

Tietoturva- ja tietosuojapolitiikka

Luonnos 13.6.2018





Sisällys

1 Johdanto	2
2 Tietoturvallisuus	2
3 Tietoturvaluustavoitteet	3
4 Organisointi ja tietoturvaluustavoitteet	3
5 Tiedon ja tietojärjestelmien käyttö	5
6 Tietoturvaluustavoitteiden varmistaminen	5
7 Tietoturvaluustavoitteiden käsittely ja niistä tiedottaminen	5
8 Tietoturvaluustavoitteiden seuranta, ylläpito ja kehittäminen	6



1 Johdanto

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

Tietoturvapoliitikassa kaupungin johto määrittelee tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet. Poliitikka toimii perustana kaupungin tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja auttaa niiden käytäntöön soveltamisessa. Tietoturvapoliitikka ja sen soveltamisohjeet pidetään käyttäjien saatavilla kaupungin intranetissä.

Tietoturvapoliitikka koskee kaupungin koko organisaatiota – niin työntekijöitä kuin luottamushenkilöitäkin – sekä niitä kaupungin sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa. Poliitikka kattaa kaupungin käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2 Tietoturvallisuus

Kajaanin kaupungissa tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kaupungin omistamaa tai hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa että poikkeusoloissa.

Tietoturvallisuus on kiinteä osa kaupungin johtamista, palveluita ja toimintoja. Se ulottuu jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin sekä luottamushenkilöiden toimintaan kaupungin asioiden käsittelijöinä. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten ihmisten yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä.

Henkilötietoja käsitellään vain perustellun käyttötarkoituksen vuoksi ja vain siinä määrin ja niin kauan, kun se on käyttötarkoituksen kannalta tarpeellista. Käytettävien tietojen oikeellisuus pyritään varmistamaan ja tietoja päivitetään. Henkilötietoja säilytetään ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Tietosuojaa ohjaavina periaatteina ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä tietojen eheys ja luottamuksellisuus.

Tietoturvallisuuteen liittyvillä vastuutuksilla ja käytännöillä pyritään varmistamaan, että kaupungin omistama ja hallinnoima tieto

- on oikeaa ja eheää, eikä muuttunut teknisen tai inhimillisen toiminnan seurauksena
- on vain siihen oikeutettujen saatavilla
- on saatavilla, kun sitä tarvitaan

Tähän liittyen tulee tiedon käsittelyprosessien omistajuus ja käyttöoikeudet määritellä sekä huolehtia tiedon elinkaaren hallinnasta niin, että tietoon sen käsittelyn eri vaiheissa tehdyt muutokset voidaan tarvittaessa jäljittää ja todentaa.



Hyvän tietoturvallisuuden aikaansaaminen ja ylläpito edellyttävät tietoista johtamista ja hyvän hallintotavan noudattamista kaupungin kaikissa toiminnoissa. Tietoturvallisuuden osalta tämä kokonaisuus sisältää suunnitteluun, toteutukseen, seurantaan ja ohjaukseen liittyvät prosessit, asiakirjat, kontrollit ja vastuut.

Kaupungin tietoturvatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- Kuntia velvoittavat lait ja asetukset
- EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR)
- Kaupungin omat voimassa olevat strategiat, hallinto- ja ohjesäännöt, riskienhallinta-, valmius- ja viestintäsuunnitelmat (tietoturvallisuutta koskevilta tai sivuavilta osiltaan) sekä näistä johdetut vaatimukset
- Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositukset
- Valtionhallinnon Tietoturvallisuuden johtoryhmän (VAHTI) ohjeet
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010).

Tietoturvallisuus on osa Kajaanin kaupungin riskienhallintaa, varautumista ja kokonaisturvallisuutta. Riskienhallintaa toteutetaan kaupungin sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti. Ohjeessa kuvattu prosessi (mukaan lukien raportointi, seuranta, vastuut) toimii myös kaupungin tietoturvallisuuden perustana. Periaatteena on, että riskienhallintaprosessia käytetään säännöllisesti toteutettavaan sisäisten ja ulkoisten tietoon kohdistuvien ja tiedosta aiheutuvien riskien hallintaan.

