

VANTAAN KAUPUNGIN TIETOTURVAPOLITIIKK A

Vantaan kaupunginhallitus xx.xx.2026

SISÄLLYSLUETTELO

1. TETOTURVATAVOITTEET.....	3
2. TETOTURVATYÖN PERIAATTEET.....	3
2.1. Tietoriskien arviointi.....	3
2.2. Tietojen arviointi suojaamisen näkökulmasta.....	4
2.3. Valvonta ja tietoturvapoikkeamien käsittely.....	4
3. TETOTURVAN VASTUUT JA ORGANISOINTI.....	5
3.1. Tietoturvan vastuut.....	5
3.1.1. Kaupunginhallitus ja kaupunginjohtaja.....	5
3.1.2. Apulaiskaupunginjohtajat.....	5
3.1.3. Palvelualueiden johtajat ja palveluyksiköiden päälliköt sekä muut esihenkilöt.....	6
3.1.4. Vantaan konserniyhteisöt.....	6
3.1.5. Palveluntuottajat.....	6
3.1.6. Työntekijät ja muut tietojen käsittelijät.....	7
3.2. Suojattavan omaisuuden omistajuus.....	7
3.2.1. Tiedon omistajat.....	7
3.2.2. Tietojärjestelmien ja tietoteknisten laitteiden omistajat.....	8
3.3. Tietoturvatyön organisointi.....	8
3.3.1. Kaupunkitasoisen tietoturvan kehittäminen ja hallinta.....	9
3.3.2. Tietoturvakoulutus.....	9
3.3.3. Tietoturva- ja tietosuojatyöryhmä.....	9
3.3.4. Tietohallinto ja tietotekniset hankinnat.....	9
3.3.5. Hankinnan palveluyksikkö ja muut kuin tietotekniset hankinnat.....	10



JOHDANTO

Tietoturvapolitiikka määrittelee Vantaan kaupungin ylätason linjaukset tietoturvan toteuttamisesta. Tietoturvapolitiikka sisältää tavoitteet, periaatteet, vastuut ja toimintatavat, jotka ohjaavat kaupungin toimintaa tietojen käsittelyssä ja suojaamisessa.

Kaupungin hallintosäännön mukaan tietoturvaa toteutetaan noudattamalla voimassa olevaa lainsäädäntöä, viranomais määräyksiä sekä kaupunginhallituksen vahvistamaa tietoturvapolitiikkaa ja kaupungin sisäisiä määräyksiä ja ohjeita. Hierarkkisesti tämä tietoturvapolitiikka on kaupungin korkeimman tason tietoturvaohje, jolle kaikki kaupungin, toimialojen sekä konserniyhteisöjen tietoturvaohjeistukset ovat alisteisia.

Tietoturvapolitiikka koskee Vantaan kaupungin johtoa, luottamushenkilöitä, viranhaltijoita, henkilöstöä, konsultteja sekä muita kaupungin tietoja käsitteleviä henkilöitä. Se tulee huomioida myös kaupungin käyttämien palveluntuottajien ja sidosryhmien sekä kaupunkikonsernin konserniyhteisöjen toiminnassa. Tietoturvapolitiikkaa täydentävät kaupungin yleiset tietoturvaohjeet sekä toimialojen omat tarkentavat tietoturvaohjeet.

Tietoturvapolitiikka on voimassa toistaiseksi. Asiakirjan sisältöä tarkistetaan ja päivitetään säännöllisesti. Asiakirja on julkinen.

1. TIIETOTURVATAVOITTEET

Tietoturvalla ei ole itseisarvoa, vaan sen tarkoitus on edistää Vantaan kaupungin tavoitteiden saavuttamista ennaltaehkäisemällä häiriöitä. Tietoturvatoimenpiteiden ensisijaisena päämääränä on sekä organisaatioiden vastuulla olevien tietojen että palvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa.

2. TIIETOTURVATYÖN PERIAATTEET

2.1. Tietoriskien arviointi

Tietoturvatyö on kiinteä osa kaupungin johtamista sekä riskienhallintaa. Tietoturvan oikea taso vaihtelee mm. tiedon arvon ja tietojenkäsittely-ympäristön myötä ja se määrittää tietojen käsittelyyn kohdistuvien riskien arvioinnissa osana laajempaa muutosvaikutusten arviointia. Tyypillisesti tietoriskien arvioinnissa tulee ottaa huomioon:

- Luottamuksellisuus: Kukaan asiaton/sivullinen ei näe tai saa haltuunsa tietoa, joka ei ole hänelle tarkoitettu
- Eheys: Tieto on yhdenmukaista alkuperäisen tiedon kanssa
- Saatavuus: Tieto, tietojärjestelmä tai palvelu on siihen oikeutettujen henkilöiden ja järjestelmien saatavilla ja käytettävissä silloin kun sitä tarvitaan
- Kiistämättömyys: Tiedonkäsittelytoimenpiteet suoritetaan niin, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana että sen jälkeen
- Varautuminen: Toiminnan jatkuvuustarpeet on huomioitu myös normaaliolojen häiriötilanteissa tai poikkeusoloissa

2.2. Tietojen arviointi suojaamisen näkökulmasta

Tietoturvan oikeaan tasoon vaikuttaa myös tiedon arvo suojaamisen näkökulmasta tarkasteltuna, arvokkaamman tiedon kohdalla riskinsietokykyä on yleensä vähemmän. Arviointia tehdään tyypillisesti kahdesta eri näkökulmasta, tiedon luottamuksellisuudesta ja tiedon arvosta toiminnalle. Tiedonhallinnan tiedonohjaussuunnitelmista löytyy laaja tietojen luokittelu julkisuus- ja säilytysaikamääreineen. Erityisesti tiedonohjaussuunnitelmien ulkopuolisen tiedon suojaamistarpeen arvioinnissa voidaan apuna käyttää seuraavia luottamuksellisuuteen tai tiedon arvoon liittyviä näkökulmia:

- Julkaistut tiedot: Esimerkiksi internetissä julkaistut tiedot
- Julkiset tiedot: Oletusarvoisesti kaikki viranomaisen asiakirjat ovat julkisia

- Salassa pidettävät tiedot: Lainsäädännön perusteella tietoja voidaan määritellä salassa pidettäväksi. Valmisteluvaiheessa olevia tai muuten ei-asiakirjaksi luokiteltuja tietoja käsitellään kuin salassa pidettäviä tietoja.
- Turvallisuusluokitellut tiedot: Lainsäädännön perusteella valtion viranomaiset voivat määritellä salassa pidettäviä tietoja turvallisuusluokitelluiksi
- Henkilötiedot: Toimintaperiaatteet määritellään kaupungin tietosuojapolitiikassa
- Varautumisen näkökulmasta suojattavat tiedot: Tiedot, jolla on erityistä merkitystä normaaliolojen häiriötilanteissa tai poikkeusoloissa

2.3. Valvonta ja tietoturvapoikkeamien käsittely

Vantaan kaupungin tietoteknisissä ympäristöissä ja palveluissa tulee aina olla kattava tietoturvan tekninen valvonta. Tietoturvapoikkeamien käsittelyssä manuaalista tutkintaa tulee suorittaa tarvittaessa.

Ensisijaisina tavoitteina ovat tietoturvapoikkeamien ennaltaehkäisy ja sen epäonnistuessa nopea toipuminen poikkeamista sekä vahinkojen minimointi.

3. TIETOTURVAN VASTUUT JA ORGANISOINTI

Tietoturvan vastuut on määritelty kaupungin hallintosäännössä. Tässä asiakirjassa syvennetään kaupungin viranhaltijoiden ja organisaatioiden tietoturvavastuita.

3.1. Tietoturvan vastuut

3.1.1. Kaupunginhallitus ja kaupunginjohtaja

Kaupunginhallitus huolehtii kuntalain perusteella kaupungin riskienhallinnan järjestämisestä sekä hallintosäännön mukaan päättää kaupungin tietoturvapoliitikasta.

Hallintosäännön mukaan kaupunginjohtaja vastaa kaupungin tietoturvan ohjauksesta.

3.1.2. Apulaiskaupunginjohtajat

Hallintosäännön mukaan apulaiskaupunginjohtajat vastaavat oman toimialansa tietoturvan järjestämisestä. Apulaiskaupunginjohtajien tulee huolehtia riittävästä tietoturvan resursoinnista, ohjeistamisesta, koulutuksesta ja asioiden säännöllisestä käsittelystä johtoryhmissä toimialoillaan. Apulaiskaupunginjohtajat vahvistavat omia toimialojansa koskevat tietoturvan erityisohjeet. Toimialakohtaiset erityisohjeet voivat tarkentaa, täydentää ja tiukentaa kaupunkitasoista ohjeistusta.

