PIEKSÄMÄEN KAUPUNGIN

# Tietoturva- ja tietosuojapolitiikka

KH 21.01.2019 (PMK/381/07.00.00/2018)

PIEKSÄMÄKI

Elämäsi asemapaikka

# Sisältö



VERSIOT

180406 Fjällström Tuomas, Malinen Päivi, Romo Seija

181129 Penttinen Anja, Romo Seija, Ullah Veera

# TIETOTURVA - JA TIETOSUOJAPOLITIIKKA

Tietoturva- ja tietosuojapolitiikka on kaupungin ylimmän johdon strateginen kannanotto tietoturvan ja tietosuojan kehittämiseen. Politiikka määrittelee kaupungin tietoturva- ja tietosuojatyön vision, tavoitteet, toimintatavat, vastuut ja valvonnan. Tietoturva- ja tietosuojapolitiikan toteuttaminen on edellytys pitkäjänteiseen kehittämiseen. Työssä onnistuminen edellyttää kaupungin johdon sitoutumisen tietoturva- ja tietosuojatyön tukemiseen.

Tietoturva- ja tietosuojapolitiikka koskee koko kaupunkikonsernia ja sen henkilöstöä. Samoin se koskee sidosryhmiä, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun ja ohjaamana. Politiikka kattaa kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä politiikka koskee henkilötietojen käsittelyä silloin, kun kaupunki toimii rekisterinpitäjänä.

## Määritelmät

Tieto ja tietojenkäsittely ovat nykymuotoisen yhteiskunnan toiminnan perusta. Tämä edellyttää ICT-palveluiden tietoturvallista ja keskeytyksetöntä toimintaa. Digitalisaatio tuo laajentuessaan tämän vaatimuksen ja yksityisyyden suojan vaatimukset uusille alueille.

Tietoturva- ja tietosuojaosaaminen voi nousta tulevaisuudessa organisaation toiminnan menestystekijäksi. Oikein toteutettuna tietoturva ja tietosuoja mahdollistavat kerätyn tiedon aikaisempaa tehokkaamman hyödyntämisen ja kustannussäästöt.

**Tietoturvalla** tarkoitetaan eri muodossa olevien tietojen - (esim. sähköisesti tallennettu tai välitetty, puhuttu tai paperilla oleva tieto) suojaamista erilaisilta uhkatekijöiltä tavoitteena toiminnan jatkuvuuden varmistaminen ja toimintaan tai tietoihin, erityisesti henkilötietoihin, liittyvien riskien minimoiminen.

**Tietoturvallisuus** määritellään yleensä kolmen peruskäsitteen kautta:

1. Tietojen saatavuus: tieto on saatavissa ja käytettävissä silloin ja siinä muodossa, kuin sitä tarvitaan. Saatavuus turvaa tietojen hyödyntämisen ennalta suunnitellun aikaviiveen puitteissa.
2. Tietojen luottamuksellisuus: tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeus. Luottamuksellisuus turvaa tietojen julkaisun tai luovuttamisen vain ja ainoastaan suunniteltuja väyliä pitkin, suunnitellussa laajuudessa.

3. Tietojen eheys: tiedot on suojattu siten, ettei niitä voi muuttaa tahallisesti tai tahattomasti siten, että niiden luotettavuus vaarantuu, tai ainakin tällaiset muutokset voidaan havaita. Eheys turvaa tietojen hyödynnettävyyden ja arvon säilymisen.

Kolmea yllämainittua tietoturvallisuuden peruskäsitettä täydentävät:

4. Kiistämättömyys: tietoon kohdistuvista toimenpiteistä jää jälki, jota muutoksen tekijä ei voi kiistää.
5. Tunnistus: tietojärjestelmän käyttäjä voidaan tarvittaessa liittää käyttäjätunnukseen.
6. Todennus: tietojärjestelmän käyttäjä voidaan luotettavasti tunnistaa luonnolliseksi henkilöksi tai oikeushenkilöksi.

**Tietosuoja:** Henkilötietojen suoja on jokaiselle kuuluva perusoikeus. Henkilötietojen käsittelyn on oltava asian- ja tarkoituksenmukaista. Henkilötietojen keräämiselle, tallentamiselle ja säilyttämiselle täytyy olla tietosuoja-asetuksen mukainen peruste.

