HYVINKÄÄN KAUPUNGIN TIETOTURVA



Käsitelty yhteistyötoimikunnassa 16.04.2020 / 28 § Dnro HYD/756/07.01.01/2020

Hyväksytty kaupunginhallituksen kokouksessa 27.04.2020 / 84 § Dnro HYD/756/07.01.01/2020

Sisällys

[1. Johdanto 2](#_Toc43211657)

[2. Roolit ja raportointi 3](#_Toc43211658)

[3. Yleiset tietoturvatavoitteet ja -periaatteet 4](#_Toc43211659)

[4. Tietoturvallisuuden johtaminen ja vaikutus tiedonhallintaan 5](#_Toc43211660)

[5. Tietoturva-asiakirjan soveltamisohjeet 6](#_Toc43211661)

[6. Toiminta tietoturva- ja tietosuojapoikkeamatilanteessa sekä ilmoitusvelvollisuus 7](#_Toc43211662)

[7. Seuranta, valvonta ja jatkuva kehittäminen 7](#_Toc43211663)

[8. Toimeenpano 7](#_Toc43211664)

[9. Keskeiset käsitteet 9](#_Toc43211665)

# Johdanto

Tämä asiakirja on Hyvinkään kaupungin tietoturvapolitiikka. Hyvinkään kaupungin toiminta perustuu tietoon ja sen hallittuun hyödyntämiseen. Onnistuminen tiedonhallinnassa ja tietojenkäsittelyssä on yksi tärkeimmistä palvelutuotannon ja hallinnon tehokkuuteen, tuottavuuteen ja laatuun vaikuttavista menestystekijöistä. Siksi myös tietoturvallisuudesta huolehtiminen on erottamaton osa kunnan ydintoimintaa.

Vastuu kaupungin toiminnasta ja sen tietoturvallisuudesta on sen ylimmällä johdolla. Johdon vahvistamat tietoturvaa koskevat määräykset ja linjaukset ovat strategisia päätöksiä, jotka vaikuttavat kunnan palvelu- ja kehittymiskykyyn sekä toiminnan säädöstenmukaisuuteen.

Tietoturva tarkoittaa tiedon luottamuksellisuuden, eheyden ja käytettävyyden ylläpitämistä. Näistä huolehditaan Hyvinkään kaupungin tietoturvatoimenpiteillä.

|  |
| --- |
| *Luottamuksellisuus:* Turvaamalla suojattavan kohteen luottamuksellisuus pyritään estämään tiedon näkyminen ulkopuolisille tahoille.*Eheys:* Eheyden tarkoituksena on varmistaa, että informaatiota ei päästä muokkaamaan ilman asianmukaisia valtuutuksia (tiedon yhtäpitävyys alkuperäisen tiedon kanssa).*Käytettävyys:* Tiedon käytettävyys turvataan, kun tieto on saatavilla silloin, kun sitä tarvitaan ja niille tahoille, jotka tietoa tarvitsevat (tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana). |

Tietoturva-asiakirja määrittelee Hyvinkään kaupungin tietoturvallisuuden yleiset tavoitteet ja periaatteet sekä toiminnan häiriötilanteissa ja poikkeusoloissa. Tietoturva-asiakirjassa kaupungin johto määrittelee tietoturvallisuuden päämäärät, periaatteet ja toteutuksessa käytettävät keinot sekä eri toimijoiden vastuut tietoturvallisuutta koskevien tavoitteiden saavuttamiseksi.

Tietoturva-asiakirja toimii perustana Hyvinkään kaupungin tietoturvallisuutta koskeville muille ohjeistuksille, joiden tehtävänä on tarkentaa tietoturva-asiakirjassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietoturva-asiakirja koskee koko emokaupungin organisaatiota (kaupunki, mukaan lukien taseyksiköt ja liikelaitokset) ja sen henkilöstöä sekä luottamushenkilöitä.

