Järvenpään kaupungin tietoturvapolitiikka 2025

Kaupunginhallitus 28.4.2025

Dokumentin tiedot	Kuvaus
Kohderyhmä ja sitovuus	Järvenpään kaupunki
Dokumentin tyyppi	Toimintapolitiikka
Dokumentin sisältö	Tietoturvapolitiikka
Omistaja	Järvenpään kaupunginhallitus
Hyväksyjä	Järvenpään kaupunginhallitus, 28.4.2025
Voimassa alkaen	1.6.2025
Päivityspäivämäärä ja keskeiset muutokset	5.2.2025, tarkennuksia
Versiohistoria	Tietoturvapolitiikka 30.5.2011 Tietoturva- ja tietosuojapolitiikka 07.05.2018 Tietoturvapolitiikka 1.6.2025

1 Tietoturvapolitiikka

1.1 Johdanto

Kuntien toiminnot - kuten koko muun yhteiskunnan toiminta - ovat jatkuvasti entistä riippuvaisempia ICT-teknologiasta ja -palveluista sekä niiden toimintavarmuudesta. Tietojen käsittelyyn ja tietotekniikkaan liittyviä riskejä on ensiarvoisen tärkeää tunnistaa ja hallita aktiivisesti. Riskien negatiivisia vaikutuksia tulee minimoida teknisillä ja hallinnollisilla keinoilla.

Edellä todetun takia on välttämätöntä laatia tietoturvapolitiikka, joka määrittää organisaation tavoitteita tietoturvan osalta. Tämä tietoturvapolitiikka määrittelee Järvenpään kaupungin sitoutumisen organisaation tietojen suojaamiseen ja tietoturvan ylläpitämiseen sekä hallintajärjestelmän jatkuvaan parantamiseen. Politiikan tavoitteena on varmistaa, että kaikki tiedot käsitellään turvallisesti ja luottamuksellisesti.

Tietoturvalla varmistetaan tietojen luottamuksellisuus, eheys, saatavuus ja käytettävyys. Tietoturva liittyy läheisesti tietosuojaperiaatteiden ja -politiikan toteuttamiseen. Tietoturvapolitiikka ja tietosuojapolitiikka muodostavat yhtenäisen ja toisiaan tukevan kokonaisuuden.

Tietoturvan tärkeyttä lisäävät myös asiakkaille suunnattujen sähköisten palvelujen laajentuminen, tietojärjestelmien etä- ja mobiilikäyttö, kuntien yhteistyö palvelujen järjestämisessä, laaja palveluntuottajien verkosto sekä palvelutuotannon ja tietojenkäsittelyn nykyaikaiset menetelmät.

1.2 Soveltamisala

Tämä tietoturvapolitiikka on sisäinen velvoittava politiikka, joka on tarkoitettu Järvenpään kaupungin sisäiseen käyttöön. Järvenpään kaupunginhallitus hyväksyy tietoturvapolitiikan. Tietosuoja- ja tietoturvatyöryhmä hyväksyy tietoturvapolitiikkaan tehtävät vähäiset muutokset, jotka eivät edellytä kaupunginhallituksen hyväksymistä. Tietoturvapolitiikkaa täydennetään tietoturvapolitiikan tasoa alemmilla tietoturvan ja tietosuojan määrityksillä ja ohjeilla.

Tietoturvapolitiikka velvoittaa sekä kaupunki- että kaupunkikonsernitasolla (ml. liikelaitokset ja konserniyhtiöt) kaupungin luottamushenkilöitä (kaupunginvaltuusto, kaupunginhallitus, lautakunnat), viranhaltijoita, työntekijöitä, alihankkijoita, toimittajia ja muita sidosryhmiä, jotka käyttävät organisaation tietojärjestelmiä ja/tai käsittelevät organisaation tietoja.

