Tietoturvapolitiikka

Tietoturvapäällikkö
1.2.2022
versio 1.0

Sisällys

1 Johdanto

Turun kaupungin toiminta perustuu kuntalakiin (410/2015). Tässä dokumentissa määritellään kaupungin johdon hyväksymä tietoturvapolitiikka, jota se sitoutuu toiminnassaan tukemaan tietoturvavaatimusten täyttämiseksi ja tietoturvan jatkuvaan parantamiseen kaupungissa.

Tietoturvapolitiikassa määritellyt periaatteet, linjaukset ja toteuttamistavat koskevat käytännössä jokaista kaupungin työntekijää, viranhaltijaa, luottamushenkilöä ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee kaupungin omistamaa tai hallinnoimaa tietoa sen sijainnista riippumatta.

Määriteltyjen periaatteiden tarkoituksena on varmistaa tietoturvakäytäntöjen asianmukainen järjestäminen ja yhdenmukaistaa niiden toteuttamista, raportointia ja valvontaa koko kaupungin organisaatiossa.

Turun kaupungilla on soveltuvin osin käytössään ISO 27001 -standardiin perustuva tietoturvallisuuden hallintajärjestelmä, joka yhdessä tämän politiikan kanssa toimii perustana kaupungin tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa. Näin luodaan edellytykset sekä hyvän tietoturvatason ylläpitoon että tietoturvallisen toiminnan pitkäjänteiseen kehittämiseen.

2 Tavoitteet

Tietoturvatyön tavoitteena on, että oikea tieto (eheys) on oikeassa paikassa (luottamuksellisuus) oikeaan aikaan (saatavuus) ja todistetusti (kiistämättömyys):

- *Luottamuksellisuus* tarkoittaa, että tieto on vain niiden käytettävissä, jotka ovat siihen oikeutettuja. Oikeudet pohjautuvat julkisuuslakiin (1999/621) ja sitä täydentäviin säädöksiin sekä annettuihin työtehtäviin. Tiedot luokitellaan sisällön perusteella eri tasoille, joiden mukaan tiedoille määritellään erilaiset tarvittavat käsittelytavat kuten luonti, lukeminen, muokkaus, siirto, säilytys ja hävitys. Käytännössä luottamuksellisuutta toteutetaan yleisimmin sovellusten käyttövaltuushallintana, siihen erikseen määritellyn politiikan mukaisesti.
- *Eheydellä* tarkoitetaan tietojen muuttumattomuutta, oikeellisuutta ja ajantasaisuutta. Käytännössä tieto ei saa muuttua ilman asianmukaisin valtuuksin tehtyjä toimenpiteitä, joita valvotaan omilla hallintajärjestelmillään.
- *Saatavuudella* tarkoitetaan, että tiedot ovat käytettävissä määritellyssä vasteajassa, joka pohjautuu toiminnallisiin kriittisyysvaatimuksiin ja jatkuvuussuunnitteluun. Käytännössä saatavuus toteutetaan sovelluskohtaisina jatkuvuus- ja toipumissuunnitelmina ja edelleen palvelutasovaatimuksina ja -sopimuksina.
- *Kiistämättömyydellä* tarkoitetaan todistettavuutta, eli sitä, että tiedonkäsittelytoimet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana, että jälkikäteen. Käytännössä tämä toteutetaan käsittelytoimien lokienhallinnan ja niiden seurantajärjestelmien avulla.

Tiedonhallintalain (906/2019) sekä sovelletun ISO27001 tietoturvan hallintajärjestelmän lisäksi kaupungin yleisenä tavoitteena on huomioida ja toteuttaa kaikessa toiminnassaan tiedonhallintalautakunnan suositukset.

Palvelukokonaisuudet tarkentavat näitä tavoitteita tarvittaessa linjauksissaan oman toimintansa ja hallinnonalaa koskevan erityslainsäädännön perusteella.

Kaikki havaitut tietoturvatapahtumat arvioidaan ja lakisääteisten vaatimusten lisäksi ilmoitetaan tarvittaessa ohjeistetusti myös edelleen vastaaville viranomaistahoille.