Jokaisella henkilöllä on oikeus tutustua niihin tietoihin, joita hänestä on kaupungin henkilörekisterissä. Henkilöllä on oikeus saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli lainsäädäntö sen sallii.

Hyvä tietoturvan ja tietosuojan taso saavutetaan noudattamalla tietoturva- ja tietosuojapolitiikkaa ja sen pohjalta laadittuja ohjeita sekä ottamalla käyttöön erilaisia turvamekanismeja, joita hallitaan jatkuvan kehittämisen periaatteita noudattaen.

## Pieksämäen kaupungin rooli ja toimintaympäristön vaikutukset tietoturvaan ja tietosuojaan

Pieksämäen kaupunki ohjaa omaa toimintaansa ylläpitämällä visiota sekä strategisia tavoitteita. Strategian päätavoite on sidosryhmien ja kuntalaisten odotuksiin ja tarpeisiin vastaaminen kaupungin käytettävissä olevilla resursseilla. Tämän toiminnan perustana on asukkaiden tarvitsemat palvelut. Tietoturva- ja tietosuojatoiminnan tehtävänä on varmistaa kaupungin palveluiden jatkuvuus, minkä kautta voidaan saavuttaa myös strategisia tavoitteita.

Pieksämäen kaupunkistrategian kolme päätavoitetta ovat: elinvoiman lisääminen, hyvin-

voinnin lisääminen sekä aluekehittämisen mahdollistava kuntatalous.

Pieksämäen kaupunkikonsernin palvelutuotanto on monipuolista ja se kattaa laajan maantieteellisen ja toiminnallisen alueen. Palveluiden toiminta perustuu pitkälti tietoteknisiin järjestelmiin (laitteisiin, verkkoihin ja sovelluksiin sekä niiden välisiin integraatioihin), jotka taas ovat tyypillisesti eri toimittajien hallussa ja siten organisatorisesti ja maantieteellisesti hajautettuja. Toiminta on haavoittuvaista, sillä se on erityisen altis häiriö- ja riskitekijöille.

Jotta voisimme jatkossakin turvata toimivat palvelut, olemme riippuvaisia ICT-ratkaisujen ja tietoverkkojen luotettavasta toiminnasta. Haasteisiin varautuminen vaatii tietoturvan ja tietosuojan jatkuvaa suunnittelua ja kehittämistä.

## Kaupungin tietoturvan, tietosuojan ja ICT-riskienhallinnan kehittäminen

Tiedon turvaaminen on merkittävä osa kaupungin toiminnan ja sen järjestämien palvelujen laatua, ICT-riskienhallintaa ja kokonaisturvallisuutta. Riskienhallinnan keskeisenä tavoitteena on tunnistaa toimintaan kohdistuvat riskit, arvioida ne ja päättää tarvittavista toimenpiteistä.

### Tietoturva- ja tietosuojanäkökulmat:

- Tietoteknisestä näkökulmasta hyvä toimintatapa edellyttää järjestelmäkokonaisuuden ja sen hallinnan pitkäjänteistä suunnittelua, jatkuvaa kehittämistä ja seurantaa.
- Organisatorisesta näkökulmasta tietoturvan ja tietosuojan kehittämisen edellytys on koko henkilöstön tietoturva- ja tietosuojaosaamisen ja -tietoisuuden lisääminen kouluttamalla, ohjeistamalla ja viestimällä sekä yhteisesti sovittujen käytäntöjen noudattamisen valvominen.
- Tietosuojan toteutuminen ja kehittäminen edellyttävät, että henkilötietojen käsittely arvioidaan ja suunnitellaan palvelukehityksessä alusta alkaen.

## TIETOTURVA- JA TIETOSUOJATYÖN TAVOITTEET JA PERIAATTEET

Tietoturva- ja tietosuojatyön tavoitteena on kehittää ja parantaa kaupungin toiminnan luotettavuutta, jatkuvuutta, laatua, ICT-riskienhallintaa ja riskeihin varautumista sekä edistää tietoturva- ja tietosuojatyön saattamista kiinteäksi osaksi kaupungin johtamista. Työn tavoitteena on luoda yhdenmukaiset käytännöt ja toimintatavat.

