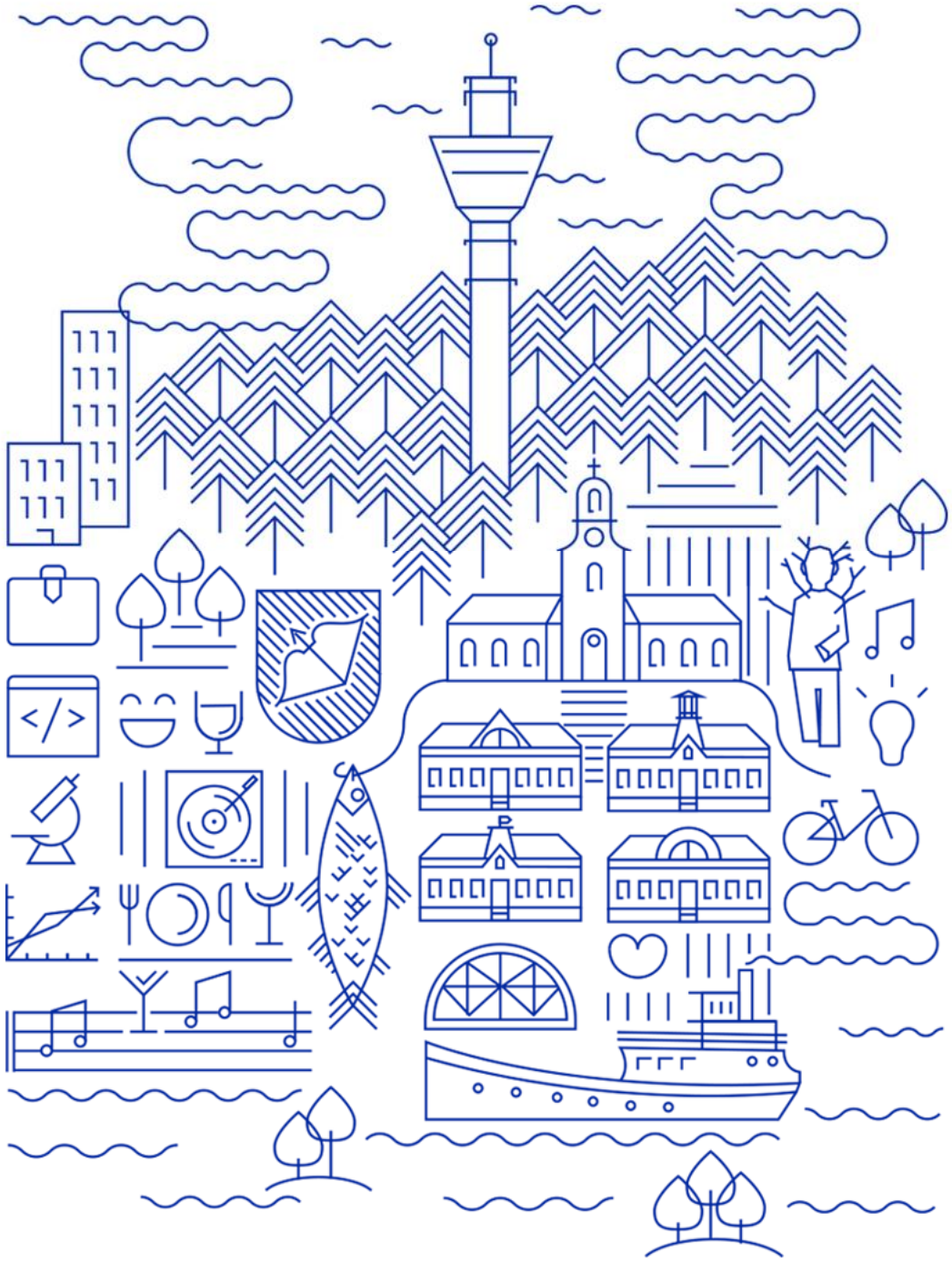
KUOPIO



Tietoturva- ja tietosuojapolitiikka

13.8.2018

Kuopion kaupunki
Elinvoima- ja konsernipalvelu
Tietohallinto

Dnro 3720/2018

13.8.2018

Laatimispäivä	13.08.2018	
Laatijat	Tietoturva- ja tietosuojaryhmä	
Versio	1.0	
Hyväksytty	Kaupunginjohtajan johtoryhmä	25.09.2018
	Kaupunginhallitus	19.11.2018

Sisällys

1 Johdanto

Tieto on keskeisessä roolissa Kuopion kaupungin toiminnassa ja palvelutuotannossa. Jotta tieto on tehokkaasti hyödynnettävissä, tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa.