3 Organisointi

3.1 Kaupungin johto

Kansliapäällikkö, hallintojohtaja ja tietohallinnon ohjausryhmä toimivat tietoturvadokumentaation, kuten tämän politiikan, hyväksyjänä ja hyväksymispäätösten virallisena hakijana.

3.2 Tietoturvavastaava

Kaupungin tietoturvavastaavana toimii kaupungin konsernihallinnon tietoturvapäällikkö. Hän huolehtii kaupunkitasolla hallintosäännön 41 §:n valtuutukseen ja sääntöön konsernihallinnon järjestämisestä 10 § perustuen.

- tietoturvallisesta toimintatavasta
- tietoturvatietouden edistämisestä
- tietoturvallisuuden kehittämisestä
- tietoturvan hallintajärjestelmän toimivuudesta
- tietoturvaan liittyvän dokumentaation ajantasaisuudesta
- tietoturvallisuuden raportoinnista johdolle
- tietoturvaan liittyvästä viestinnästä yhdessä viestintäyksikön kanssa

3.3 Tietosuojavastaava

Kaupungin tietosuojavastaava huolehtii tietosuoja-asetuksen 39 artiklan mukaista tehtävistä. Tähän liittyvistä periaatteista, toimintatavoista, vastuista, valvonnasta ja seuraamusjärjestelmästä määritellään lisäksi kaupungin erillisissä tietosuojapolitiikassa ja lokienhallintapolitiikassa, joiden sisällöistä ohjeistaa kaupungin tietosuojavastaava.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja laki sähköisestä lääkemääräyksestä (61/2007) edellyttävät, että jokainen sosiaali- ja terveydenhuollon palvelujen antaja nimeää yksikkönsä toimintaa seuraavan ja valvovan tietosuojavastaavan. Tähän perustuen Turun kaupungin Hyvinvoinnin palvelukokonaisuuteen nimetään oma tietosuojavastaavansa.

3.4 Kaupungin tietoturvaryhmä

Tietoturvavastaavan tukena toimii kaupungin tietoturvan ja tietosuojan kehittämisryhmä, joka on samalla koko kaupungin tietoturvaryhmä. Se vastaa kaupunkitasoisten tietoturvalinjausten ja -ohjeiden jalkauttamisesta palvelukokonaisuuksiin sekä käsittelee palvelukokonaisuuksien tietoturva- ja tietosuojatilannetta ja niihin liittyviä esille nostettuja kehitystarpeita.
Tietoturva-vastaava puuttuu havaitsemiinsa epäkohtiin välittömästi ja tuo ne tietoturva-ryhmän edelleen käsiteltäväksi tapauksesta riippuen. Kaupungin tietoturva-ryhmä kokoontuu tarvittaessa tietoturvavastaavan johdolla.

3.5 Palvelukokonaisuuksien tietoturva- ja tietosuojaryhmä

Palvelukokonaisuuksien toimintaan liittyvästä tietoturvallisuudesta ja tietosuojasta vastaa niiden johtaja apunaan hänen nimeämänsä oma tietoturva- ja tietosuojaryhmä sekä siitä nimetty tietoturva- ja tietosuojayhteyshenkilö jäseneksi kaupungin tietoturvaryhmään. Palvelukokonaisuudet käsittelevät dokumentoiden ryhmissään säännöllisesti toimintojensa, sovellustensa, rekisteriselosteidensa ja tilojensa tietoturvallisuuteen liittyviä asioita sekä henkilökunnan tietoturvaosaamista. Havainnot ja poikkeamat sekä ryhmien jäsentiedot tuodaan aina tiedoksi kaupungin tietoturvavastaavalle viipymättä sekä kokoontumisissa käsiteltäviksi.

Palvelukokonaisuudet päättävät osaltaan myös henkilöstönsä turvallisuusselvitysten teosta tarvittaessa yhteistyössä sovellusten omistajien kanssa perustuen turvallisuusselvityslakiin ja kaupungin riskienhallinnan ohjeisiin.