1.3 Vastuut ja roolit

- **Kaupunginhallitus**: Vastaa hallintosäännön mukaisesti kaupungin tiedonhallinnasta, tietoturvasta, tietosuojasta ja asiakirjahallinnosta.
- **Tietohallinto tietohallintojohtajan johtamana**: Vastaa tietoturvapolitiikan kehittämisestä, ylläpidosta ja valvonnasta yhteistoiminnassa tietoturva- ja tietosuojaryhmän kanssa. Tietohallinto vastaa teknisten tietoturvakontrollien toteuttamisesta ja ylläpidosta.
- **Tietojärjestelmän liiketoimintaomistaja:**
    - Vastaa siitä, että järjestelmä tukee liiketoiminnan tarpeita ja tavoitteita.
    - Vastaa siitä, että järjestelmän tietosuojavaikutukset ja riskit on asianmukaisesti arvioitu.
    - Vastaa järjestelmän sisällön elinkaarisuunnittelusta ja dokumentoinnista.
    - Tekee päätöksiä järjestelmän ja sen sisällön tietoturvallisesta käytöstä, pääsyoikeuksista ja kehityksestä liiketoiminnan näkökulmasta.
    - Yhteistyössä järjestelmän omistajan kanssa varmistaa, että järjestelmä on turvallinen ja tehokas.
- **Tietohallinto tietojärjestelmän omistajana:**
    - Vastaa järjestelmän teknisestä elinkaaresta, mukaan lukien sen hankinta, käyttö ja lopettaminen.
    - Varmistaa, että järjestelmä täyttää tekniset tietoturvavaatimukset ja että siihen liittyvät tekniset riskit hallitaan asianmukaisesti.
    - Huolehtii järjestelmän teknisestä dokumentoinnista ja pääsyoikeuksien teknisestä hallinnasta.
- **Tietojärjestelmän pääkäyttäjä:**
    - Vastaa järjestelmän päivittäisestä käytöstä ja tukee muita käyttäjiä.
    - Vastaa muutostenhallinnasta ja tarpeellisten sidosryhmien informoinnista.
    - Hallinnoi käyttäjätilejä ja pääsyoikeuksia.
    - Toimii yhteyshenkilönä teknisten ongelmien ja käyttäjien tukipyyntöjen käsittelyssä.
- **Tietojärjestelmien käyttäjät ja tietojen käsittelijät**:
    - Ovat vastuussa tietoturvapolitiikan noudattamisesta
    - Toimivat tietoturvakäytäntöjen mukaisesti.

1.4 Tietoturvan tavoitteet

Tietoturvallisuuden ensisijaisena päämääränä on organisaatioiden vastuulla olevien tietojen ja palvelujen jatkuvuuden turvaaminen ja mahdollistaa organisaation tietojen ja ICT-ratkaisujen käytettävissä oleminen (saatavuus) sekä käytettävien tietojen eheys ja luottamuksellisuus.

Toimintalähtöisesti painottuvalla tietoturva- ja tietosuoja-asioiden hoidolla tuetaan oman organisaation toiminnalle asetettuja vaatimuksia ja varmistetaan tietojen ja tietojärjestelmien huolellinen käsittely varmistaen samalla asiakkaiden, työntekijöiden ja muiden osallisten yksityisyyden suoja.

Tiedonhallintalain mukaisesti kuntien on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.

Toiminnan tietoturvallisuuden kannalta tärkeitä turvattavia kohteita ovat mm. henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan.

Tavoitteena on operatiivisten järjestelmien ja tietoverkon toiminnan turvaaminen sekä palvelujen tuottamisen ja jatkuvuuden turvaaminen normaali- ja poikkeusoloissa.

Tietoturvatoimien keskeinen tarkoitus on:

- Suojata organisaation tiedot luvattomalta käytöltä, muutoksilta ja tuhoutumiselta.
- Varmistaa tietojen eheys, luottamuksellisuus ja saatavuus.
- Noudattaa sovellettavia lakeja, säädöksiä ja standardeja.

1.5 Tietoturvaperiaatteet

- Tietoturva ja tietosuoja ovat osa organisaation päivittäistä toimintaa ja riskienhallintaa, jota seurataan ja kehitetään jatkuvasti.
- Käytössä olevat tietojärjestelmät ja niiden väliset riippuvuudet kuvataan ja niiden pohjalta arvioidaan riskit yhdessä tietosuojavaikutusten arvion kanssa.
- Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan tiedon suojaamista uhkilta. Suojaamisen tavoitteena on varmistaa toiminnan jatkuvuus ja minimoida toiminnalliset riskit.
- Tietoturva- ja tietosuoja-asiat pitää huomioida tietovälineestä riippumatta eli ne liittyvät muuhunkin kuin vain tietotekniikkaan ja koskevat kaikkia henkilöitä.