Kuopion kaupungin johto määrittelee tässä politiikassa tietoturvallisuutta sekä tietosuojaa koskevat periaatteet ja linjaukset. Politiikka toimii perustana kaupungin tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa. Politiikka ohjaa ja on osa kaupungin tietoturvallisuuden hallintajärjestelmää.

Tämä politiikka koskee jokaista kaupungin työntekijää, viranhaltijaa, luottamushenkilöä ja yhteistyökumppania, joka työnsä tai toimeksiantonsa perusteella käsittelee Kuopion kaupungin omistamaa tai hallinnoimaa tietoa.

Tätä politiikkaa sovelletaan kaikkeen tietoon riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotiestä.

Tämä politiikka korvaa dokumentin Kuopion kaupunki, Tietoturvastrategia *25.9.2008 (A4750 / 014 / 2008).*

Tämän politiikan, velvoittavien säädösten ja kaupungin strategian lisäksi kaupungin tietoturva-ja tietosuojadokumentaatio koostuu erillisistä ohjedokumenteista, joista keskeisimmät ovat

- Loppukäyttäjän tietoturvaohje
- Internetin käyttösääntö
- Sähköpostisääntö
- Käyttövaltuuspolitiikka
- Poikkeamanhallintasääntö
- Tietoturvarikkomusten tulkinta- ja seuraamussäännöstö
- Riskienhallintapolitiikka

Tietoturva- ja tietosuojatoimintaa ohjaavat myös lait, joista keskeisimmät ovat

- Perustuslaki (731/1999)
- Kuntalaki (410/2015)
- Hallintolaki (434/2003)
- Arkistolaki (831/1994)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Henkilötietolaki (523/1999)
- Euroopan unionin yleinen tietosuoja-asetus (EU 679/2016)

- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- Rikoslaki (39/1889)
- Valmiuslaki (1552/2011)
- Tietoyhteiskuntakaari (917/2014)
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010, 5 §).

Muita keskeisiä toimintaa, soveltuvilta osin, ohjaavia dokumentteja ovat

- Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) ohjeet
- Kansallinen turvallisuusauditointi-kriteeristö (KATAKRI).

Termit

Tietoturva, tietoturvallisuus: Kaiken tiedon käytettävyyden, saatavuuden, oikeellisuuden ja luottamuksellisuuden turvaamista.

Tietosuoja: Henkilötietojen (eräs tiedon muoto) luottamuksellisuuden turvaaminen.

2 Tietoturvallisuus

Tieto kaikissa sen olomuodoissa, niin paperimuotoisena kuin tietoteknisenä, on keskeinen resurssi Kuopion toiminnassa. Tämän vuoksi tietoturvallisuus on keskeistä toiminnan kehittämisessä ja luottamuksen rakentamisessa.

Kuopion kaupungissa tietoturvallisuudella tarkoitetaan hallinnollisia, toiminnallisia, teknisiä ja muita keinoja, joilla suojataan kaupungin omistamaa tai hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa että poikkeusoloissa. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toimintaa suunnitellessa.

Toteutuakseen tietoturvallisuus vaatii seuraavien, painoarvoltaan tapauskohtaisesti vaihtelevien asioiden, toteutumista:

- Luottamuksellisuus: Tieto on vain tietoon oikeutettujen käytettävissä.
- Eheys: Tietoa ei ole muutettu tahallisesti tai tahattomasti, eikä tieto ole muuttunut teknisen häiriön seurauksena.
- 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 jälkikäteen.

Periaatteena on, että tieto on ensi sijassa julkista ja avointa jolloin tiedon eheys- ja saatavuusvaatimukset korostuvat. Kaupunki käsittelee myös salassa pidettäviä tietoja, jotka määritetään julkisuuslaissa ja eri hallinnonalojen erityissäädöksissä.