3.6 Sovellus

Ratkaisu, joka on tarkoitettu jonkin tietyn, yhtenäisen, pysyväisluonteisen tietojenkäsittelyn kokonaisuuden suorittamiseen.

Muodostaa kokonaisuuden yhdestä tai useammasta sovelluksesta, käsiteltävistä tiedoista, niiden käsittelysäännöistä, henkilö- ja laiteresursseista, käyttäjähallinnasta, tiedonsiirtolaitteista, integraatioista ja toimintaohjeista.

Sovellus voi sisältää yhden tai useita rekistereitä, tai tietoja useista rekistereistä (7215-2021).

3.7 Sovelluksen omistaja

Tämän tietoturvapolitiikan ja muiden siihen pohjautuvien politiikkojen, linjausten ja ohjeistusten jalkauttamiseksi toiminnan kannalta usean käyttäjän käyttämiin sovelluksiin, niille nimetään tietoturva- ja tietosuojakontaktiksi sovelluksen omistaja, joka on kaupungin työntekijä ja vastaa sovelluksen tietoturvasta ja -suojasta päätöksen (7215-2021) mukaisesti.

Palvelukokonaisuuden johto nimeää toimivaltansa mukaisesti sovellusten omistajat. Kun kaupungissa otetaan käyttöön tai hankitaan uusi sovellus, omistaja nimetään sovelluksen käyttöönottoprosessissa tai hankintaprosessissa ennen sovelluksen käyttöönottoa.

Uusien sovellusten omistajat ja muutokset omistajatietoihin viedään tiedoksi tietohallinnon ohjausryhmään. Uusien sovellusten listaa ja sen omistajatietoja ylläpidetään IT-palveluissa.

3.8 Sovelluksen pääkäyttäjä

Sovelluksille nimetään palvelukokonaisuuksien toimesta myös yksi tai useampi pääkäyttäjä, jotka toteuttavat omistajan vastuulla olevia tehtäviä yhteistyössä IT-palvelupäälliköiden, palveluntuottajan ja muiden liittyvien eri yksiköiden kanssa. Pääkäyttäjä toimii omistajan ohjauksessa päätöksen (7215-2021) mukaisesti.

3.9 Esihenkilö

Esihenkilö vastaa uusien työntekijöiden ja sijaisten perehdytyksestä ja koulutuksesta noudatettaviin tietoturva- ja tietosuojaohjeisiin ja valvoo, että niitä noudatetaan. Esihenkilö käsittelee vähäpätöiset ja tahattomat tietoturvarikkomukset ja tiedottaa tarvittaessa tietoturva- ja tietosuojavastaavaa. Kaikki merkittävät, törkeät ja tuottamukselliset tietoturva- ja tietosuojarikkomukset saatetaan heidän kauttaan johdon ja tarvittaessa myös viranomaisten tietoon. Esihenkilö vastaa myös yksikkönsä avainhenkilöriskeistä esimerkiksi osoittamalla tarvittavat varahenkilöt.

3.10 Henkilöstö

Henkilöstö velvoitetaan työsopimuksin noudattamaan kaupungin tietoturva- ja tietosuojaohjeita ja vastaamaan omalta osaltaan siitä, että tietoturvallisuus toteutuu. Henkilöstö raportoi viipymättä havaitsemistaan niin tahallisista kuin tahattomistakin rikkomuksista ja tietoturvallisuuden puutteista henkilöstön tietoturvaoppaassa määritellysti vähintäänkin esihenkilölleen, ellei muusta menettelytavasta ole sovittu. Rikkomusten osalta työtehtävissä menetellään, kuten seuraamuksista kaupungin säännöstössä on kuvattu.

3.11 Ulkopuoliset

Myös kaupungin ulkopuoliset työntekijät velvoitetaan sopimuksin, kuten turvallisuussopimus ja Turun kaupungin ehdot henkilötietojen käsittelijälle, noudattamaan kaupungin tietoturva- ja tietosuojaohjeita, Ulkopuolisen työn tilaajan vastuulla on valvoa niiden noudattamista.

