyväksyy koko kaupunkia koskevat tietoturva- ja tietosuojaohjeet.

Toimialajohtaja vastaa toimialansa tietoturvallisuuden ja tietosuojan toteutumisesta. Toimialajohtajan tehtäviin kuuluu lisäksi varmistaa tietoturvaan ja tietosuojaan liittyvän lainsäädännön, linjausten, periaatteiden ja ohjeistusten noudattaminen toimialallaan.

Tytäryhtiöiden ja -säätiöiden hallitukset ja toimitusjohtajat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta omissa organisaatioissaan.

Rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta koko käsittelyn elinkaaren ajan. Rekisterinpitäjä hyväksyy kaupunginhallituksen päättämien tietoturvan ja tietosuojan keskeisten periaatteiden pohjalta omaa sektoriaan koskevat tietosuojan ja tietoturvan keskeiset periaatteet sekä täydentävät erityismääräykset (Rekisterinpitäjän vastuut liitteessä 1).

Rekisterin vastuuhenkilö vastaa omalta osaltaan kyseisen rekisterin tietosuojasta, riskienhallinnasta ja tietosuojaselosteen lainmukaisuudesta. Palvelualuepäällikkö toimii vastuullaan olevan palvelualueen henkilötietojen käsittelyn vastuuhenkilönä. Vastuualuepäällikkö toimii vastuualueensa henkilötietojen käsittelyn vastuuhenkilönä. Mikäli palvelualuepäällikköä tai vastuualuepäällikköä ei ole nimetty, tällöin rekisterinpitäjä nimeää rekisterin vastuuhenkilön.

Rekisterin vastuuhenkilö
- ✓ nimeää rekisterin yhteyshenkilön
- ✓ määrittelee ja hyväksyy toiminnassaan tarpeelliset eri tehtävissä muodostuvat henkilörekisterit
- ✓ huolehtii, että henkilötietojen käsittelyn vaiheet sekä seloste käsittelytoimista on kuvattu Rovaniemen kaupungin tiedonhallintamallissa ja että rekisteröidyn informointi on ajantasainen
- ✓ hyväksyy omaa sektoriaan koskevat tietosuojaan liittyvät ohjeet henkilötietojen käsittelyyn

(Rekisterin vastuuhenkilön vastuut liitteessä 1).

Rekisterin yhteyshenkilö avustaa rekisterin vastuuhenkilöä rekisteröityjen informoinnista kyseisen rekisterin osalta. Rekisteröity voi kääntyä rekisterin yhteyshenkilön puoleen saadakseen tarkempia tietoja rekisteristä tai omista oikeuksistaan.

Esihenkilö vastaa tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan. Esihenkilön keskeisimmät tehtävät on huolehtia

- ✓ oman yksikkönsä henkilöstön perehdyttämisestä kaupungin tietoturva- ja tietosuojaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin
- ✓ oman yksikkönsä henkilöstön tietoturva- ja tietosuojakoulutusten suoritusten seurannasta
- ✓ oman yksikkönsä lainsäädännön mukaisesta tiedon käsittelystä
- ✓ työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
    - työnantajalle kuuluvan tiedon ja muun omaisuuden palauttamisesta
    - työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta

Luottamushenkilö vastaa

- ✓ omasta perehtymisestään kaupungin tietoturva- ja tietosuojaohjeisiin
- ✓ tietosuoja- ja tietoturvakoulutuksen suorittamisesta
- ✓ luottamustehtäväänsä hoitaessaan lainsäädännön mukaisesta tiedon käsittelystä
- ✓ luottamustehtävän päättyessä kaupungille kuuluvan tiedon ja muun omaisuuden palauttamisesta

Henkilöstö ja luottamushenkilöt vastaavat omalta osaltaan tietoturva- ja tietosuojaohjeiden noudattamisesta. Jokaisen vastuulla on lisäksi tietoturvallisuuteen ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi kaupungin intranetistä löytyvän tietoturvapoikkeamien ohjeistuksen mukaisesti. Jokaisella on vastuu työtehtäväänsä liittyvän tietosuojan toteuttamisesta sekä tiedon ja tietojärjestelmien asianmukaisesta käytöstä.

Tiedon laatija vastaa tiedon elinkaaren hallinnasta, luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

Tietojärjestelmästä vastaava viranhaltija tai hänen määräämä vastuuhenkilö vastaavat tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy käyttöoikeuden hakijan esihenkilö.

Tietohallintojohtaja johtaa tietohallintoyksikön ja tietoturva- ja tietosuojatyöryhmän toimintaa. Hän vastaa tietoturvallisuuden arjen toimivuudesta sekä tietoturva- ja tietosuojapolitiikan ja kaupunkitasoisen tietoturvadokumentaation valmistelusta ja kehittämisestä. Lisäksi hän johtaa ja valvoo kaupungin ICT-teknologista arkkitehtuuria mukaan lukien pilvipalvelut. Tietohallintojohtaja raportoi tieto- ja kyberturvallisuuden toteutumisesta kaupunginjohtajalle ja kaupunginhallitukselle.