Kajaanin kaupunki varautuu turvaamaan ensisijassa kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia valmius- ja muita suunnitelmia. Varautumiseen liittyvät roolit ja vastuut kuvataan em. suunnitelmissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

3 Tietoturvallisuustavoitteet

Kaupungin tavoitteena on saavuttaa Tietoturvallisuusasetuksen (681/2010) kuvaaman tietoturvallisuuden perustason vaatimukset koko kaupungin laajuisesti ja korotetun tason vaatimukset lainsäädännön edellyttämässä toiminnoissa tai toiminnan muutoin niin vaatiessa.

4 Organisointi ja tietoturvavastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kaupungin sääntöjen mukaisesti.

Kaupunginhallitus seuraa tietoturvallisuuden toteutumista kaupungissa. Kaupunginhallitus hyväksyy tietoturvapoliittikan ja siihen ehdotetut muutokset. Kaupunginhallituksella on vastuu kaupungin sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kaupunginjohtajalla on kokonaisvastuu tietoturvallisuuden toteuttamisesta ja tietoturvallisuuden toteutumisen raportoinnista kaupunginhallitukselle. Kaupunginjohtaja omistaa tietoturvapoliittikan ja esittelee muutokset kaupunginhallitukselle. Kaupunginjohtaja hyväksyy kaupunkitasoiset ohjeet ja



linjaukset. Kaupunginjohtajan tukena tietoturvallisuusasioissa on kaupungin johtoryhmä.

Toimialojen ja liikelaitosten johtajat vastaavat toimialansa / liikelaitoksensa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

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

Esimies vastaa tietoturvallisuuden toteutumisesta omalla vastuualueellaan. Esimiehen keskeisimpinä tehtävinä on huolehtia:

- oman organisaationsa perehdyttämisestä kaupungin tietoturvaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturvavastuisiin.
- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
 - kaupungin tiedon ja muun omaisuuden palauttamisesta
 - ilmoittamisesta kaupungin tietohallinnolle työntekijän käyttöoikeuksien ja -valtuuksien poistamiseksi.

Henkilöstö vastaa tietoturvan ja -suojan toteuttamisesta omalta osaltaan. Jokaisen vastuulla on lisäksi tietoturvaa ja -suojaa koskevien ohjeiden noudattaminen sekä tietoturvallisuuteen liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi tietosuojavastaavalle ja omalle esimiehelleen.

Tiedon tuottaja vastaa tiedon luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

Tietojärjestelmän omistaja vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy henkilön esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.

Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Tietohallintopäällikkö vastaa tietoturvaprosessien ohjauksesta ja integroitumisesta muihin kokonaisturvallisuuden osa-alueisiin sekä tietoturvaa koskevasta viestinnästä johdolta saamiensa resurssien ja toimivaltuuksien puitteissa. Tehtävään sisältyy tietoturvatyön suunnittelu, ohjeistus, seuranta ja kehittäminen, sekä tietoturvariskien ja -poikkeamien hallinnan koordinointi.

Tietosuojavastaava antaa tietoa ja neuvoja tietosuojaan liittyvissä asioissa, seuraa tietosuoja-asetuksen ja kansallisten tietosuoja koskevien lakien noudattamista, tekee yhteistyötä valvontaviranomaisen kanssa ja toimii valvontaviranomaisen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaava koordinoi tietosuojaryhmää.

Tietosuojaryhmä toimii tietosuojavastaavan tukena organisaation sisäisenä verkostona. Tietosuojaryhmän jäsenet toimivat yhteyshenkilöinä, jotka välittävät tietoa tietosuojaan liittyvissä kysymyksissä.