Tietoturva-asiakirjan ja sen soveltamisohjeiden lisäksi ja niiden kanssa yhtenevästi tulee noudattaa myös Hyvinkään kaupungin tietosuoja-asiakirjaa ja siinä määriteltyjä tietosuojan toimintaperiaatteita.

# Roolit ja raportointi

Tietoturvallisuuteen liittyvät vastuut ja tehtävät jakautuvat eri rooleissa toimiville henkilöille seuraavasti:

**Kaupungin ylin johto** Hyvinkään kaupungin ylin johto (kaupunginhallitus ja kaupunginjohtaja sekä toimialojen johto) vastaa tietoturvan yleisistä linjauksista ja yleisen vaatimustason määrittelystä, yleisen tietoturvaohjeistuksen riittävyydestä ja ajantasaisuudesta, säädösten huomioon ottamisesta sekä halutun tietoturvatason toimeenpanoon tarvittavien resurssien osoittamisesta.

**Kaupunginjohtaja** Kaupunginjohtaja nimeää kaupungin yhteisen tietoturvapäällikön sekä tietosuoja- ja tietoturvatyöryhmän jäsenet ja puheenjohtajan/t.

**Tietoturvapäällikkö** Vastaa tietoturva-asiakirjaa soveltavan ohjeistuksen valmistelusta, tietoriskien kartoittamisesta ja niiden hallintakeinojen tunnistamisesta, tietoturvatyön koordinoinnista, tietoturvaa koskevasta yleisestä tiedottamisesta, tietoturvallisuuden toteutumisen seurantajärjestelyistä sekä tarvittavasta raportoinnista kaupungin johdolle.

**Tietosuoja- ja tietoturvatyöryhmä**

Hyvinkään kaupungilla toimii tietosuoja- ja tietoturvatyöryhmä, johon osallistuu edustaja kaikilta toimialoilta. Ryhmä kokoontuu säännöllisesti ja sen tehtävänä on kehittää koko Hyvinkään kaupungin tietosuojaa ja tietoturvaa. Työryhmä raportoi Hyvinkään kaupungin johdolle.

**Työryhmän jäsenet** Tietosuoja- ja tietoturvatyöryhmän jäsenten tehtävänä on kommunikoida työryhmässä esiin tulleita ja siellä käsiteltyjä asioita toimialoille sekä tuoda toimialoilta tietoa ja kysymyksiä työryhmän käsittelyyn. Työryhmän jäsenet edistävät oman toimialansa tietosuoja- ja tietoturvatyötä.

**Tietojärjestelmien omistajat**

Vastaavat tietojen luokittelusta, tietoon liittyvien oikeuksien määrittelystä, näihin liittyvästä soveltavasta tietoturvaohjeistuksesta ja tietojärjestelmä-kohtaisten käyttövaltuuksien hallinnasta.

**Tietohallintopäällikkö**

 Vastaa kaupungin tietojenkäsittely-ympäristön tietoteknisestä tietoturva-suunnittelusta ja tähän liittyvästä ylläpidon ja käytön ohjeistuksesta sekä näiden noudattamisen seurannasta.

**Tietohallinto**

 Vastaa suunniteltujen tietoteknisten tietoturvatoimien järjestämisestä yhdessä palveluntuottajien kanssa.

**Esimiestehtävässä toimiva**

 Jokainen esimies vastaa alaisensa henkilöstön perehdyttämisestä ja sitouttamisesta voimassa olevaan tietoturvallisuutta koskevaan ohjeistukseen ja tarvittaviin muihin tietoihin sekä valvoo, että hänen johtamassaan toiminnassa näitä ohjeita noudatetaan.

**Kaupungin työntekijä**

 Jokainen kaupungin työntekijä vastaa osaltaan asianmukaisesta tietojen käsittelystä ja tietojärjestelmien käytöstä annettujen ohjeiden ja säädösten mukaisesti.