Kehittämisen painopisteitä ovat kokonaisvaltainen johtaminen, riskien tunnistaminen ja ennaltaehkäisy sekä tietojen suojaaminen. Kehittämisen avulla varmistetaan yhtenäinen toimintaympäristö ja -tapa. Tavoitteena on kaupungin palveluiden käyttäjien, yhteistyökumppaneiden ja työntekijöiden luottamus kaupungin palveluihin ja niiden tietoturvaan ja tietosuojaan.

Tietosuojan toteuttamisessa kaupungin tavoite on varmistaa tietosuojalainsäädännön ja toimialakohtaisen lainsäädännön vaatimusten toteutuminen koko käsiteltävien henkilötietojen elinkaaren ajan. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan.

Rekisterinpitäjät (lautakunnat ja hallitus) arvioivat henkilötietojen käsittelyyn liittyvät riskit ja valitsevat teknisen ympäristön ja toimenpiteet halutun tason mukaan. Tietosuojariskien hallinta on osa kaupungin riskienhallintaprosessia. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Henkilötietojen käsittely toteutetaan noudattamalla tietosuojaperiaatteita.

Vaikutustenarviointi suoritetaan sellaisten henkilötietojen käsittelytoimenpiteille, joiden suunnitteluvaiheessa ilmenee, että toimenpiteisiin liittyy henkilön oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa.

| **Strateginen painopiste** | **Tavoite** | **Arviointi ja mittarit** |
|---|---|---|
| Tietoturvaan ja tietosuojaan kohdistuvien uhkatekijöiden tunnistaminen | Tuloksellinen ja kokonaisvaltainen riskienhallinta<br>ICT-varautumisen kehittäminen<br>Tietosuoja; tarvittaessa vaikutusten arviointi | Vakavien uhkatekijöiden tunnistaminen ja niihin liittyvät toimenpiteet<br>Tehokas tietoturva- ja tietosuojatyö ja raportointi<br>Tietotilinpäätös |
| Palveluiden jatkuvuuden ja tietojen turvaaminen | Luotettava ICT-infrastruktuuri<br>Lakisääteisten velvoitteiden täyttäminen<br>Häiriötilanteiden hallinta ja tekniset ratkaisut<br>Häiriötilanteiden varautumis-, toipumis- ja viestintäsuunnitelmat (toimintamallit) | Tarpeiden mukaisesti mitoitetut palvelutasot ja tietoturvaratkaisut ovat käytössä<br>Palvelutasojen toteutuminen<br>Toimintamallien arviointi<br>Häiriötilanteiden määrä |
| Henkilöstön tietoturva- ja tietosuojaosaamisen kehittäminen | Positiivisen kulttuurin ja asenteiden kehittäminen<br>Selkeät vastuut, toimintamallit ja ohjeistukset<br>Yhtenäisten, tietoturvallisten toimintatapojen noudattaminen<br>Koulutus ja ohjeistus on ehdoton koskien työtehtäviä, joissa käsitellään henkilötietoja tai erityisiä henkilötietoja | Tietoturva- ja tietosuojapolitiikan ja -ohjeiden noudattaminen<br>Tietoturva- ja tietosuojakoulutusten kattavuus<br>Työntekijöiden osaamismittarit |
| Tietoturva ja tietosuoja toiminnan kehittämisen mahdollistajana | Ratkaisut mahdollistavat toiminnan turvallisen kehittämisen<br>Käyttötarkoituksenmukaisuus (paras mahdollinen tekninen ja organisatorinen riskiarvioon perustuva ratkaisu) ja kustannustehokkuus ohjaavat valintoja<br>Toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta; osaksi tarvemäärittelyä<br>Ongelmanratkaisukyky | Tietoturvan ja tietosuojan kypsyys ja toteutuminen osana kokonaisarkkitehtuuria |
| Suositusten mukainen toiminta | Kaupungin tietoturva ja tietosuoja ovat kansallisesti hyvällä tasolla<br>Toiminnan dokumentointi on ajan tasalla<br>Sopimuksissa on ajan mukaiset tietoturva- ja tietosuojasisällöt<br>Kansallisten strategioiden, ohjeistusten ja hyvien käytäntöjen tehokas hyödyntäminen<br>Kansainvälisten strategioiden, ohjeistusten ja hyvien käytäntöjen hyödyntäminen | Toiminnan arviointi vasten kansallisia ja kansainvälisiä ohjeistuksia (soveltuvat viitearkkitehtuurit, tietosuoja-asetus)<br>Sopimusseuranta |

# TIETOTURVA- JA TIETOSUOJATYÖN VASTUUT

Pieksämäen kaupungin tietoturva- ja tietosuojatyön toteuttamisen perustana on kaupunginhallituksen hyväksymä tietoturva- ja tietosuojapolitiikka ja sen pohjalta laaditut ohjeistukset.