4 Tietoturvariskien hallinta

Tietoturvallisuuden hallinta on pohjimmiltaan riskienhallintaa, jossa käsitellään tietoturvariskejä. Myös fyysinen turvallisuus ja ympäristön turvallisuus ovat keskeisiä tekijöitä tietoturvallisuuden kannalta. Kaupungin IT-palvelut-yksikön tuottamien palveluiden tietoturvariskien hallintaa käsitellään myös tietohallinnon ohjausryhmässä sekä laajennetussa tietohallinnon ohjausryhmässä perustuen sovellusten omistajien vaatimusten pohjalta tunnistettuihin tai tietoturvavastaavan esiin nostamiin riskeihin.

Tietoturvariskeistä raportoidaan johdolle myös osana yleistä riskienhallinnan raportointia. Kokonaisuutena riskienhallinnasta, niiden käsittelyprosessista ja raportoinnista on oma erillinen ohjeensa, josta vastaa riskienhallintapäällikkö.

5 Tietoaineiston käsittely

Työtilat, konesalit, jaetut verkkoresurssit ja sovellukset sisältävät suuret määrät kaupungin tietoaineistoa, jonka käsittelystä niiden elinkaaren eri vaiheissa ohjeistetaan henkilöstön tietoturvaoppaassa. Tietoaineiston säilyttämisessä on huomioitava kaupungin arkistotoimen säännökset.

6 Koulutus

Tietoturvallisuus ja tietosuoja huomioidaan henkilöstön koulutuksessa ja työhönotossa. Uusien työntekijöiden perehdyttämiseen kuuluu kaupungin tietosuoja- ja tietoturvaohjeiden läpikäynti. Vastuu tästä on esihenkilöllä. Työntekijöiden käytössä on sähköinen tietoturvallisuuden oppimisympäristö. Jokainen työntekijä suorittaa oppimisympäristöön sisältyvän testin aluksi perehdytyksen yhteydessä ja myöhemmin kerran vuodessa taitojensa

ylläpitämiseksi ja arvioimiseksi. Palvelukokonaisuuteen erityisesti liittyvää tietoturvakoulutusta annetaan lisäksi muun koulutuksen yhteydessä tai tarvittaessa erikseen. Vastuu tämän koulutuksen organisoimisesta on palvelukokonaisuuden johtajalla.

7 Mittaaminen ja arviointi

Tietoturvallisuutta arvioidaan seuraavin mittarein:

1. tietoturvan hallintajärjestelmän tila ja dokumentaatio
2. tietoturvaloukkausten määrä
3. merkittävimmät tietoturvariskit ja -riskin aiheuttavat tietoturvapoikkeamat
4. tietoturvaosaamisen tila

Kaupungin tietoturvavastaava seuraa mittareiden kehitystä IT-palvelut-yksikön tuottamien raporttien ja tietoturvan sähköisen oppimisympäristön tulosten perusteella sekä tietoturvan hallintajärjestelmän dokumentaation perusteella.

Tietoturvallisuutta ja sen hallintaa arvioidaan säännönmukaisesti. Kaupungin sisäinen tarkastus tekee tähän liittyviä tarkastuksia. Tarvittaessa käytetään ulkopuolista konsultointia. Tulokset raportoidaan kaupungin tietoturvavastaavalle.

8 Raportointi

Kaupungin tietoturvavastaava raportoi kaupungin johdolle (3.1) kerran vuodessa tietoturvan tilasta seuraavat asiat:

1. aiempien johdon katselmusten seurantatoimenpiteet
2. tietoturvallisuuden mittarit
3. tietoturvallisuutta koskevat tulevat muutokset lainsäädännössä
4. tietoturvallisuuden kehittämissuunnitelma (vuosikello)
5. erityiset seurantatoimenpiteet

Raportin perusteella ko. ryhmä päättää tarvittavista toimenpiteistä tietoturvallisuuden hallintajärjestelmän, tietoturva-arvioinnin ja sen hallintakeinojen parantamiseksi sekä mahdollisista muutoksista resurssitarpeissa.

< ========== Dokumentin loppu ========== >