



**Lieksan** kaupunki

**Lieksan kaupungin  
tietoturva- ja tietosuojapolitiikka  
2019**



## **Sisällys**

Johdanto .....	3
Käsitteet.....	3
Tavoitteet .....	5
Toteutus.....	5
Organisointi ja vastuut.....	6
Riskienhallinta .....	7
Seuranta ja valvonta .....	7
Dokumentit ja keskeinen lainsäädäntö.....	8

## Johdanto

Tietoturva- ja tietosuojapolitiikkaan on koottu Lieksan kaupungissa noudatettavat tietoturvan ja tietosuojan tavoitteet, periaatteet, toteuttamisen organisoitavat ja vastuut. Palvelujensa toiminnan varmistamiseksi Lieksan kaupunki on sitoutunut kaikessa toiminnassaan lainsäädäntöön perustuvaan tietoturvan ja tietosuojan ylläpitoon ja sen jatkuvaan kehittämiseen. Tietoturva- ja tietosuojan parantaminen on osa kunnan 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 Lieksan kaupungin toimeksiantoja tekeviä palveluntuottajia toimeksiannon mukaisia tehtäviä hoitaessaan.

Kaupungin tietoturva- ja tietosuojatyötä tehdään kiinteässä yhteistyössä Meidän IT ja Talous Oy kanssa, joka toimittaa kaupungin ICT- palvelut, tietojärjestelmät ja tietotekniset laitteet. Meidän IT ja Talous Oy vastaa tietojärjestelmien toipumis-, varautumis- ja valmiussuunnitelmista.

## Käsitteet

**Tietoturva** tarkoittaa tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä nor-

maali- että poikkeusoloissa. Tavoitteena on varmistaa tiedon luottamuksellisuus, eheys ja käytettävyys.

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

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)

**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 EU:n tietosuojasetuksen 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 sopimuksilla riittävä sitoutuminen tietoturvaan ja -suojaan.

## Toteutus

Tietoturva- ja tietosuojapolitiikan toteuttamiseksi Lieksan 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 esimiehet, henkilötietojen käsittelijät) tarpeiden mukaan,
- otetaan tietoturva ja tietosuoja osaksi uuden työntekijän perehdytystä,
- jokainen kaupungin työntekijä suorittaa tietoturva- ja tietosuojatestit,
- 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 Meidän IT ja Talous Oy:tä varmistamaan tietojärjestelmätoiminnot siten, että niiden keskeytyksistä ja häiriöistä huolimatta Lieksan kaupungin toiminta ja palvelut voidaan hoitaa vähintään ennalta sovitulla minimitasolla,
- laaditaan toimintaohjeet havaittujen tietoturva- ja tietosuojapoikkeaminen käsittelylle.

## Organisointi ja vastuut

**Kaupunginhallitus** hyväksyy tietoturva- ja tietosuojapolitiikan ja tietoturva- ja tietosuojasuunnitelman.

**Johtoryhmä** vastaa tietoturva- ja tietosuojapolitiikan toteutuksesta.

**ICT-työryhmä** valmistelee ja ohjaa tietotekniikkaan liittyen tietoturvan ja tietosuojan käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa. ICT-työryhmän tehtävänä on käynnistää toimenpiteet vakavien tietoturvaongelmien korjaamiseksi

**Tietosuojaryhmä** seuraa tietoturvan ja tietosuojan toteutumista sekä informoi siitä johtoryhmää. Ryhmä käsittelee tietoturva- ja tietosuojapoikkeamat hyväksytyyn prosessiin mukaisesti. Ryhmä kehittää tietoturvaa ja -suojaa sekä vastaa siihen liittyvän dokumentaation ja ohjeistuksen valmistelusta.

**Esimiehet** vastaavat siitä, että heidän alaisillaan on riittävä osaaminen, mahdollisuus riittävään kouluttautumiseen, ohjeistus ja asianmukaiset välineet tietoturvan ja tietosuojan mukaiseen tietojenkäsittelyyn. Heidän tehtävänä on valvoa tietoturvan ja tietosuojan toteutumista omalla toimialallaan ja raportoida niiden vaarantumisesta sekä poikkeamista.

**Työntekijällä ja luottamushenkilöllä** on velvollisuus toimia henkilötietolainsäädännön, julkisuuslain sekä tietosuojaperiaatteiden, tietoturvaperiaatteiden

ja ohjeistuksen mukaisesti. Jokaisen vastuulla on organisaatiossa määrättävän toimintamallin mukaisesti raportoida havaitsemansa tietoturvan ja tietosuojan vaarantuminen tai poikkeamat esimiehelle ja tietosuojavastaavalle.

**Tietoturvavastaava** vastaa tietoturvan seurannasta, raportoinnista ja kehittämisestä yhdessä ICT-työryhmän ja tietosuojaryhmän kanssa.

**Tietosuojavastaavan** tehtävänä on neuvonta, kehittäminen ja valvonta sekä johtoryhmälle raportointi. Tietosuojavastaava vastaa tietosuojaryhmän toiminnasta.

## Riskienhallinta

Tietoturvan ja tietosuojan riskien arvioinnista ja riskienhallinnasta vastaa kaupungin johtoryhmä osana kaupungin sisäistä valvontaa. Riskienhallintaprosessin toteuttamisesta vastaavat palvelualueiden johtajat ja esimiehet. Tietoturva ja tietosuoja ovat osa kunnan normaalia toimintaa, jota kehitetään jatkuvasti riskiarvioinnin ja havaittujen epäkohtien pohjalta.

## Seuranta ja valvonta

Tietosuojaryhmä laatii vuosittain tietoturvan ja tietosuojan toteutumisesta valvontasuunnitelman, jonka johtoryhmä hyväksyy. Tietosuojavastaava yhdessä tietosuojaryhmän kanssa seuraa valvontasuunnitelman toteutumista ja raportoi siitä johtoryhmälle.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturva- ja tietosuojapuutteista, tietoturvaan ja tietosuojaan liittyvistä väärinkäytöksistä tai epäilemistään tietoturva- ja tietosuojarikkomuksista esimiehelle ja tietosuojavastaavalle. Tietoturva- ja tietosuojapoikkeamat käsitellään hyväksytyyn prosessin mukaisesti.

## Dokumentit ja keskeinen lainsäädäntö

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

- Tietoturva- ja tietosuoja-suunnitelma
- Henkilöstön tietosuoja- ja tietoturvaopas
- Tietosuojan ja tietoturvan valvontasuunnitelma
- Tietoaineistojen käsittelyohje
- Tietoturva- ja tietosuojapoikkeamien käsittelyprosessi

Meidän IT ja Talous Oy laatii

- 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)
- Henkilötietolaki (523/1999) 31.12.2018 saakka
- Julkisuuslaki (Laki viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallinta-tavasta 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 lukuisissa eri aloja koskevissa laissa
- Tietosuoja-laki.

Tulossa

- Tiedonhallintalaki