- On varmistettava, että luottamukselliset, arkaluonteiset ja muut salassa pidettävät tiedot käsitellään asianmukaisesti riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
- Tietoturvallisuuden saavuttamiseksi toteutetaan riittäviä turvakontrolleja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto- ja laitteistotoiminnoista.
- Jokaisen esihenkilön on huolehdittava, että tietoturva- ja tietosuojamääräykset ja ohjeet koulutetaan ja perehdytetään henkilöstölle.
- Tietoturvaan liittyvä ohjaus, valvonta, raportointi ja seuranta tulee organisoida.
- Yhteistyökumppanit on sitoutettava sopimuksellisesti tietoturvapolitiikan ja -ohjeiden noudattamiseen.

1.6 Tietoturvakontrollit

1.6.1 Fyysinen tietoturva

Fyysiseen tietoturvaan kuuluvat kaikki ne keinot, joilla pyritään suojaamaan riskiarvion perusteella kriittisiä kaupungin tietoja, tietovarantoja ja tietoverkon kohteita. Näitä keinoja ovat:

- Taloturvallisuus (paloturvallisuus, kosteudelta ja vedeltä suojaaminen, sähköhäiriöihin varautuminen, pelastussuunnitelma), lukitut tilat, kulunvalvonta ja kameravalvonta
- Henkilökortin käyttäminen (henkilön tunnistaminen)
- Kaupungin tärkeiden palveluiden ja prosessien keskeytymättömän toiminnan suojaaminen ja häiriöihin varautuminen mukaan lukien tietojärjestelmät ja -verkot
- Jatkuvuus- ja toipumissuunnitelmat (esim. järjestelmäkohtaiset)
- Sopimuskumppaneilta edellytetään riittäviä toimia (mm. jatkuvuussuunitelmat) Järvenpään kaupungin tietojen suojaamiseen

1.6.2 Tietoaineistojen tietoturva

Riippumatta tiedon olomuodosta tietoturvallisilla toimilla tähdätään tietoaineistojen (mm. paperiset ja sähköiset asiakirjat, kuvat jne.) käytettävyyteen, eheyteen ja luottamuksellisuuden ylläpitämiseen seuraavin keinoin:

- Tietoaineistojen luettelointi ja luokitus
- Tietoaineistojen käsittelyn ohjeistus
- Pääsynhallinta

- Käyttöoikeusprosessit
- Salassapitosopimukset
- Salaustekniikat
- Dokumenttien tunnistetiedot
- Tietosuojaohjeet ja -sopimukset
- Tietovälineiden ja -aineistojen ohjeistettu hallinta, käsittely, säilytys, arkistointi ja tuhoaminen

Nämä toimet kattavat tiedon koko elinkaaren alkaen tiedon syntymisestä tiedon tuhoamiseen. Tietoaineistojen tietoturvatyötä tehdään yhteistyössä tietosuojan ja asiakirjahallinnan kanssa.

1.6.3 Tekniset kontrollit

1.6.3.1 Palomuurit ja etäyhteysratkaisut

- Palomuuriratkaisuilla sallitaan vain erikseen määritelty tietoliikenne organisaation ulkopuolelle ja ulkopuolelta.
- Organisaation määrittämiä etäyhteysratkaisuja käytetään suojaamaan ja salaamaan tietojärjestelmäyhteyksiä etätyötilanteissa ja järjestelmien välisissä yhteyksissä.

1.6.3.2 Haittaohjelmien torjunta

- Ajantasalla olevat haittaohjelmien torjuntaratkaisut ehkäisevät virusten ja haittaohjelmien pääsyä tietojärjestelmiin.

1.6.3.3 Salaus

- Tietoliikenneyhteydet ovat aina lähtökohtaisesti salattuja.
- Sähköpostin salauksessa on käytössä turvapostijärjestelmä.
- Päätelaitteiden massamuistit ovat salattuja.

1.6.3.4 Pääsynvalvontajärjestelmät

- Pääsynvalvontaa suoritetaan monivaiheisella tunnistautumisella ja salasanan muoto- ja pituusvaatimuksilla.
- Käyttäjille myönnetään vain työtehtävien suorittamiseen riittävät käyttö- ja pääsyoikeudet. Pääsääntöisesti käyttöoikeuksien saamiseen vaaditaan esihenkilön hyväksyntä.
- Tarvittaessa erityistä suojausta vaativiin kohteisiin voidaan soveltaa pääsynhallinnan lisäturvaominaisuuksia kuten monimenetelmäistä tunnistautumista ml. fyysinen kirjautumistunniste tai -laite.
- Pääsynvalvontaa ja siihen liittyvää lokitietoa hallitaan automaattisilla kontrolleilla ja niiden herätteisiin sidotuilla toimenpiteillä.