**Hankintoja ja sopimuksia tekevät**

 Vastaavat siitä, että tavoiteltava tietoturvallisuuden taso otetaan huomioon myös ostopalvelusopimuksissa sekä kumppanuus- ja ulkoistusratkaisuissa.

Myös muita kuin tässä mainittuja tietoturvapolitiikan toteuttamisen kannalta tarpeellisiksi katsottavia tehtävärooleja on mahdollista määritellä ja antaa kaupunginjohtajan tai toimialajohdon päätöksillä nimetyille henkilöille tai työryhmille.

# Yleiset tietoturvatavoitteet ja -periaatteet

Hyviinkään kaupungin tietoturvatyön tavoitteena on varmistaa tietojen luottamuksellisuus, eheys ja käytettävyys sekä näiden myötä kaupungin palvelutuotannon ja muiden toimintojen luotettavuus, laatu ja jatkuvuus. Kaupungissa noudatetaan lainsäädännön tarkoittamaa hyvää hallintotapaa ja hyvää tiedonhallintatapaa. Tietojenkäsittelyssä noudatetaan voimassa olevia lakeja, asetuksia ja niihin verrattavia viranomaisten määräyksiä.

Tietojen luottamuksellisuuden turvaamiseksi tulee salassa pidettävät ja käyttörajoitetut tietoaineistot luokitella ja merkitä asianmukaisesti. Tietojärjestelmiin tulee sisällyttää tehokkaat käyttöoikeuksien määrittelyt ja tekniset suojaukset, joilla varmistetaan, että luokiteltuja tietoja saavat käyttöönsä vain ne, jotka ovat niihin julkisuus-, salassapito- tai tietosuojasäädösten tai kaupungin omien tietojenkäsittelyä koskevien määräysten perusteella oikeutettuja.

Hyvinkään kaupunki huolehtii tietojen eheydestä tietoaineistojen suunnitelmallisella kartoittamisella ja säilyttämisellä, jossa otetaan huomioon sekä toiminnallisten tarpeiden että säädösten tietojenkäsittelylle asettamat vaatimukset. Tietojärjestelmien vaatimusmäärittelyissä ja toteutuksissa sekä käyttöohjeissa tulee huomioida tietosisältöjen pysyminen tarkoituksenmukaisina, tarpeet kattavina ja vääristymättöminä (oikeina, aitoina, ehjinä) tietojenkäsittelyn kaikissa vaiheissa, sekä käyttötilanteessa helppotulkintaisina.

Tietohallintopalvelut yhdessä ulkoisten palveluntarjoajien kanssa varmistaa tietojen käytettävyyden huolehtimalla mm. tietojärjestelmien hyvästä toimintavarmuudesta ja riittävästä suorituskyvystä sekä tietoaineistojen asianmukaisesta säilyttämisestä ja varmuuskopioimisesta. Myös manuaalisesti käsiteltävien tietojen saatavuus tulee varmistaa asianmukaisilla säilytystavoilla ja toimenpiteillä. Työntekijöillä on kulloinkin ilman kohtuutonta vaivaa tai viivästystä oltava käytettävissään työn menestyksekkään hoitamisen edellyttämät tiedot.

Kaupungin tietoturvallisuus mitoitetaan kaupungin kokonaistaloudellinen etu huomioiden mahdollisimman tarkoituksenmukaiseksi eli optimaaliseksi — ei välttämättä maksimaaliseksi.

Tietoturvallisuuden tavoitetasoa määritettäessä ja eri tilanteisiin sovellettaessa otetaan huomioon kaupungin omien tarpeiden lisäksi yleisesti kunnalliselle ja muulle viranomaistoiminnalle asetetut vaatimukset ja suositukset. Tietoturvallisuuden toteutuskeinoja valittaessa ja eri tilanteisiin sovellettaessa tulee lisäksi huomioida tietojen ja tietojärjestelmien käytettävyyteen liittyvät vaatimukset ja tietoturvajärjestelyjen aiheuttamat kustannukset.