Tietoturvallisuus Kuopion kaupungissa sisältää tiedon suojaamisen lisäksi tietosuojaan, tekniseen tietoturvaan ja muihin turvallisuuden osa-alueisiin liittyviä toteutuksia, joista kaupungin kannalta keskeisimpiä ovat

- sisäänrakennettu ja oletusarvoinen tietosuoja henkilötietojen käsittelyssä, jolla varmistetaan henkilön yksityisyyden suojan ja muiden sitä turvaavien oikeuksien toteutuminen henkilötietoja käsiteltäessä.
- toimenpiteet, joilla turvataan teknisen toimintaympäristön luottamuksellisuus, eheys, saatavuus ja jatkuvuus.
- tietoturvallisuuteen vaikuttavat toimenpiteet, joita suoritetaan henkilöstöprosessissa ennen palvelussuhdetta, sen aikana ja sen päättymisen yhteydessä.
- sopimustekniset toimenpiteet, joilla varmistetaan tässä politiikassa kuvattujen periaatteiden toteutuminen myös sidosryhmien kanssa tehtävässä yhteistyössä.

3 Tietosuoja

Tietosuojalla tarkoitetaan Kuopion kaupungin asiakkaiden, henkilöstön ja sidosryhmien yksityisyyden suojaamista henkilötietojen käsittelyssä.

Kuopion kaupunki käsittelee henkilötietoja sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden mukaisesti.

Kuopion kaupunki

1 Ylläpitää selkeää kokonaiskuvaa hallussaan olevista henkilötiedoista ja niiden käsittelyyn sisältyvistä riskeistä.

2 Kerää ainoastaan ennalta määriteltyjen käyttötarkoitusten kannalta tarpeellisia henkilötietoja kaupungin tehtävien suorittamiseksi ja palveluiden kehittämiseksi.

3 Huolehtii suunnitelmallisesti ja läpinäkyvästi henkilötietojen elinkaaren hallinnasta ja suojaamisesta.

4 Varmistaa säännöllisten koulutusten avulla, että henkilöstöllämme on riittävä tietosuojaosaaminen tehtävänkuvasta riippuen.

5 Mahdollistaa asiakkailleen kontrollin ja tiedonsaannin omiin henkilötietoihinsa.

6 Arvioi jatkuvasti henkilötietojen käsittelyyn liittyviä riskejä yksilöiden oikeuksille ja vapauksille.

7 Varmistaa, että kaupungin sopimuskumppanit noudattavat lainsäädännön mukaisia tietosuojaperiaatteita.

4 Tietoriskien hallinta

Riskienhallintaa toteutetaan Kuopion kaupungin riskienhallintapolitiikan mukaisesti. Periaatteena on, että riskienhallintaprosessia käytetään säännöllisesti toteutettavaan sisäisten ja ulkoisten tietoon kohdistuvien ja tiedosta aiheutuvien riskien hallintaan.

Tietoriskien turvaamisen lähtökohtana on riskiperusteinen lähestymistapa. Tällöin pienen riskin tietojen käsittelyyn ei kohdisteta ylimitoitettuja toimenpiteitä, ja toisin päin. Riskipohjaisen lähestymisen avulla tietoturvaan ja tietosuojaan liittyvät velvoitteet ja suojaustoimet määritellään Kuopion kaupungilla aina kyseisen tiedon käsittelyyn liittyvien ja havaittujen riskien pohjalta.

5 Poikkeamanhallinta

Tietoturva- ja tietosuojapoikkeamien hallintaa ohjaa kaupungin Tietoturvapoikkeamien käsittelysääntö.

6 Varautuminen

Kuopion kaupunki varautuu turvaamaan tiedonhallintaan liittyvien kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

7 Vaatimustenmukaisuus ja tavoitteet

Kuopion kaupunkia velvoittavien säädösten lisäksi kaupungin tietoturvallisuudelle sekä tietosuojalle voidaan asettaa vaatimuksia ja tavoitteita mm. kaupungin strategiassa.