1.6.4 Hallinnolliset kontrollit

1.6.4.1 Tietoturvakoulutus, -käytännöt ja -menettelyt

- Henkilöstön tietoturvatietoisuutta pidetään yllä säännöllisillä tietosuoja- ja tietoturvakoulutuksilla sekä ajantasaisilla toimintaohjeilla tietoturvaan liittyvien toimintamallien osalta.
- Tietoturvakäytännöillä ja -menettelyillä pyritään varmistamaan riittävä tietoturvan taso ja mahdollistamaan sujuva työskentely.

1.6.4.2 Sallitut ohjelmistot ja sovellukset

- Sallitut ohjelmistot ja sallitut tietojen tallennuspaikat ja -tavat kuvataan erillisissä tietohallinnon tuottamissa ohjeissa tiedonhallinnan, tietoturvan, tietosuojan ja asiakirjahallinnan käsittelyohjeet huomioiden.

1.6.4.3 Hankinnat

- Hankinnoissa noudatetaan tietosuoja- ja tietoturvapolitiikan ja niihin liityviä alempien ohjeiden ja periaatteiden mukaisia tietoturvavaatimuksia.
- Tietoteknisten ratkaisujen toimittajilta edellytetään sitoutumista Järvenpään kaupungin tietosuoja- ja tietoturvapolitiikan vaatimuksiin.

1.7 Tietoturvapoikkeamien hallinta

Riskienhallinta ja varautuminen tulee tehdä kaupungin sekä oman toiminnan lähtökohdista ja laatia suunnitelmat siitä, miten toimitaan häiriöiden aikana ja miten toiminta palautetaan normaaliksi häiriöiden jälkeen. Tietohallinto turvaa ja priorisoi organisaation järjestelmät toiminnan prioriteetit ja riskit huomioiden. Tietojärjestelmien ylläpitoon liittyvät tietoturva-asiat tietohallinto määrittelee tarkemmin asiaa käsittelevissä erillisissä ohjeissa.

- **Havainnointi:** Tietoturvapoikkeamien havainnointia pyritään mahdollisimman laajasti automatisoimaan teknisellä valvonnalla, lisäksi jokaisen organisaation tietoja ja järjestelmiä käyttävän tahon on pyrittävä havainnoimaan mahdollisia tietoturvapoikkeamia ja -uhkia.
- **Tietoturvapoikkeamien tunnistaminen ja ilmoittaminen:** Tunnistetut tietoturvapoikkeamat on raportoitava välittömästi annetun ohjeistuksen mukaan. Jokainen organisaation tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä eteenpäin tietohallinnon ohjeistamalla tavalla.

- **Poikkeamien käsittely**: Poikkeamat tutkitaan ja korjaavat toimenpiteet toteutetaan mahdollisimman pian. Henkilötietoihin kohdistuvat tietoturvaloukkaukset tulee käsitellä sovellettavan tietosuojalainsäädännön ja tietosuojapolitiikan mukaisesti.

1.8 Tietoturvapolitiikan seuranta ja auditointi

- **Seuranta**: Tietoturvakontrollien tehokkuutta seurataan säännöllisesti, erikseen sovitun omavalvontasuunnitelman mukaisesti. Omavalvontasuunnitelma laaditaan ja sitä käsitellään tietoturva- ja tietosuojaryhmässä.
- **Auditointi**: Tietoturvan toteutuksen periaatteena on jatkuva valvonta. Sen lisäksi voidaan tarpeen mukaan suorittaa toiminnan kannalta keskeisille tietojärjestelmille erillisiä tietoturva-auditointeja.

1.9 Koulutus ja tietoisuuden lisääminen

- **Koulutusohjelmat**: Säännölliset tietoturvan ja tietosuojan koulutukset kaikille työntekijöille ja luottamushenkilöille.
- **Tietoisuuden lisääminen**: Kampanjat ja tiedotustilaisuudet tietoturvatietoisuuden lisäämiseksi.

1.10 Dokumentaatio

Tietoturvan toteuttamiseen tarvittava dokumentaatio muodostuu tiedonhallintalain vaatimusten mukaisesti tietosuojan ja tietohallinnon yhteisestä ja hallitusti ylläpidetystä tietokokonaisuudesta.