## Kaupunginhallitus ja kaupunginjohto

Kuntalain mukaisesti kokonaisvaltainen riskienhallinta ja sitä kautta tietoturvan ja tietosuojan toteuttamisen kokonaisvastuu on kaupunginhallituksella ja kaupunginjohtajalla. Kaupungin johdon on sitouduttava tietoturvan ja tietosuojan jatkuvaan kehittämiseen ja huolehdittava resursoinnin riittävyydestä ja jatkuvuudesta.

## Tietohallinto

Tietohallinnon vastuulle kuuluu strategisten ICT-linjausten muodostaminen ja toteuttaminen, ICT-palveluiden järjestäminen ja niihin liittyvä riskinhallinta sekä tietoturvan ja tietosuojan kehittäminen ja hallinta.

Tietohallinnon tehtävänä on ylläpitää yhdessä tietosuojavastaavan kanssa kaupungin tietoturva- ja tietosuojapolitiikkaa ja ohjeistuksia tietoturvan osalta, suorittaa seurantaa ja arviointeja, välittää tietoa organisaatiotasolla sekä tarvittaessa järjestää koulutuksia ja jalkauttaa yhteisiä toimintatapoja.

## Tietosuojavastaava

Tietosuojavastaavan työtä ohjaa EU:n yleinen tietosuoja-asetus. Hänenydintehtäviinsä kuuluu organisaation tietosuojan kehittäminen riskienhallinnan näkökulmasta ja organisaation tietosuojaosaamisen lisääminen. Tietosuojavastaava on henkilökunnan ja tietosuojavaltuutetun yhteyshenkilö.

Vastuu tietosuoja-asioista on aina rekisterinpitäjällä. Rekisteröidyllä on oikeus saada tarkastella omia henkilörekisteriin tallennettuja tietojaan. Tietopyyntöihin vastaamista valvoo tietosuojavastaava.

Tietosuojavastaavan tehtävänä on ylläpitää tietohallinnon kanssa kaupungin tietoturva- ja tietosuojapolitiikkaa ja ohjeistuksia tietosuojan osalta sekä valvoa tietosuojan toteutumista.

## Tietoturva- ja tietosuojaryhmä

Yhteistyössä tietosuojavastaavan kanssa kaupungissa toimii konsernijohdon perustama tietoturva- ja tietosuojaryhmä. Ryhmän tarkoituksena on tukea tietoturva- ja tietosuoja-työtä sekä politiikan toimeenpanoa. Konsernin tietoturva- ja tietosuojaryhmään nimetään edustaja jokaiselta palvelualueelta, liikelaitoksista, taseyksiköistä sekä tytäryhtiöistä.

## Palvelualueet ja konsernin osat

Palvelualueiden ja konsernin osien johtajat vastaavat tietoturva- ja tietosuojapolitiikan ja ohjeiden noudattamisesta toiminnassaan sekä oman yksikön sisällä että sopimussuhteissa ostopalveluiden toimittajiin.

Johdon vastuulla on nimetä edustaja tietoturva- ja tietosuojaryhmään. Edustajan vastuulla on tuntea toimialansa erityispiirteet ja lainsäädäntö, seurata niiden kehittymistä ja viestiä niistä kaupungin tietohallinnolle ja tietosuojavastaavalle.

## Tietojärjestelmän omistaja

Jokaisella tietojärjestelmällä tulee olla yksilöity omistaja, joka vastaa koko järjestelmän elinkaaren hallinnasta, tietosuojasta ja tietoturvan toteuttamisesta. Järjestelmän omista-juuteen liittyvät tiedot dokumentoidaan tietohallinnon ylläpitämään tietojärjestelmäluet-teloon. Henkilötietoja sisältävistä tietojärjestelmistä on oltava ajantasainen tietosuojase-loste, joka voi olla myös usean tietojärjestelmän yhteinen. Selosteen tekemisestä vastaa järjestelmän omistaja. Tietojärjestelmän omistajan on huolehdittava tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsynvalvonnasta sekä tuotettava lakisääteiset seurantaraportit.