Kaupungin tietoturvallisuuden tavoitteena on rakentaa ja varmistaa kaupungin toimintaympäristö siten, että häiriön (kuten inhimillinen erehdys, tekninen vika tai tahallinen haitanteko) vaikutukset saadaan rajoitettua ja toiminnot palautettua mahdollisimman nopeasti normaalitilanteeseen. Näin varmistetaan kuntalaisille tarjottavien palveluiden ja kaupungin sisäisten toimintojen korkea laatu. Lisäksi tavoitteena on kaupungin tietoturva- sekä tietosuojakäytäntöjen yhdenmukaistaminen.

Tietosuojan tavoitteena on huolehtia henkilötietojen oikeaoppisesta ja lainsäädännön mukaisesta käsittelystä, jolloin tiedot on suojattu luvattomalta käsittelyltä. Näin henkilöiden yksityisyys kyetään turvaamaan. Tietosuojalla pyritään myös parantamaan luottamusta verkkopalveluihin sekä hyödyntämään digitalisaation tarjoamia mahdollisuuksia Kuopion kaupungin toiminnassa.

Tietoturvatavoitteet saavutetaan vain, jos kaikki noudattavat yhteisesti sovittuja periaatteita.

8 Organisointi, roolit ja vastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kaupungin sääntöjen mukaisesti.

Kaupunginhallitus seuraa tietoturvallisuuden sekä tietosuojan toteutumista kaupungissa. Kaupunginhallitus hyväksyy tietoturva- ja tietosuojapolitiikan ja siihen ehdotetut muutokset. Kaupunginhallituksella on vastuu kaupungin sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Luottamushenkilöt ovat vastuussa tietoturvasta kaikilta niiltä osin kuin tietoturva suoraan tai välillisesti liittyy luottamushenkilöiden toimintaan tai heidän edustamiinsa ympäristöihin.

Kaupunginjohtajalla on kokonaisvastuu tietoturvallisuuden sekä tietosuojan toteuttamisesta ja näiden toteutumisen raportoinnista kaupunginhallitukselle. Kaupunginjohtaja omistaa tietoturva- ja tietosuojapolitiikan ja esittelee muutokset kaupunginhallitukselle. Kaupunginjohtaja hyväksyy kaupunkitasoiset ohjeet ja linjaukset. Kaupunginjohtajan tukena tietoturvallisuus- ja tietosuoja -asioissa on kaupunginjohtajan johtoryhmä ja tietoturva- ja tietosuojaryhmä.

Apulaiskaupunginjohtajat vastaavat palvelualueidensa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Liikelaitosten, tytäryhtiöiden ja -säätiöiden hallitukset ja toimitusjohtajat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta omissa organisaatioissaan.

Esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan. Esimiehen keskeisimmät tehtävät ovat huolehtia

1 oman organisaationsa perehdyttämisestä kaupungin tietoturva- ja tietosuojaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin.
2 työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin
   – kaupungin tiedon ja muun omaisuuden palauttamisesta
   – ilmoittamisesta Kuopion kaupungin ICT-palveluntuottajille työntekijän käyttöoikeuksien ja -valtuuksien poistamiseksi.

Henkilöstö vastaa omalta osaltaan ohjeiden noudattamisesta. Jokaisen vastuulla on lisäksi tietoturvallisuuteen ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi tietoturvapäällikölle, tietosuojavastaavalle tai omalle esimiehelleen. Jokaisella on vastuu omaan tehtäväänsä liittyvän tietoturvan ja tietosuojan toteuttamisesta.

Tiedon omistaja vastaa tiedon elinkaaren hallinnasta, luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

Tietojärjestelmän omistaja vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy henkilön esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.

Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Tietoturvapäällikkö edistää tietoturvallisuuden toteutumista kaupungissa. Hän vastaa tietoturva- ja tietosuojaryhmän toiminnasta, tietoturvallisuuden hallinta-

järjestelmän toimivuudesta sekä tietoturvapolitiikan ja kaupunkitasoisen tietoturvadokumentaation valmistelusta ja kehittämisestä. Tietoturvapäällikkö raportoi tietoturvallisuuden toteutumisesta kaupungin johdolle sekä vastaa tietoturvallisuuteen liittyvästä viestinnästä yhdessä kaupungin viestintäyksikön kanssa.