Tilanteissa, joissa tietoturvatoimet voisivat aiheuttaa ristiriitoja kaupungin muiden tavoitteiden ja velvoitteiden kanssa, sovelletaan seuraavaa tärkeysjärjestystä:

1 ihmishenkien ja terveyden turvaaminen

2 merkittävien omaisuusvahinkojen estäminen

3 salaisen, arkaluonteisen tai muun erityisen tärkeän tiedon turvaaminen

4 muun kaupungin toiminnan kannalta olennaisen tiedon turvaaminen

5 tieto ja viestintäjärjestelmien vahingoittumisen estäminen

6 tieto ja viestintäjärjestelmien käytettävyyden turvaaminen

7 vähäisten omaisuusvahinkojen tai (lisä)kustannusten estäminen

# Tietoturvallisuuden johtaminen ja vaikutus tiedonhallintaan

Tietoturvallisuuden varmistaminen ja edistäminen on osa Hyvinkään kaupungin toiminnan johtamista ja riskienhallintaa. Tietoriskien hallinnasta ja tietojen riittävästä turvallisuudesta huolehditaan sekä manuaalisessa että tietotekniikan avulla tapahtuvassa tietojenkäsittelyssä.

Tietoturvallisuudesta huolehditaan tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan, mukaan lukien tietojen arkistointi ja suunniteltu hävittäminen. Poikkeusoloihin varautuminen kuvataan erikseen kaupungin tietojenkäsittelyn valmiussuunnitelmassa, ja vakavien järjestelmäkeskeytysten varalle laaditaan erilliset toipumis- ja jatkuvuussuunnitelmat.

Tietoturvan suunnittelussa huomioon otettavat osa-alueet ovat:

hallinnollinen turvallisuus

henkilöstöturvallisuus

fyysinen turvallisuus

tietoaineistoturvallisuus

laitteistoturvallisuus

ohjelmistoturvallisuus ja

* käyttöturvallisuus

Käytännön tietoturvajärjestelyt on mahdollisuuksien mukaan toteutettava niin, että turvallisuusloukkausten ja muiden tietoturvapoikkeamien havaitseminen ja selvittäminen myös jälkikäteen on mahdollista.

Kaupungin tietoaineistot ja tietojärjestelmät luokitellaan niiden kriittisyyden mukaan hyödyntäen kunta-alalle sovittuja tai suositeltuja yleisesti käytettäviä luokituksia. Luokittelut on tehtävä ennakoivasti niin, että niiden vaatimat tietoturvallisuusjärjestelyt — kuten toimintatapoihin tai teknisiin suojauksiin kohdistuvat erityisvaatimukset — voidaan ottaa huomioon jo tietojärjestelmiä hankittaessa.

Tietoturvajärjestelyjen aiheuttamia kustannuksia käsitellään normaaleina toimintamenoina, jotka tulee ottaa huomioon toimintaa suunniteltaessa ja talousarvioesityksiä valmisteltaessa.

Henkilöstön tietoturvatietoisuudesta huolehditaan perehdytyksen, työnjohdon ja sisäisen tiedottamisen keinoin; päävastuu tästä on esimiehillä. Tietohallintopalvelut tukee ja koordinoi esimiehiä tässä työssä. Tietoturvapolitiikan toteuttamisen kannalta avaintehtävissä oleville ja tarpeen mukaan myös muulle henkilöstölle järjestetään mahdollisuus saada tietoturvallisuuskoulutusta.

