

JOENSUUN KAUPUNGIN TIETOTURVA- JA TIETOSUOJAPOLITIikka 2021

Käsitelty: Tietosuojaryhmä 25.5.2021

Käsitelty: Johtoryhmä 6.9.2021

Hyväksytty:

Johdanto

Tietoturva- ja tietosuojapolitiikkaan on koottu Joensuun kaupungissa noudatettavat tietoturvan ja tietosuojan tavoitteet, periaatteet, toteuttamisen organisointitavat ja vastuut. Palvelujensa toiminnan varmistamiseksi Joensuun kaupunki on sitoutunut kaikessa toiminnassaan lainsäädäntöön perustuvaan tietoturvan ja tietosuojan ylläpitoon sekä sen jatkuvaan kehittämiseen.

Tietoturva- ja tietosuojan parantaminen on osa kaupungin toiminnan kehittämistä, jatkuvuuden varmistamista ja sisäistä valvontaa.

Tietoturva- ja tietosuojapolitiikkaan pohjautuvat suunnitelmat, ohjeet ja määräykset kattavat kaikki tietojen käsittelytoiminnot koko tiedon elinkaaren ajan niiden keräämisestä arkistointiin tai hävittämiseen saakka riippumatta siitä, missä muodossa tieto on. Ohjeet ja määräykset koskevat kaikkia kaupungin työntekijöitä, luottamushenkilöitä, työryhmiä, toimielimiä sekä Joensuun kaupungin toimeksiantoja tekeviä palveluntuottajia toimeksiannon mukaisia tehtäviä hoitaessaan. Kaupungin tietoturva- ja tietosuojatyötä tehdään kiinteässä yhteistyössä Meidän it ja talous Oy:n kanssa (myöhemmin Meita Oy), joka toimittaa kaupungin ICT- palvelut, tietojärjestelmät ja tietotekniset laitteet. Meita Oy vastaa tietojärjestelmien toipumis-, varautumis- ja valmiussuunnitelmista.

Joensuun kaupungilla on ollut aikaisemmin hyväksytyt ohjeistukset tietoturvapoliitikasta ja -suunnitelmasta sekä henkilöstön tietoturvaoppaasta, jotka kaupunginhallitus on hyväksynyt 23.2.2015. Tämä uusi politiikka korvaa aikaisemmin hyväksytyt politiikat ja ohjeet.

Tietoturvan ja tietosuojan tavoitteet

Joensuun kaupungissa käsitellään erilaisia henkilötietoja, taloustietoja ja hallinnon asiakirjoja. Osa näistä tiedoista on salassa pidettävää, arkaluonteista tai muuten luottamuksellista tietoa.

Joensuun kaupungin tietoturva- ja tietosuojatyön tavoitteena on

- mitoittaa ja järjestää käyttöympäristö ja resurssit siten, että toiminta on tehokasta ja se edistää tietoturvan ja tietosuojan toteutumista kaupungin eri toiminnoissa
- turvata tärkeiden tietojärjestelmien ja tietoverkkojen häiriötön toiminta
- varmistaa, että toiminnassa käytettävän tieto on oikeaa, ajantasaista, luotettavaa ja sitä käsitellään lainmukaisesti, että julkinen tieto on helposti löydettävissä ja käytettävissä
- rekisteröidyn laissa määriteltyjen oikeuksien turvaaminen varmistaa, että tiedot eivät joudu tahattomasti tai tahallisesti asiattomien haltuun tai tuhottavaksi
- varmistaa, että tietoja ja tietojärjestelmiä käyttävät vain henkilöt, joilla on niihin oikeus työtehtäviensä hoitamiseksi
- noudattaa henkilötietojen käsittelyssä periaatteita, joita ovat kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus
- dokumentoinnilla osoittaa, että lainmukaisuusperiaatteita on noudatettu.

Normaalitoiminnan jatkuvuuden turvaamisen lisäksi varaudutaan normaaliajan toiminnan keskeyttäviin erityistilanteisiin sekä poikkeusoloihin, ja niistä toipumiseen hallinnollisten, teknisten ja muiden toimenpiteiden avulla.

Tietoturva- ja tietosuojakäsitteitä

Tietoturva tarkoittaa tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi lainsäädännöllisillä, hallinnollisilla, teknisillä ja muilla toiminnoilla sekä normaali- että poikkeusoloissa.