Tietohallinto vastaa teknisestä tietoturvallisuudesta, sitä tukevien tietoturvalinjausten tekemisestä ja asetettujen tietoturva vaatimusten toteuttamisesta.

Asiakirjahallinto vastaa asiakirjatiedon hallinnasta ja siihen liittyvästä ohjeistuksesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta asiakirjahallinnossa



Palveluntuottajat vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmissä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

5 Tiedon ja tietojärjestelmien käyttö

Kaupungin tietojärjestelmäympäristössä käytetään Tietohallinnon hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten.

Käyttöoikeudet kaupungin omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi kaupungin ohjeita. Henkilötietojen käsittelyssä noudatetaan voimassa olevaa lakia ja tietosuojaa ohjaavia periaatteita.

6 Tietoturvaosaamisen varmistaminen

Johdon tehtävänä on varmistaa koulutuksen ja ohjeiden avulla, että henkilöstön tietoturvaosaaminen on riittävää. Myös osaamisen ylläpidosta on huolehdittava niin, että se vastaa kulloinkin vallitsevia tilanteita ja toimintaympäristön vaatimuksia.

Jokainen uudessa tehtävässä aloittava työntekijä perehdytetään tietoturvan ja -suojan perusteisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään. Lisäksi tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti, ja tietoturvaohjeet pidetään kaikkien työntekijöiden saatavilla kaupungin intranetin kautta.

Jokaisen Kajaanin kaupungin työntekijän on suoritettava omatoiminen tietoturva- ja tietosuojakoulutus ja siihen liittyvä testi. Testi tehdään henkilökohtaisesti, ja esimiehet tarkistavat alaistensa osalta sen suorittamisen.

Luottamushenkilöiden tulee osallistua kaupungin järjestämään tietoturvakoulutukseen (osana luottamustoimen hoitamiseen perehtymistä) ja sitoutua noudattamaan luottamustoimessaan kaupungin tietoturva- ja tietosuojaohteja.

7 Tietoturvapoikkeamien käsittely ja niistä tiedottaminen

Tietoturva- ja tietosuojaohteiden noudattamista valvotaan sekä säännöllisin rutiinein tai automaattisesti että pistokokein. Väärinkäytöksiin puututaan. Väärinkäytöksiä tai rikoksia epäiltäessä tietoturvavastaava ja epäillyn esimies ratkaisevat, mikä on oikea ja sopiva tapa käsitellä asiaa.

Sekä odottamattomista että ennalta tiedetyistä palvelukatkoksista ja muista tietojärjestelmien käytön häiriöistä tiedotetaan tietohallinnon tiedotussuunnitelman mukaisesti kaupungin tavanomaisia tiedotuskanavia hyödyntäen.

Tietoturvapoikkeamat käsitellään ja niistä raportoidaan johdolle kaupunginjohtajan ja tietohallintopäällikön erikseen tarkemmin ohjeistamalla tavalla. Muulle organisaatiolle havaituista poikkeamista tiedotetaan niiden luonteen ja laajuuden edellyttämällä tavalla. Tietoturvaloukkauksissa noudatetaan EU:n tietosuojasetuksen määräyksiä henkilötietojen



tietoturvaloukkauksen ilmoittamisesta valvontaviranomaiselle ja rekisteröidylle artiklojen 33 ja 34 mukaisesti.

8 Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Tietoturvallisuustyön tulee olla suunnitelmallista ja käytännön toteutusten tulee vastata toiminnan tarpeisiin, lainsäädännön vaatimuksiin sekä kaupungin riskienhallintatyössä asetettuihin muihin tavoitteisiin, ulkoiset toimintaolosuhteet huomioiden.

Seurannan ja muutoshallinnan keinoin varmistetaan, että tietoturvallisuuteen liittyvät kokemukset, palaute ja muutokset vaatimuksissa tai olosuhteissa tulevat oikea-aikaisesti huomioon otetuiksi.

Kaupungin tietoturvapoliittikka katselmoidaan vuosittain ja päivitetään tarvittaessa.