# Tietoturva-asiakirjan soveltamisohjeet

Tietoturva-asiakirjan noudattamiseksi ja soveltamiseksi laaditaan tarpeen mukaan tarkentavia ohjeita, joiden hyväksymisestä ja vahvistamisesta vastaa ohjeen kattavuudesta ja soveltamisalasta riippuen joko kaupunginjohtaja, toimialajohtaja, kaupungin tietoturvapäällikkö, tietohallinto-päällikkö tai asianomaisen tietojärjestelmän omistaja – ellei vastuuta ole hallintosäännössä tai muutoin määritetty tietyn luottamuselimen käsiteltäväksi. Ohjeet on saatettava kohderyhmänsä tietoon ja saataville riippumatta siitä, onko ne laadittu erillisinä asiakirjoina vai sisällytetty muihin asiakirjoihin.

Kaupunginjohtaja vahvistaa ohjeet, jotka:

* koskevat kaupungin johtamisjärjestelmää tai käytäntöjä tai muutoin laajavaikutteisesti koko henkilöstöä
* ovat taloudellisesti, toiminnallisesti tai henkilöstöpoliittisesti merkittäviä
* liittyvät varautumis- tai valmiussuunnitteluun

tai

* vaikuttavat välittömästi kaupungin julkisuuskuvaan tai sidosryhmäyhteistyöhön

Toimialajohtajat voivat vahvistaa ohjeita, jotka koskevat tiettyä toimialaa tai hallintokuntaa. Nämä ohjeet ovat tyypillisesti tarkennuksia kaupungin yleisiin ohjeisiin eivätkä saa olla näiden kanssa ristiriidassa. Toimialakohtaiset ohjeet voivat perustua myös toimialaa koskevaan erityislain-säädäntöön.

Tietojärjestelmien omistajat voivat antaa ohjeita, jotka koskevat kyseistä tietojärjestelmää. Nämä ohjeet ovat tyypillisesti tarkennuksia kaupungin yleisiin tai toimialakohtaisiin ohjeisiin eivätkä saa olla näiden kanssa ristiriidassa.

Tietoturvapäällikkö ja tietohallintopäällikkö voivat antaa muita ohjeita, tiedotteita ja esimerkiksi asiakirjamalleja, joiden avulla tietoturvapolitiikkaa voidaan soveltaa erilaisiin käytännön tilanteisiin.

Sellaiset tietoturvajärjestelyjä käsittelevät ohjeet ja muut asiakirjat (esimerkiksi tietojärjestelmien tekniset spesifikaatiot), joiden julkistaminen voisi vaarantaa kaupungin tietoturvallisuuden toteuttamisen ja ylläpidon tietoturvapolitiikan tarkoittamalla tavalla, tulee luokitella kaupungin sisäiseen käyttöön tarkoitetuiksi ja tarvittaessa tätäkin rajoitetummin salassa pidettäviksi. Käyttörajoitus tulee merkitä ao. asiakirjaan.

# Toiminta tietoturva- ja tietosuojapoikkeamatilanteessa sekä ilmoitusvelvollisuus

Jokainen Hyvinkään kaupungin työntekijä ja erityisesti tässä tietoturva-asiakirjassa määritellyissä rooleissa toimivat henkilöt ovat velvoitettuja ilmoittamaan havaitsemistaan tietoturvallisuuden loukkauksista tai muista tietoturvapoikkeamista viipymättä esimiehelleen, asianomaisen tietojärjestelmän omistajalle sekä toimialansa tietoturvavastaavalle tai kaupungin tietoturvapäällikölle. Tällaisen ilmoituksen saaja on velvoitettu viipymättä ryhtymään havaitun loukkauksen, poikkeaman tai puutteen edellyttämiin jatkotoimiin tietoturvapolitiikan soveltamisohjeissa määritetyllä tavalla.

Mikäli Hyvinkään kaupungin ja sen toimialojen toiminnassa herää epäilys henkilötietoihin kohdistuvasta tietoturvaloukkauksesta, osallistetaan kaupungin tietosuojavastaava tapauksen käsittelyyn välittömästi. Hyvinkään kaupunki on määrittänyt erikseen sisäisen prosessin henkilötietoihin kohdistuvien tietoturvaloukkausten käsittelemiseksi, arvioimiseksi sekä valvontaviranomaiselle ja/tai rekisteröidyille ilmoittamiseksi.