Omistajan tulee etukäteen kartoittaa yhteistyössä tietohallinnon, tietosuojavastaavan sekä palvelu- ja järjestelmätoimittajan kanssa tietojärjestelmään kohdentuvat riskite-kijät, häiriötilanteiden toimintamallit ja varmistettava toiminnan jatkuvuus. Omistajan on laadittava tietoturva- ja tietosuojaohjeet käyttäjille sekä huolehdittava, että työntekijät saavat niihin riittävän koulutuksen.

## Tietojärjestelmän pääkäyttäjän vastuu

Jokaiselle tietojärjestelmälle on nimettävä pääkäyttäjä, jonka vastuulla on huolehtia järjestelmän käyttöoikeuksista. Pääkäyttäjältä vaaditaan hyvää tietoturva- ja tietosuojaosaamista.

## Esimiehen vastuu

Esimiesten vastuulla on lakisääteisten tietoturva- ja tietosuojavelvoitteiden toteutuminen. Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa. He huolehtivat loppukäyttäjän riittävästä perehdytyksestä konsernin tietoturva- ja tietosuojakäytänteisiin varmistaen, että jokainen ymmärtää niiden merkityksen työtehtävissään.

Esimiesten ja pääkäyttäjien vastuulla on myös huomioida työtehtävien muutokset järjestelmien käyttöoikeuksissa. Työsuhteen päättyessä käyttöoikeudet järjestelmistä poistetaan ja työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden. Esimiehiltä odotetaan esimerkillistä sekä vastuullista tietoturva- ja tietosuojakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvapoikkeamista ja kehittämistarpeista tietohallinnolle.

## Työntekijän vastuu

Kaupungin työntekijän velvollisuus on suorittaa hyväksytysti tietoturva- tai tietosuojakoulutus säännöllisin väliajoin. Työntekijällä on vastuu noudattaa hyväksyttyjä tietoturva- ja tietosuojaohjeita. Lisäksi hänellä on velvollisuus raportoida havaitsemistaan tietoturvaongelmista ja kehittämistarpeista esimiehelle.

## ICT-palveluiden hankintoihin liittyvät vastuut

Kaupunki voi ulkoistaa valitsemansa osan ICT-palvelutuotantoa tai henkilötietojen käsittelystä sopimusperusteisesti. Kaupunki valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa.

Kaupunki huolehtii sopimuksin siitä, että palveluntuottaja järjestää palvelun asianmukaisin teknisin ja organisatorisin toimenpitein sekä täyttää tietosuoja-asetuksen vaatimukset ja pystyy huolehtimaan rekisteröidyn oikeuksien toteutumisesta silloin kun palveluun sisältyy henkilötietojen käsittelyä.

ICT-palveluiden tietoturvasta ja siihen liittyvästä ohjeistuksesta vastaavat palveluntuottajat. Rekisterinpitäjän vastuulla on huolehtia siitä, että henkilötietojen käsittely ja käsittelytoimet on kuvattu sopimuksessa. Palveluntuottajien tehtävä on avustaa tietoturva- ja tietosuojaohjeiden laatimisessa ja ylläpidossa. Samoin heidän kuuluu raportoida ja tiedottaa merkittävistä tietoturvaan liittyvistä poikkeustilanteista ja riskeistä.

Tietosuoja huomioidaan jo hankintojen suunnitteluvaiheessa. Tilaajan vastuulla on huolehtia, että tarjouspyyntöihin ja palvelusopimuksiin sisällytetään kaupungin tietohallinnon ylläpitämät tietoturva- ja tietosuojavaatimukset täydennettynä palvelua käyttävän toimialaan tai yksikköön sekä palveluun itseensä mahdollisesti liittyvillä erityisvaatimuksilla. Lisäksi tarjouspyyntöihin ja sopimuksiin on sisällytettävä palvelutaso, toiminta häiriötilanteissa ja vastuunjako koko arvoketjun läpi.

## TOIMINTAMALLIT

### Seuranta

Tietohallinnon tehtävänä on raportoida tietoturvaloukkauksista, riskeistä ja kehittämiskohteista viipymättä konsernijohdolle, tietoturva- ja tietosuojaryhmälle sekä ICT-palveluiden tuottajille. Vakavista poikkeamista tiedotetaan myös kaupunginhallitusta. Konsernin tietoturva- ja tietosuojaryhmän tehtävänä taas on seurata tietoturvan- ja tietosuojan nykytilaa.