Tietoturvallisuus kattaa kaikenlaiset tietojenkäsittelytehtävät sisältäen myös erityyppisten dokumenttien arkistoinnin. Tietoturvallisuustoimet koskevat sähköisessä, puhutussa ja kirjallisessa muodossa olevan tiedon käsittelyä, säilyttämistä, luovutusta ja siirtoa.

Tietoturvallisuuteen sisältyy

- hallinnollinen turvallisuus (johtaminen ja hallinnointi)
- henkilöturvallisuus (osaaminen, roolit, riittävyys)
- fyysinen turvallisuus (toimitilojen ja laitteiden fyysinen suojaaminen)
- tietoliikenneturvallisuus (tiedon siirron turvaaminen)
- laitteistoturvallisuus (tietokoneiden, puhelinten ym. suojaaminen)
- ohjelmistoturvallisuus (käyttövarmuus, jatkuvuus, käyttöoikeudet)
- tietoaineiston turvallisuus (sähköisten ja paperisten dokumenttien käsittely ja seuraaminen)

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Tietosuojalla tarkoitetaan henkilöiden yksityisyyden, suojaamista, luottamuksen turvaamista sekä oikeuksien ja oikeusturvan varmistamista henkilötietoja käsiteltäessä. Hyvä tietosuojaja edellyttää hyvää tietoturvasoaa.

Organisointi ja vastuut

Kaupunginhallitus hyväksyy kaupungin tietoturva- ja tietosuojapolitiikan ja vastaa tietoturvan ja tietosuojan toteuttamisen edellytyksien luomisesta asetettujen tavoitteiden saavuttamiseksi.

Joensuun kaupungin johtoryhmä vastaa tietoturva- ja tietosuojapolitiikan toteutuksesta hallinnollisella tasolla, sekä tietoturvan ja tietosuojan integroimisesta kaupungin strategiaan. Johtoryhmä varmistaa toimintaan kuuluvien tietojen turvaamisen ja suojaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Toimialajohtajien tehtäviin kuuluu varmistaa tietoturvaan ja tietosuojaan liittyvien suunnitelmien ja ohjeistuksien käytäntöön vienti sekä varmistaa koulutusten järjestäminen yhteistyössä tietoturva- ja tietosuojaryhmän kanssa. Toimialajohtajien tehtävänä on käynnistää yhdessä esimiesten kanssa toimenpiteet vakavien

tietoturvaongelmien korjaamiseksi sekä käsitellä tietosuojarikkomukset ennalta suunnitellun prosessin mukaisesti.

Tietoturva- ja tietosuojaryhmän tehtäviin kuuluvat tietoturvaan ja tietosuojaan liittyvien suunnitelmien ja ohjeistuksien valmisteluun osallistuminen ja avustaa käytäntöön vientiä sekä koulutusten järjestämistä. Ryhmä valmistelee ja tukee kaupungin tietoturvan sekä tietosuojan käytännön toteutusta, kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa.

Tietoturvavastaava vastaa tietoturvan seurannasta, raportoinnista ja kehittämisestä yhdessä muiden tietoturvaryhmän jäsenien sekä Meita Oy:n kanssa.

Tietosuojavastaava valvoo ja seuraa tietosuojan toteutumista tietosuojan valvontasuunnitelman mukaisesti ja raportoi havaitsemistaan puutteista ja esittää parannusehdotuksia niihin tietoturva- ja tietosuoja- sekä johtoryhmälle. Tietosuojavastaava on mukana uusien tietojärjestelmien hankintaprosessissa.

Esihenkilöiden tehtävänä on käynnistää yhdessä toimialajohdon kanssa toimenpiteet vakavien tietoturvaongelmien korjaamiseksi sekä käsitellä tietosuojarikkomukset ennalta suunnitellun prosessin mukaisesti. Esihenkilöt vastaavat siitä, että työntekijät perehdytetään tietoturva- ja tietosuoja-asioihin sekä ohjeistuksiin ja työntekijät ymmärtävät lakien sekä asetusten merkityksen työtehtävissään. Esihenkilöiden tehtäviin kuuluu havainnoida ja reagoida tietoturva- ja tietosuojaongelmiin.