Tahallisista tai tuottamuksellisista tietoturvarikkomuksista voi olla seurauksena palvelussuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä rangaistuksia.

# Seuranta, valvonta ja jatkuva kehittäminen

Hyvinkään kaupunki on sitoutunut säännöllisesti arvioimaan ja varmistamaan riittävän tason tietoturvaan liittyvissä käytännöissään. Tietoturvaan liittyvien ohjeistusten noudattamista valvotaan. Kaikki tietoturvaan liittyvät rikkomustilanteet selvitetään ja niihin suhtaudutaan vakavasti. Tietoturvarikkomustilanteet ja niistä aiheutuvat seuraamukset käsitellään tapauskohtaisesti.

# Toimeenpano

Tämä tietoturva-asiakirja tulee voimaan ja noudatettavaksi heti, kun kaupunginhallitus on sen vahvistanut ja soveltamisohjeineen se korvaa kaupunginhallituksen 11.4.2011 (§ 97) vahvistaman tietoturvapolitiikan (Dnro 480/2011) (00.011).

Ennen tämän tietoturva-asiakirjan vahvistamista laaditut tietoturvallisuutta käsittelevät ohjeet tulee tarkistaa ja päivittää (tai kumota) kuuden kuukauden kuluessa tämän tietoturva-asiakirjan voimaantulosta siten, etteivät ne ole ristiriidassa tietoturva-asiakirjan tahi sen perusteella laadittujen uusien soveltamisohjeiden kanssa.

Oikeus aiemman ohjeen päivittämiseen tai kumoamiseen on sillä, jolle tämän tietoturva-asiakirjan mukaan kuuluu oikeus korvaavan ohjeen antamiseen.

Kulloinkin voimassa oleva ohjeistus on saatettava viipymättä koko henkilöstön saataville, ja esimiesten on varmistettava, että henkilöstö on ohjeistuksesta ja sen sisällöstä tietoinen.

Tietoturvapäällikkö avustaa kaupunginjohtajaa ja tietosuoja- ja tietoturvatyöryhmän jäsenet toimialajohtajia tietoturva-asiakirjan noudattamisen seurannassa ja valvonnassa.

Tämä tietoturva-asiakirja on voimassa toistaiseksi ja sen luokitus on julkinen.

Tämän tietoturva-asiakirjan lisäksi Hyvinkään kaupungilla on erillinen tietosuoja-asiakirja.

# Keskeiset käsitteet

”Riski” Riski tarkoittaa tapahtuman todennäköisyyden ja vaikutusten yhdistelmää.

Riski lasketaan tapahtuman todennäköisyyden (t) ja vaikutuksen (v) tulona (riski = t \* v). Riskit voivat olla myönteisiä tai kielteisiä. Riskit voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön tai yhteisöllisiin arvoihin.

”Tietoturva; tietoturvallisuus”

Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.

Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa.

”Haavoittuvuus”

Haavoittuvuus tarkoittaa alttiutta tietoturvaan kohdistuville uhkille.

Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa. Jos haavoittuvuus on saatettu julkiseen tietoon, mutta sitä ei ole tiedon julkaisemiseen mennessä korjattu, sitä kutsutaan nollapäivä-haavoittuvuudeksi.

”Tietoturvahäiriö; tietoturvapoikkeama”

Tietoturvahäiriö tai -poikkeama on yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka erittäin todennäköisesti vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan.

”Tietoturvahäiriön hallinta; tietoturvapoikkeaman hallinta”

Toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi.

”Tietoturvaloukkaus”

Tietoturvaloukkauksella tarkoitetaan oikeudetonta puuttumista tietoon tai tietojärjestelmiin.

Yleisimmät tietoturvaloukkaukset ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.