ICT-palveluiden tuottajien tehtävänä on raportoida tietoturvaloukkauksista, riskeistä ja kehittämiskohteista viipymättä sekä tietohallinnolle että kaupungin nimeämälle palvelun omistajalle tai pääkäyttäjälle.

Vastuualueiden johdon on oltava ajan tasalla tietoturvasta, tietosuojasta ja niihin liittyvistä riskeistä. Tietoturva- ja tietosuoja-asioista raportoidaan osana sisäistä tarkastusta. Sisäisestä tarkastuksesta Pieksämäen kaupungissa vastaavat hallintojohtaja ja tarkastuslautakunta.

Kaupungissa laaditaan vuosittain tietotilinpäätös, johon on koottu tietojenkäsittelyn tärkeimmät tunnusluvut ja tietovirrat. Lisäksi kaupunginhallitukselle tuodaan kerran vuodessa tiedoksi koonti tietoturvaan ja -suojaan liittyvistä häiriöistä, poikkeamista ja uhkista.

Tietosuojavastaava ylläpitää kokonaiskuvaa kansallisesta tietosuojasta ja siihen liittyvistä riskeistä.

## Arviointi

Tietohallinnon tehtävänä on säännöllisesti arvioida tietoturvaa järjestelmäkohtaisesti ja kokonaisuutena. Arvioinnit voivat kohdistua sekä kaupungin ja sen sidosryhmien että ICT-palveluntuottajien toimintaan. Arvioinnin kohteena on tietoturvan kolmen pääkäsitteen - saatavuuden, eheyden ja luottamuksellisuuden - toteutuminen ja tavoitteena on tunnistaa niihin liittyviä riskejä ja kehittämiskohteita.

Tietohallinto priorisoi arviointikohteet. Priorisointiperusteena on järjestelmän tai palvelun vaikutus kaupungin palvelutuotantoon.

Tietosuojan toteutumisen arviointi lisätään osaksi sisäisen tarkastuksen toimintaa vuosittain toteutuvaksi. Tietosuoja-arvioinnista vastaa tietosuojavastaava.

## Kehittäminen

Tietohallinto tarkentaa tietoturvan ja tietosuojan kehittämisen tavoitteet vuosittain tavoitteiden pohjalta huomioiden sekä seurannan että arviointien tuottaman tiedon. Tietohallinto huomioi kehittämistavoitteet kaupungin kokonaisarkkitehtuurin kehittämisen yhteydessä.

## Tiedottaminen

Kaupungin sisäisestä tietoturva- ja tietosuojatiedottamisesta vastaa tietohallinto ja tietosuojavastaava. Toimialat ja liikelaitokset vastaavat lisäksi tiedon välittämisestä oman orga-

nisaation sisällä.

ICT-palvelun tai tietojärjestelmän operatiivisista ongelmista ja häiriöistä tiedottaminen on tietohallinnon sekä tietojärjestelmän omistajan tai sen sopimuksin valtuuttaman tahon vastuulla.

Ulkoisesta tiedottamisesta huolehtii viestintävastaava.

## Toiminta häiriötilanteissa

Kaupungin toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Palvelualueet, liikelaitokset, taseyksiköt ja yhtiöt laativat kukin valmiussuunnitelman omalta osaltaan. Suunnittelussa tulee varautua pieneen, keskisuureen ja suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin.

Kaupunginvaltuusto hyväksyy kaupunkikonsernia koskevat sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa.

Kaupungin ICT-infrastruktuurin tai tietojärjestelmien toimintaa, tietoturvaa tai tietosuojaa uhkaavissa tilanteissa vastatoimenpiteet on aloitettava välittömästi ja niistä on raportoitava tietohallintopäällikölle.

Tietoturva- ja tietosuojarikkomukset käsitellään tapauskohtaisesti. Tietohallintopäälliköllä tai tietohallinnon sopimuksin valtuuttamalla taholla on oikeus sulkea tietoliikenneyhteys, järjestelmä, käyttäjätunnus tai laite uhkatilanteen vahinkojen minimoimiseksi. Tietohallintopäällikkö informoi asianosaisia suoritetuista toimenpiteistä ja mahdollisista jatkotoimenpiteistä mahdollisimman pian.

