



Haapajärven kaupunki

Haapajärvellä on hyvä  
ASUA - ELÄÄ - YRITTÄÄ - HARRASTAA



# TIETOTURVA- POLITIikka

Kaupunginhallitus 3.9.2013 § 216

# HAAPAJÄRVEN KAUPUNGIN TIETOTURVAPOLITIIKKA

1. JOHDANTO .....	3
2. KATTAVUUS .....	3
3. TIETOTURVA .....	3
4. TIETOTURVATYÖ.....	4
5. ORGANISOINTI JA VASTUUT .....	4
6. TIETOTURVAN TOTEUTUS .....	5
7. TIETOTURVAN SEURANTA JA VALVONTA.....	6

## 1. JOHDANTO

Tietojenkäsittely tukee Haapajärven kaupungin palvelujen tuottamista, ja palveluiden tehokkuus riippuu osaltaan tietojenkäsittelystä. Tietoaineistot sisältävät asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittely on oltava tehokasta, virheetöntä ja varmaa.

Tietoturvapoliittikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita kaupungin päävastuualueilla noudatetaan tietoturvan toteuttamisessa ja kehittämisessä. Tietoturvapoliittikkaa täydentävät tietoturvasuunnitelma sekä yksityiskohtaiset määräykset ja ohjeet, joita ovat mm. henkilökunnan tietoturvaohjeet.

## 2. KATTAVUUS

Kaupunginhallituksen vahvistama tietoturvapoliittikka kattaa päävastuualueiden kaikkien toimintaan liittyvät tietojen käsittelyn tehtävät.

Jokaisen Haapajärven kaupungin viranhaltijan, työntekijän ja luottamushenkilön sekä tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapoliittikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Myös ulkopuolisten toimijoiden, toimittajien ja muiden ulkopuolisten tahojen tulee sitoutua noudattamaan tätä tietoturvapoliittikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsulle kaupungin tietojärjestelmiin ja niiden tietoaineistoihin.

## 3. TIETOTURVA

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, saatavuudesta, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta.

Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Hyväksytyn tietoturvapoliittikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa kaupungin yleistä turvallisuustoimintaa, riskien

hallintaa ja sisäistä valvontaa.

## 4. TIETOTURVATYÖ

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvatyön päämäärä on turvata kaupungin toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

## 5. ORGANISOINTI JA VASTUUT

Tietoturvaa johtaa ja valvoo kaupunginhallitus. Kaupunginjohtaja päättää kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan ja tietosuojavastaavan.

**Tietoturvavastaavana** toimii talous- ja hallintojohtaja. Tietoturvavastaava vastaa kaupungin tietoturvatyön kokonaisuudesta johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Hän vastaa myös tietoturva-asioista tiedottamisesta toimintayksikön ulkopuolelle ja toimintayksikössä yleisellä tasolla.

**Tietosuojavastaavana** toimii hallintosihteeri. Tietosuojavastaava vastaa henkilökosten suojauksesta ja valvonnasta sekä muusta käyttöturvallisuudesta.

Kaupungin keskeisten toimintojen turvanäkemyksiä edustaa **tietoturvatyöryhmä**. Tietoturvatyöryhmän puheenjohtajana toimii tietoturvavastaava ja sihteerinä tietosuojavastaava. Tietoturvatyöryhmään kuuluvat jäseninä puheenjohtajan ja sihteerin lisäksi päävastuualueiden johtajat ja It-palvelujen edustajana ppsy Selänteen It-vastaava. Tietoturvatyöryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi.

Ryhmän jäsenten tehtävät ovat:

- Ryhmän jäsenet vastaavat oman vastuun alueensa tietoturvaprosessin asioiden valmistelusta
- Tietoturvavastaava vastaa kaupungin tietoturvasuostason määrittelystä ja arvioinnista ja raportoinnista sekä muusta hallinnollisesta tietoturvasta. Hän vastaa tietoturvan kehittämissuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvasuostasta

toimintatavasta toimintayksikössä ja sen ostamissa palveluissa sekä raportoinnista johdolle.

- It- vastaava vastaa laitteisto- ja ohjelmistoturvallisuudesta
- Tekninen johtaja vastaa tila- ja laiteteknisestä turvallisuudesta.
- Talous- ja hallintojohtaja vastaa henkilöstöturvallisuudesta
- Hallintosihteeri vastaa arkistotoimen tehtävien mukaisesta tietoaineistoturvallisuudesta

Jokaisella tietojärjestelmällä on **omistajayksikkö** ja **vastuuhenkilö**. Tietojärjestelmän vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely sekä käyttöoikeuksien myöntäminen ja valvonta.

Tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa **päävastuualueen johtaja**.

Jokainen vastuualueen työpaikan **työntekijä**, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen tai tietoturvavastaavalle.

## 6. TIETOTURVAN TOTEUTUS

Tietoturvan toteuttamisen perusta on tämä kaupunginhallituksen hyväksymä kirjallinen tietoturvapoliittikka, joka annetaan tiedoksi jokaiselle vastuualueen työpaikan työntekijälle ja tietojärjestelmien käyttäjälle.

Kaupungin tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaan, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin.

Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon kaupungin tietoturvan kehittämisessä.

Tietoturvan toteuttaminen ja ylläpito kuvataan yksityiskohtaisesti tietoturvasuunnitelmassa. Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuusluokka asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille. Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määrittäminen tapahtuu säännöllisesti

suoritettavilla turvallisuusanalyseillä.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla. Ne kuvataan tietoturvasuunnitelmassa ja tarvittaessa käyttöympäristöille ja yksiköille laadituissa erillisissä tietoturvan kehittämissuunnitelmissa. Keskeiset kehittämistoimet toteutetaan hankkeina, joista tehdään hankesuunnitelma.

Käyttäjien toimintaa ohjataan tietoturvasuunnitelmaan sisältyvillä käytösäennöillä sekä vahvistetuilla ja saatavilla olevilla toimintaohjeilla sekä tietoturvakoulutuksella. Jokainen käyttäjä allekirjoittaa käyttäjän tietosuojaohjeen ja sitoumuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

## **7. TIETOTURVAN SEURANTA JA VALVONTA**

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai tietoturvavastaavalle.

Vastuualueen työpaikan esimiehen tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään.

Tietoturvavastaavan tehtävänä on yleisesti seurata ja valvoa tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.