Sisäinen tarkastaja vastaa toiminnan tuloksellisuuden tarkastamisesta ja arvioinnista. Tähän kuuluu myös tietoturvallisuuden asianmukaisuuden ja riittävyyden arviointi ja tarkastaminen.

Tietosuojavastaava toimii kaupunkiorganisaation tukena ja antaa neuvoa sekä ohjausta tietosuojan toteuttamisesta. Tietosuojavastaava seuraa ja valvoo kaupungin tietojenkäsittelyyn liittyviä toimintatapoja ja tuo esille havaitsemiaan puutteita. Tietosuojavastaava toimii kaupungin yhteyshenkilönä sekä valvontaviranomaisiin että rekisteröityihin. Tietosuojavastaava raportoi tietosuojan toteutumisesta kaupungin johdolle. Kaupunkikonsernin tytäryhtiöt ja säätiöt vastaavat tietosuojavastaavan nimittämisestä EU:n tietosuoja-asetuksen edellyttämällä tavalla.

Tietoturva- ja tietosuojatyöryhmä seuraa tietoturvallisuuden yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden toteutumista kaupungissa. Ryhmä analysoi ja arvioi edellä mainittua kokonaisuutta ja valmistelee siihen perustuen kehitysehdotuksia ja linjauksia tietoturvallisuuden parantamiseksi. Työryhmä seuraa osaltaan tietosuojan toteutumista kaupungissa. Ryhmä valmistelee tietosuojaan liittyviä ohjeita ja toimintatapoja, tuottaa raportteja sekä analysoi toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietosuojariskejä.

Työryhmä valmistelee vuosittaisen toimintasuunnitelman, jossa yhtenä tehtävänä on valita keskeinen tietoturvan ja/tai tietosuojan kehittämiskohde. Kohteen, joka voi olla hallinnollinen (esimerkiksi henkilöstön osaaminen) tai tekninen (esimerkiksi pääsynhallintaratkaisut), keskeiset tavoitteet ja linjaukset tarkistetaan ja päivitetään. Tietosuoja- ja tietoturvatyöryhmän jäsenet nimetään asemansa ja asiantuntemuksensa perusteella.

Tietosuojan ja tietoturvan yhdyshenkilöt nimetään palvelualue- tai yksikkökohtaisesti, joka osaltaan tukee toimialakohtaista tietoturva- ja tietosuojakäytäntöjen jalkautumista ja ajantasaisen tietosuojatietoisuuden ylläpitämistä henkilöstölle. Yhdyshenkilöiden koordinoijana toimii tietosuojavastaava ja tietohallintoasiantuntija. Tietosuojan ja tietoturvan yhdyshenkilö jakaa tietoa ja seuraa tietosuojan ja tietoturvan toteutumista sekä kehittää ja lisää tietosuoja- ja tietoturvatietoisuutta edustamallaan alueella.

Tiedon ja tietojärjestelmien käyttö

Kaupungin tietojärjestelmäympäristössä käytetään tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Tietoturvallinen toimintatapa on kuvattu kaupungin henkilöstölle tarkoitetussa tietoturva- ja tietosuojaoppaassa, jota päivitetään säännöllisesti.

Käyttöoikeudet kaupungin omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa, jotka esihenkilö määrittelee ja hyväksyy.

Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi Työoikeudelliset seuraamukset tietoturva/tietosuojarikkomuksista ja -rikoksista (Yhteistyötoimikunta 15.12.2020 61§) päätöstä.

Tietoturva- ja tietosuojapoikkeamien ja väärinkäytösten selvittämiseksi sekä nykytilan ja käytön valvomiseksi kaupungin tietohallintojohtajalle ja tietosuojavastaavalle mahdollistetaan pääsy tehtävän edellyttämään tietoon ja tietojärjestelmiin.

Tietoturva- ja tietosuojaosaaminen

Esihenkilö huolehtii uudessa tehtävässä aloittavan työntekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin sekä työntekijän omissa työtehtävissä tarvittavaan erityisosaamiseen.

Tietoturvallisuuden ja tietosuojan perus- ja jatkokoulutusta on tarjolla säännöllisesti. Tietoturva- ja tietosuojatietoisuutta ylläpidetään

- ✓ työntekijän perehdytykseen sisältyvällä koulutuksella
- ✓ työ- ja luottamustehtävien mukaisilla koulutuksilla ja säännöllisillä kertauskoulutuksilla

Kaupungin tietoturva- ja tietosuojaohjeistus kokonaisuudessaan on henkilöstön saatavilla kaupungin sisäisissä informaatiokanavissa työtehtävien edellyttämässä laajuudessa.

Riskienhallinta ja varautuminen

Tietoriskien hallinta

Riskienhallintaa toteutetaan Rovaniemen kaupungin riskienhallintapolitiikan mukaisesti. Periaatteena on, että riskienhallintatyö on säännöllisesti toteutuvaa sisäisten ja ulkoisten tietoon kohdistuvien ja tiedosta aiheutuvien riskien hallintaa.