3.1.3. Palvelualueiden johtajat ja palveluyksiköiden päälliköt sekä muut esihenkilöt

Hallintosäännön mukaan palvelualueiden johtajat vastaavat oman palvelualueensa tietoturvan järjestämisestä. Johtajat, päälliköt ja esihenkilöt vastaavat oman vastualueensa osalta

- Palveluiden tuottamisesta tietoturvallisesti
- Riittävästä resursoinnista tietoturvan toteutumiseksi
- Oman ja mahdollisen ulkoisen palveluntuottajan henkilöstön perehdyttämisestä ja sitouttamisesta tietoturvaohjeiden ja -käytäntöjen noudattamiseen sekä heidän käyttöoikeuksiensa hallinnasta ja ajantasaisuudesta
- Toimimisesta tietoturvahavaintojen ja -loukkausten kohdalla kaupungin yleisen sekä palvelualueen oman ohjeistuksen mukaisesti

3.1.4. Vantaan konserniyhteisöt

Vantaan kaupunkikonsernin konserniyhteisöjen toimitusjohtajat ja hallitukset ovat vastuussa organisaationsa tietoturvan järjestämisestä voimassa olevan lainsäädännön sekä kaupungin tietoturvapolitiikan ja ohjeistusten mukaisesti.

Konserniyhteisöjen johto vastaa organisaationsa tietoturvasta. Hallitus valvoo johdon toimintaa. Johdon tulee huolehtia riittävästä resursoinnista, ohjeistamisesta ja koulutuksesta organisaatiossaan. Toimitusjohtaja vahvistaa organisaatiota koskevat tietoturvan erityisohjeet. Konserniyhteisöjen erityisohjeet voivat tarkentaa, täydentää ja tiukentaa kaupunkitasoista ohjeistusta.

3.1.5. Palveluntuottajat

Palvelusopimuksessa tulee sopia tietoturvaan liittyvistä vaatimuksista ja käytännön toteuttamistoimenpiteistä. Sopimuksissa tulee määritellä tarkasti kaupungin

ohjeistukseen ja lainsäädäntöön perustuvat osapuolten roolit, vastuut ja velvollisuudet tietoturvan toteuttamiseksi.

3.1.6. Työntekijät ja muut tietojen käsittelijät

Jokainen Vantaan kaupungin omistamia tai hallinnoimia tietoja käsittelevä (esim. viranhaltija, työntekijä, luottamushenkilö sekä sopimus- ja yhteistyötahojen edustaja) on vastuussa tietoturvan toteutumisesta omissa tehtävissään.

Jokaisen on noudatettava Vantaan kaupungin

- tietoturvapoliittikkaa ja muuta tietoturvaohjeistusta
- tietoturva- ja salassapitositoumuksia

Jokaisen vastuulla on tietoturvaan liittyvien uhkien, riskien, havaintojen tai rikkomusten ilmoittaminen viipymättä ensisijaisesti esihenkilölleen.

3.2. Suojattavan omaisuuden omistajuus

Kaikella suojattavalla omaisuudella tulee olla omistaja. Yksilöitä ja muita tahoja, joilla on hyväksytty hallintavastuu suojattavan omaisuuden elinkaaresta, kutsutaan suojattavan omaisuuden omistajiksi. Tietoturvan näkökulmasta tärkeimmät suojattavat omaisuudet ovat tieto-omaisuus sekä järjestelmät ja laitteet, joissa tietoa käsitellään.

Suojattavan omaisuuden omistaja on vastuussa suojattavan omaisuuden asianmukaisesta hallinnasta koko sen elinkaaren ajan.

3.2.1. Tiedon omistajat

Tiedon omistaja on se, jonka toimintaan tiedot lähinnä liittyvät tai jonka toimintaa ne tukevat ja joka käyttää niihin kuuluvaa määräysvaltaa. Tieto voi olla sähköisessä, paperisessa tai muussa muodossa.

Tiedon omistaja

- määrää tiedon käytöstä ja siitä kenellä on tietoon pääsy
- vastaa tiedon luokittelusta ja asianmukaisesta suojaamisesta
- vastaa tiedon pääsynhallinnasta ja käyttöoikeuksien myöntämisestä
- vastaa tiedon käytön valvonnasta
- vastaa tietoon kohdistuvien riskien arvioinnista sekä lakisääteisistä velvollisuuksista kuten muutosvaikutusten arvioinnista ja henkilötietojen kohdalla tietosuojan vaikutustenarvioinnista
- vastaa tiedon elinkaaren lopussa sen asianmukaisesta poistamisesta, arkistoinnista tai tuhoamisesta

Tiedon omistajan vastuu säilyy, vaikka käytännön tehtävät delegoitaisiin muille tahoille.