Lisäksi **jokainen Joensuun kaupungin työntekijä ja luottamushenkilö** on vastuussa tietoturvan ja tietosuojan toteuttamisesta omalta osaltaan. Jokainen työntekijä vastaa siitä, että henkilötietoja käsitellessään noudattaa niitä koskevia lakeja ja annettua ohjeistusta.

Toteutus

Tietoturva- ja tietosuojapolitiikan toteuttamiseksi Joensuun kaupungissa:

- laaditaan tietoturva- ja tietosuojasuunnitelma, jossa kuvataan keskeiset toimintatavat ja -menetelmät tietojen käsittelylle,
- laaditaan ohjeistus vastuuhenkilöille, henkilöstölle ja tiedon käsittelijöille,

- järjestetään koulutusta eri kohderyhmien (koko henkilöstö, johto ja esihenkilöt, henkilötietojen käsittelijät) tarpeiden mukaan,
- varmistetaan, että tietoturva ja tietosuoja ovat osana uuden työntekijän perehdytystä,
- jokainen kaupungin työntekijä suorittaa säännöllisesti tietoturva- ja tietosuojatestit,
- huolehditaan, että tiedot ja järjestelmät on suojattu siten, jotta niitä voivat käyttää vain siihen oikeutetut henkilöt,
- mitoitetaan käyttöympäristö ja resurssit siten, että toiminta on tehokasta ja laadukasta ja se edistää tietoturvan ja tietosuojan toteutumista kaupungin eri toiminnoissa,
- vaaditaan palveluntuottajilta sopimukseen riittävä tietoturva- ja tietosuojataso,
- edellytetään Meita Oy:tä varmistamaan tietojärjestelmätoiminnot siten, että niiden keskeytyksistä ja häiriöistä huolimatta Joensuun kaupungin toiminta ja palvelut voidaan hoitaa vähintään ennalta sovitulla minimitasolla,
- varmistetaan prosessi havaittujen tietoturva- ja tietosuojapoikkeaminen käsittelylle.

Seuranta ja valvonta

Tietoturvan ja tietosuojan toteutumisesta laaditaan vuosittain tietosuojan valvontasuunnitelma, jonka pohjalta tietoturvan ja tietosuojan toteutumista seurataan tietoturva- ja -suojaryhmässä sekä kaupungin johtoryhmässä.

Jokaisen Joensuun kaupungin työntekijän ja luottamushenkilön tulee ilmoittaa havaitsemistaan tietoturva- ja tietosuojapuutteista, tietoturvaan ja tietosuojaan liittyvistä väärinkäytöksistä tai epäilemistään tietoturva- ja tietosuojarikkomuksista esihenkilölle ja tietoturvavastaavalle. Tietoturvapoikkeamat käsitellään ennalta suunnitellun ja ohjeistetun prosessin mukaisesti.

Dokumentit ja keskeinen lainsäädäntö

Tietoturva- ja tietosuojapolitiikassa määriteltujen tavoitteiden saavuttamiseksi ja prosessien kehittämisen turvaamiseksi Joensuun kaupungissa päivitetään ja laaditaan:

- tietoturva- ja tietosujasuunnitelma
- henkilöstön tietosuojaopas
- tietosuojan valvontasuunnitelma
- tietoaaineistojen käsittelyohje

Meita Oy laatii ja huolehtii:

- toipumissuunnitelmat (palvelin- ja verkkolaittekohtaiset)
- varautumissuunnitelmat (järjestelmäkohtaiset)
- ICT-Valmiussuunnitelma

Tietoturva- ja tietosuojatyötä ohjaavaa keskeistä lainsäädäntöä ovat mm:

- Arkistolaki (831/1994)
- Euroopan parlamentin ja neuvoston tietosuoja-asetus (EU) (679/2016)
- Hallintolaki (434/2003)
- Tietosuojalaki (1050/2018)
- Tiedonhallintalaki (906/2019)
- Laki digitaalisten palvelujen tarjoamisesta (306/2019)
- Julkisuuslaki (Laki viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 621/1999)
- Julkisuusasetus (Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999)
- Kuntalaki (410/2015)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki valmiuslain muuttamisesta (198/2000)
- Henkilötietojen käsittelyä koskevia erityissäännöksiä on useissa eri aloja koskevissa laissa