Henkilötietojen tietoturvaloukkauksen sattuessa kaupungilla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

# LIITE 1:
# TIETOTURVAAN JA TIETOSUOJAAN LIITTYVIÄ OHJEITA JA LAKEJA

Toimintaa ohjaa aina voimassa olevat lait, asetukset, direktiivit ja hyvät käytännöt.

Kansallisia ohjeita (tilanne 29.11.2018)

| **Sisältö** | Sijainti |
|---|---|
| VAHTI, voimassaolevat ohjeet | http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp |
| VM:n VAHTI, julkisen hallinnon digitaalisen turvallisuuden johtoryhmä | http://vm.fi/vahti |
| VAHTI - ohjesivusto | https://www.vahtiohje.fi/web/guest/home |
| EU:n tietosuojauudistus | http://www.tietosuoja.fi/1554.htm |

Kaupungin tietoturva- ja tietosuojatyötä ohjaavaa lainsäädäntöä (tilanne 29.11.2018)

| **Laki** | Sisältö tietoturvan näkökulmasta |
|---|---|
| Arkistolaki 831/1994 | Arkistointia on hoidettava siten, että se tukee arkistonmuodostajan tehtävien suorittamista sekä yksityisten ja yhteisöjen oikeutta saada tietoja julkisista asiakirjoista, että yksityisten ja yhteisöjen oikeusturva samoin kuin tietosuoja on otettu asianmukaisesti huomioon ja että yksityisten ja yhteisöjen oikeusturvaan liittyvien asiakirjojen saatavuus on varmistettu sekä että asiakirjat palvelevat tutkimuksen tiedon lähteinä. |
| Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999 | Viranomaisen on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 18 §:n 1 momentin 4 kohdassa tarkoitettujen toimenpiteiden suunnittelua ja toteuttamista varten arkistolaissa (831/1994) tarkoitettua arkistonmuodostussuunnitelmaa hyväksi käyttäen selvitettävä ja arvioitava asiakirjansa ja tietojärjestelmänsä sekä niihin talletettujen tietojen merkitys samoin kuin asiakirja- ja tietohallintonsa. |
| Hallintolaki 434/2003 | Tämän lain tarkoituksena on toteuttaa ja edistää hyvää hallintoa sekä oikeusturvaa hallintoasioissa. Lain tarkoituksena on myös edistää hallinnon palvelujen laatua ja tuloksellisuutta. |
| Henkilötietolaki 523/1999 | Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. (1§)<br><br>Tätä lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Myös muuhun henkilötietojen käsittelyyn sovelletaan tätä lakia silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. (2 §) |
| Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011 | Tämän lain tarkoituksena on tehostaa julkisen hallinnon toimintaa sekä parantaa julkisia palveluja ja niiden saatavuutta säätämällä julkisen hallinnon tietohallinnon ohjauksesta ja tietojärjestelmien yhteentoimivuuden edistämisestä ja varmistamisesta. (1 §) |