Tietoriskien turvaamisen lähtökohtana on riskiperusteinen lähestymistapa. Pienen riskin tietojen käsittelyyn ei kohdisteta ylimitoitettuja toimenpiteitä, ja toisin päin. Riskipohjaisen lähestymisen avulla tietoturvaan ja tietosuojaan liittyvät velvoitteet ja suojaustoimet määritellään Rovaniemen kaupungissa aina kyseisen tiedon käsittelyyn liittyvien ja havaittujen riskien pohjalta.

Tietoturvapoikkeamien hallinta

Henkilöstö ja luottamushenkilöt on ohjeistettu miten heidän tulee toimia jos he havaitsevat poikkeamia tai epäilevät tietoturvaloukkausta.

Kaikki tietoturvapoikkeamailmoitukset dokumentoidaan. Poikkeamatilanteen olemassaoloon reagoidaan ja ryhdytään toimenpiteisiin sen edellyttämällä tavalla. Ohjeiden ja toimintatapojen päivitystarve arvioidaan poikkeamahavaintojen jälkeen tapahtumien riskiarvioinnin perusteella.

Varautuminen

Rovaniemen kaupunki varautuu turvaamaan tiedonhallintaan liittyvien kriittisten toimintojen ja palveluiden jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

Jokaisen työntekijän on edistettävä omien vaikutuskeinojensa mukaisesti tietojärjestelmien toiminnan jatkuvuuden turvaamista. Henkilöstön tulee omalla toiminnallaan vastuullisesti edistää häiriötilanteissa tietojärjestelmistä riippumattomien työskentelytapojen käytettävyyttä.

Häiriötilanteiden toimintakortit/valmiussuunnitelma tai muut ohjeet perehdytetään henkilöstölle toimialan esihenkilöiden toimesta tai tarvittaessa asiantuntijaohjauksella. Palveluiden tuottaminen tietojärjestelmien ongelmatilanteissa turvataan hyvällä etukäteissuunnittelulla, koulutuksella ja harjoittelemalla. Valmiussuunnitelmissa määritellään palveluiden palauttamisjärjestys laajassa vikatilanteessa.

Viestintä

Tietosuojan ja tietoturvallisuuden muut määritellyt vastuut kattavat myös vastuun tietosuojasta ja tietoturvallisuudesta viestimiseen. Tietosuojaan ja tietoturvallisuuteen liittyvien päätösten viestimisestä vastaa kyseisen päätöksen tehnyt vastaava viranhaltija tai toimielimen ollessa kyseessä toimielimen puheenjohtaja.

Tietohallintojohtaja, tietohallinto ja ICT-palveluiden tuottajat ylläpitävät henkilöstön saatavilla käytännön tietoturvaohjeita ja viestivät tarvittavassa laajuudessa henkilöstölle ja muille sidosryhmille akuuteista tietoturvauhkista sekä suojautumiskeinoista.

Seuranta, valvonta ja seuraamukset

Tietoturva- ja tietosuojapolitiikan ja ohjeiden noudattamisen valvonta on tärkeä osa kaupungin sisäistä valvontaa. Tietosuoja- ja tietoturvatyöryhmä seuraa teknisen ja hallinnollisen tietoturvan toteutumista ja sillä on oikeus toimeenpanna tietoturva-arviointeja.

Tietosuoja- ja tietoturvatyöryhmä tekee vuosittain arvioinnin tietoturvan ja tietosuojan toteutumisesta kaupungissa. Kohde ja laajuus valitaan työryhmän tekemän selvityksen perusteella. Vuosittaisen tarkistuksen yhteydessä arvioidaan tietoturva- ja tietosuojapolitiikan ja muun ohjeistuksen ajantasaisuus.

Palvelusopimuksissa määritellään palveluntuottajien raportointivelvollisuudet tietoturvaan ja tietosuojaan liittyvissä poikkeamatilanteissa.

Jokainen Rovaniemen kaupungin tietojärjestelmien käyttäjä on sitoutunut noudattamaan organisaation tietosuoja- ja tietoturvaperiaatteita hyväksymällä salassapito- ja käyttäjäsitoumuksen. Tietosuoja- ja tietoturvaohjeen sekä muiden ohjeiden, politiikkojen ja lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti. Tietoturva- ja suojarikkomusten mahdollisiin seuraamuksiin sovelletaan Työoikeudelliset seuraamukset tietoturva/tietosuoja rikkomuksista ja rikoksista -dokumenttia (käsitelty ja hyväksytty yhteistyötoimikunnassa 15.12.2020 päätös 61§). Tietosuojarikkomukset raportoidaan organisaation johdolle ja tietosuojavastaavalle.

Liitteet

LIITE 1 Henkilötietojen käsittelyn vastuut ja roolit Rovaniemen kaupungissa (taulukko)