Nurmeksen kaupungin tietoturva- ja tietosuojapolitiikka

Sisällys

Nurmeksen kaupunginhallitus 16.4.2018 § 81

Johdanto

Nurmeksen kaupungin toiminnassa käsitellään paljon eri muodossa olevaa julkista ja salaista tietoa. Vaatimus tietojenkäsittelyn hyvään tietoturvaan ja tietosuojaan perustuu lainsäädäntöön. Tietoturvan ja tietosuojan parantaminen on myös osa kaupungin toiminnan kehittämistä, jatkuvuuden varmistamista ja valvontaa.

Nurmeksen kaupunki on sitoutunut kaikessa toiminnassaan hyvään tietoturvan ja tietosuojan ylläpitoon ja jatkuvaan kehittämiseen. Tietoturva- ja tietosuojapolitiikkaan on koottu Nurmeksen kaupungissa noudatettavat tietoturvan ja tietosuojan tavoitteet, toteuttamisen organisointitavat ja vastuut.

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 Nurmeksen kaupungin toimeksiantoja tekeviä palveluntuottajia toimeksiannon mukaisia tehtäviä hoitaessaan.

Kaupungin tietoturva- ja tietosuojatyötä tehdään kiinteässä yhteistyössä Pohjois-Karjalan tietotekniikka Oy:n kanssa, joka toimittaa kaupungin ICT- palvelut, tietojärjestelmät ja tietotekniset laitteet. PTTK Oy vastaa tietojärjestelmien toipumis-, varautumis- ja valmiussuunnitelmista.

Käsitteet

Tietoturva tarkoittaa tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa. Tavoitteena on varmistaa tiedon luottamuksellisuus, eheys ja käytettävyys.

Tietoturvallisuuden osa-alueita ovat:
- 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 suojaaminen)

Tietosuojalla tarkoitetaan henkilöiden yksityisyyden suojaamista, luottamuksen turvaamista sekä oikeuksien ja oikeusturvan varmistamista Eu:n tietosuoja-asetuksen periaatteiden mukaisesti henkilötietoja käsiteltäessä.

Hyvä tietosuojan toteuttaminen edellyttää hyvää tietoturvan tasoa.

Tavoitteet

Tietoturvan ja tietosuojan on oltava osa koko organisaation jokapäiväistä toimintaa, jonka seurauksena

- kaupungin tietoturva ja tietosuoja täyttää lainsäädännön vaatimukset
- toiminnassa ja päätöksenteossa tarvittava tieto on oikein, ajantasaista ja luotettavaa ja sitä käsitellään lainmukaisesti,
- julkinen tieto on helposti löydettävissä ja käytettävissä,
- luottamuksellinen ja salassa pidettävä tieto on suojattu siten, että niitä voivat käyttää vain ne, jotka työtehtäviensä takia ovat siihen oikeutettuja,
- henkilöstö on motivoitunut noudattamaan annettuja ohjeita ja toimintatapoja,
- toimeksiantojen osapuolilta vaaditaan riittävä tietoturva ja -suoja.

Hyvä tietoturva ja tietosuoja parantavat osaltaan Nurmeksen kaupungin toiminnan tehokkuutta ja tuloksellisuutta.

Toteutus

Tietoturva- ja tietosuojapolitiikan toteuttamiseksi Nurmeksen kaupungissa:

- laaditaan tietoturva- ja tietosuojaperiaatteet, jossa kuvataan keskeiset toimintatavat ja -menetelmät tietojen käsittelylle,
- laaditaan riittävät toimintaohjeet vastuuhenkilöille, henkilöstölle ja tiedon käsittelijöille
- järjestetään koulutusta eri kohderyhmien (koko henkilöstö, johto ja esimiehet, henkilötietojen käsittelijät) tarpeiden mukaan ja otetaan tietoturva ja tietosuoja osaksi uuden työntekijän perehdytystä
- suojataan tiedot ja järjestelmät siten, että 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 sopimuksin riittävä tietoturva- ja tietosuojataso
- edellytetään PTTK Oy:tä varmistamaan tietojärjestelmätoiminnot siten, että niiden keskeytyksistä ja häiriöistä huolimatta Nurmeksen kaupungin toiminta ja palvelut voidaan hoitaa vähintään ennalta sovitulla minimitasolla,
- laaditaan toimintaohjeet havaittujen tietoturva- ja tietosuojapoikkeaminen käsittelylle.

Tietoturva ja tietosuoja ovat osa Nurmeksen kaupungin normaalia toimintaa, jota kehitetään jatkuvasti riskiarvioinnin ja havaittujen epäkohtien pohjalta.