| | |
|---|---|
| Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004 | kansainvälisellä tietoturvallisuusvelvoitteella sellaista Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä sellaista muuta Suomea koskevaa velvoitetta, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä; erityissuojattavalla tietoaineistolla sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu; turvallisuusluokitellulla sopimuksella sopimusta, jonka toisen valtion viranomainen tai siellä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimielin aikoo tehdä tai on tehnyt kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon. (2 §) |
| Laki potilaan asemasta ja oikeuksista 785/1992 | Potilaan asemaan ja oikeuksiin terveyden- ja sairaanhoitoa järjestettäessä sovelletaan tätä lakia, jollei muussa laissa toisin säädetä. |
| Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 22.9.2000/812 | Tämän lain tarkoituksena on edistää asiakaslähtöisyyttä ja asiakassuhteen luottamuksellisuutta sekä asiakkaan oikeutta hyvään palveluun ja kohteluun sosiaalihuollossa. |
| Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007 | Tämän lain tarkoituksena on edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä. Lailla toteutetaan yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjestelmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi. (1§)<br><br>Tässä laissa säädetään sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Tätä lakia sovelletaan julkisten ja yksityisten sosiaalihuollon ja terveydenhuollon palvelujen antajien järjestäessä taikka toteuttaessa sosiaalihuoltoa tai terveydenhuoltoa (2 §). |
| Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003 | Tämän lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa edistämällä sähköisten tiedonsiirtomenetelmien käyttöä. Laissa säädetään viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa. (1 §) |
| Laki sähköisestä lääkemääräyksestä 61/2007 | Jollei tästä laista muuta johdu, sähköistä lääkemääräystä laadittaessa, toimitettaessa ja käsiteltäessä on noudatettava, mitä muualla säädetään potilaan asemasta ja oikeuksista, lääkkeen määräämisestä ja toimittamisesta, henkilötietojen käsittelystä, viranomaisten toiminnan julkisuudesta, sähköisestä viestinnästä ja asioinnista sekä sähköisistä allekirjoituksista. (2 §, 3. kappale) |
| Laki tietoyhteiskunnan palvelujen tarjoamisesta 458/2002 | Tässä laissa säädetään tietoyhteiskunnan palvelujen tarjoamiseen liittyvistä seikoista, erityisesti palvelujen tarjoamisen vapaudesta, palvelun tarjoajien velvollisuudesta antaa tietoja, sopimusta koskevien muotovaatimusten täyttämisestä sähköisesti sekä välittäjänä toimivien palvelun tarjoajien vastuuvapaudesta. (1 §) |
| Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009 | Tässä laissa säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä niihin liittyvien palveluiden tarjoamisesta niitä käyttäville palveluntarjoajille ja yleisölle. (1 §) |
| Laki viranomaisten toiminnan julkisuudesta 621/1999 | Laissa säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. (3 §) |

| | |
|---|---|
| Laki yksityisyyden suojasta työelämässä 759/2004 | Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. (1 §)<br><br>Tässä laissa säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta. Mitä tässä laissa säädetään työntekijästä, sovelletaan myös virkamieheen, virkasuhteessa olevaan ja näihin verrattavassa julkisoikeudellisessa palvelussuhteessa olevaan sekä soveltuvin osin työnhakijaan. (2 §) |
| Rikoslaki 39/1889 | 34 luku, 9 a § Vaaran aiheuttaminen tietojenkäsittelylle<br>38 luku, Tieto- ja viestintärikoksista |
| Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 30.3.2009/298 | Tätä asetusta sovelletaan potilaan hoidon järjestämisessä ja toteuttamisessa käytettävien asiakirjojen laatimiseen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämiseen. (2 §) |
| Laki sosiaalihuollon asiakasasiakirjoista 254/2015 | Tämän lain tarkoituksena on toteuttaa yhdenmukaisia menettelytapoja käsiteltäessä sosiaalihuollon asiakasta koskevia tietoja ja siten edistää sosiaalihuollon tehtävien asianmukaista hoitamista. |
| Suomen perustuslaki 731/1999 | Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu.<br>Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. (10 §) |
| Sähköisen viestinnän tietosuojalaki 516/2004 | Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. (1 §) |
| Terveydenhuoltolaki 1326/2010 | Käytettäessä toisen terveydenhuollon toimintayksikön tietoja tietojärjestelmien välityksellä, on potilastietojen käyttöä seurattava sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 5 §:n edellyttämällä tavalla. Hoitosuhde potilaan ja luovutuspyynnön tekijän välillä on varmistettava tietoteknisesti. (9 §, 4 kappale)<br><br>Sairaanhoitopiirin kuntayhtymän on vastattava yhteisen potilastietorekisterin edellyttämistä koordinointitehtävistä sekä huolehdittava siitä, että tietojärjestelmien välityksellä tapahtuvissa tietojen luovutuksissa noudatetaan 2 ja 3 momentissa säädettyjä velvoitteita. Kukin terveydenhuollon toimintayksikkö vastaa omassa toiminnassaan syntyneiden potilasasiakirjojen rekisterinpidosta henkilötietolain (523/1999) mukaisesti. (9 §, 5 kappale) |

Tietoturva- ja tietosuojapolitiikka on käsitelty YT:ssä 10.12.2018 ja kaupunginhallituksessa 21.01.2019.

PIEKSÄMÄKI

Elämäsi asemapaikka

PIEKSÄMÄEN KAUPUNKI Kauppakatu 1, 76100 Pieksämäki.
Puh. 015 788 2111, kirjaamo@pieksamaki.fi