3.2.2. Tietojärjestelmien ja tietoteknisten laitteiden omistajat

Kaikki tietojärjestelmät ja tietotekniset laitteet, joissa käsitellään kaupungin tietomaisuutta, tulee olla luetteloitu keskitettyyn omaisuusluetteloon ja niillä tulee olla omistaja. Tietojärjestelmien tai tietoteknisten laitteiden omistaja ei välttämättä ole sama kuin niissä käsitellyn tiedon omistaja.

Tietojärjestelmien ja tietoteknisten laitteiden omistaja vastaa niiden riskienhallinnasta ja tietoturvasta.

3.3. Tietoturvatyön organisointi

Hallintosäännön mukaan konsernipalvelut vastaa kaupunkitasoisen tietoturvan kehittämisestä ja hallinnasta, jotka konsernipalveluissa ovat tietohallintojohtajan vastuulla.

xx.xx.2026

3.3.1. Kaupunkitasoisen tietoturvan kehittäminen ja hallinta

Tietohallinto vastaa tietohallintojohtajan johdolla kaupunkitasoisen tietoturvan kehittämisestä, ohjeistamisesta, kouluttamisesta, hallinnasta, viestinnästä ja seurannasta.

Tietohallinnossa toimii tietoturvapäälikkö, jonka tehtäväalueeseen kuuluu edellisten lisäksi myös tietoturvarikkomusten hallinnointi, kaupunkia ohjaavan tietoturvasääntelyn seuranta ja säännöllinen raportointi tietoturvasta kaupungin johdolle sekä tarvittaessa kaupungin eri toimielimille.

3.3.2. Tietoturvakoulutus

Henkilöstön tietoturvatietoisuutta pidetään yllä säännöllisellä koulutuksella sekä ajantasaisilla ohjeilla ja tiedotuksella.

Kaupunkitasoiseen sekä toimialan, palvelualueen tai konserniyhteisön omaan tietoturvaohjeistukseen tutustuminen kuuluu työntekijöiden perehdytykseen.

3.3.3. Tietoturva- ja tietosuojatyöryhmä

Kaupungin tietoturva- ja tietosuojatyöryhmä on perustettu ja sen tehtävät määritetty kaupunginjohtajan päätöksellä. Työryhmän jäsenet toimivat yhteyshenkilöinä tietoturva- ja tietosuoja-asioissa työryhmän ja oman toimialansa tai palvelualueensa välillä.

3.3.4. Tietohallinto ja tietotekniset hankinnat

Hallintosäännön mukaan tietohallintojohtaja päättää IT-palvelujen, ohjelmistopalvelujen, tietojärjestelmien, IT- ja AV-laitteiden sekä niihin liittyvien palvelujen, puhelin- ja vaihdepalvelujen sekä puhelineläitteiden ja digitalisaation edistämiseen liittyvien IT-palvelujen hankinnoista. Tietohallinto ja hankintayksikkö vastaavat tietoteknisten hankintojen asianmukaisesta tietoturvan tasosta.

xx.xx.2026

Tietohallinto vastaa kaupungin tietoteknisen ympäristön tietoturvasta ja riskienhallinnasta.

3.3.5. Hankinnan palveluyksikkö ja muut kuin tietotekniset hankinnat

Hallintosäännön mukaan konsernipalveluiden palvelualue vastaa konsernipalvelujohtajan johdolla kaupungin hankintojen ohjauksesta ja ohjeistuksesta. Konsernipalveluissa sijaitseva hankinnan palveluyksikkö vastaa hankinnan kohteen tietoturvatavoitteiden ja -vaatimusten käsittelyn sisällyttämisestä osaksi hankintaprosessia.

Hankinnan palveluyksikkö vastaa siitä, että hankintaprosessissa toteutetaan hankinnan kohteeseen liittyvien tietoriskien arviointi ja niihin liittyvien suojaamisvaatimusten määrittely. Suojaamisvaatimusten määrittelyn sisältö tulee toteuttaa yhteistyössä substanssiasiantuntijoiden, hankinnan asiantuntijoiden ja tietohallinnon kanssa. Hankinnan palveluyksikkö vastaa siitä, että tietoriskien seuranta koskeva toimintamalli sisällytetään hankintasopimukseen, mutta seurannasta vastaa tiedon omistaja.

Toimialojen hankinnoista vastaavien tulee arvioitujen tietoriskien mukaisesti huomioida tietoturvatavoitteet ja -vaatimukset hankinnoissa, sopimuksissa sekä toimittajien hallinnassa.