Organisointi ja vastuut

Kaupunginhallitus hyväksyy tietoturva- ja tietosuojapolitiikan ja vastaa tarvittavien edellytysten luomisesta niiden toteuttamiseksi.

Johtoryhmä vastaa tietoturva- ja tietosuojapolitiikan toteutuksesta hallinnollisella tasolla sekä tietoturvan ja tietosuojan integroimisesta kaupungin kokonaistoimintastrategiaan. Johtoryhmä vahvistaa politiikan mukaiset periaatteet ja antaa määräykset ja ohjeet sekä vastaa niiden käytäntöön viennistä. Johtoryhmä varmistaa toimintaan kuuluvien tietojen turvaamisen ja suojaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet

ICT-työryhmä, joka toimii myös tietoturva- ja tietosuojaryhmänä, valmistelee ja ohjaa tietoturvan ja tietosuojan käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa. Sen tehtäviin kuuluu tietoturvaan ja tietosuojaan liittyvien suunnitelmien, määräysten ja ohjeiden valmistelu ja ylläpito sekä niiden noudattamisen valvonta. ICT-työryhmän tehtävänä on käynnistää toimenpiteet vakavien tietoturvaongelmien korjaamiseksi sekä käsitellä tietosuojarikkomukset ennalta suunnitellun prosessin mukaisesti.

Esimiehet vastaavat siitä, että heidän alaisillaan on riittävä osaaminen, mahdollisuus riittävään kouluttautumiseen, ohjeistus ja asianmukaiset työkalut tietoturvan ja tietosuojan mukaiseen tietojenkäsittelyyn. Heidän tehtävänään on valvoa tietoturvan ja tietosuojan toteutumista omalla toimialallaan ja raportoida tietosuojan vaarantumiset sekä poikkeamat periaatteista tai ohjeistuksesta.

Jokaisella työntekijällä ja luottamushenkilöllä on henkilötietoja käsitellessään velvollisuus toimia henkilötietolainsäädännön sekä tietosuojaperiaatteiden, tietoturvaperiaatteiden ja muun ohjeistuksen mukaisesti. Jokaisen vastuulla on raportoida havaitsemansa tietosuojan vaarantuminen tai poikkeamat periaatteista tai ohjeistuksesta organisaatiossa määrättävän toimintamallin mukaisesti.

Tietosuojavastaavan tehtävänä on neuvonta, kehittäminen ja valvonta sekä johdolle raportointi

Riskienhallinta

Riskienhallinta tarkoittaa järjestelmällistä ja ennakoivaa tapaa tunnistaa, analysoida, hallita ja raportoida toimintaan liittyviä uhkia ja mahdollisuuksia.

Kaupunginvaltuusto on hyväksynyt Nurmeksen kaupungin ja Nurmes-konsernin sisäisen valvonnan ja riskienhallinnan perusteet. Näitä perusteita noudatetaan myös tietoturvaan ja tietosuojaan liittyvien riskien arvioinnissa ja tarvittavien tavoitetasojen ja korjaustoimenpiteiden määrittelyssä.

Seuranta ja valvonta

Tietoturvan ja tietosuojan toteutumisesta laaditaan vuosittain tietosuojan valvontasuunnitelma, jonka toteutumista käsitellään ict-työryhmässä ja johtoryhmässä.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturva- ja tietosuojapuutteista, tietoturvaan ja tietosuojaan liittyvistä väärinkäytöksistä tai epäilemistään tietoturva- ja tietosuojarikkomuksista esimiehelle ja tietoturvavastaavalle. Tietoturvapoikkeamat käsitellään ennalta suunnitellun prosessin mukaisesti.

Dokumentit ja keskeinen lainsäädäntö

Tietoturva- ja tietosuojapolitiikassa määriteltyjen tavoitteiden saavuttamiseksi ja prosessien kehittämisen turvaamiseksi kunnassa laaditaan:

- Tietoturva- ja tietosuojaperiaatteet
- Toimintaohjeet
- Henkilöstön tietoturva- tietosuojaopas

- Tietosuojan valvontasuunnitelma
- Tietoaineistojen käsittelyohjeet

Pohjois-Karjala tietotekniikkakeskus Oy laatii

- Toipumissuunnitelmat (palvelin- ja verkkolaitekohtaiset)
- 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)
- Henkilötietolaki (523/1999) 31.12.2018 saakka
- 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)
- Henkilötietietojen käsittelyä koskevia erityissäännöksiä on lukuisissa eri aloja koskevissa laissa.

Tulossa

- Tietosuojalaki (1.1.2019 alkaen)
- Tiedonhallintalaki
- Erityislakien päivitykset asetuksen mukaiseksi