Tietosuojavastaava toimii kaupunkiorganisaation tukena ja antaa neuvoja ja ohjausta tietosuojan toteuttamisesta. Tietosuojavastaava seuraa kaupungin tietojenkäsittelyyn liittyviä toimintatapoja ja tukee toimijoita tietosuojalainsäädännön vaatimuksien täyttämisessä. Tietosuojavastaava toimii kaupungin yhteyshenkilönä sekä valvontaviranomaisiin että rekisteröityihin. Tietosuojavastaava raportoi tietosuojan toteutumisesta kaupunginjohtajalle ja sekä vastaa tietosuojaan liittyvästä viestinnästä yhdessä viestintäyksikön kanssa. Tietosuojavastaava ei vastaa kaupungin henkilötietojen käsittelyn lainmukaisuudesta, vaan siitä on vastuussa kaupungin johto.

Tietoturva- ja tietosuojaryhmä kehittää tietoturvan ja tietosuojan toteutumista ja seuraa tietoturvallisuuden yleistä kehittymistä kaupungissa ja tekee siihen perustuen kehitysehdotuksia kaupungin tietoturvallisuuden parantamiseksi. Ryhmä seuraa ja analysoi toimintaympäristön ja lainsäädännön muutoksia sekä arvioi kokonaisvaltaisesti tietoturva – ja tietosuojariskejä.

Ryhmä toimii asiantuntijana tietoturvaa koskevissa asioissa, valmistelee kaupungin johdolle esitykset yhteisistä tietoturva- ja tietosuojaohjeista, linjauksista ja ratkaisuista sekä tietoturvallisuuden hallintajärjestelmän kokonaiskehittämisestä.

Ryhmä organisoi kaupungin henkilöstön tietoturva- ja tietosuojakoulutuksia, toimii koko kaupunkiorganisaation tukena tietoturva- ja tietosuoja-asioissa ja raportoi toiminnastaan osana tietotilinpäätöstä.

Tietoturvan – ja tietosuojan yhteyshenkilöt palvelualueilla huolehtivat vastuualueillaan tietoturvan ja tietosuojan seurannasta ja raportoivat yksikön tietoturvaan liittyvistä huomioista ja toimenpiteistä tietoturvaryhmälle.

Ict -palveluntuottajat vastaavat teknisestä tietoturvallisuudesta, tietohallinnon tekemien linjausten ja ohjeiden mukaisesti. Ict-palveluntuottajat seuraavat ja informoivat vastuualueensa tietoturvallisuuden toteutumisesta sopimusten mukaisesti.

Asiakirjahallinto vastaa asiakirjatiedon hallinnasta ja siihen liittyvästä ohjeistuksesta.

Sisäinen tarkastus vastaa tietoturvallisuuden asianmukaisuuden ja riittävyyden arvioinnista sekä tarkastamisesta.

9 Tiedon ja tietojärjestelmien käyttö

Kaupungin tietojärjestelmäympäristössä käytetään kaupungin tietohallinnon hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Tietoturvallinen toimintatapa on kuvattu *Loppukäyttäjän tietoturvaohjeessa* ja muissa tietoturva-ohjeissa.

Käyttöoikeudet kaupungin omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeuksien hallintaa ohjaa *Kaupungin käyttövaltuuspolitiikka.*

Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi Kuopion kaupungin *Tietoturvarikkomusten käsittely, tulkinta ja seuraamuskäytännöt*- ohjetta.

Tietoturva- ja tietosuojapoikkeamien ja väärinkäytösten selvittämiseksi sekä nykytilan ja käytön valvomiseksi kaupungin tietoturvapäällikölle, teknologiapäällikölle sekä tietosuojavastaavalle mahdollistetaan pääsy tehtävän edellyttämään tietoon ja tietojärjestelmiin.

10 Tietoturvatietoisuus ja -osaaminen

Esimies huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin sekä työntekijän omissa työtehtävissä tarvittavaan erityisosaamiseen.

Tietoturvallisuuden ja tietosuojan perus- ja jatkokoulutusta on tarjolla säännöllisesti. Tietoturva- ja tietosuojatietoisuutta ylläpidetään

1 työntekijän perehdytykseen sisältyvällä koulutuksella,

2 roolipohjaisilla lisäkoulutuksilla ja

3 säännöllisillä kertauskoulutuksilla.

Kaupungin tietoturvadokumentaatio kokonaisuudessaan on henkilöstön saatavilla kaupungin sisäisissä informaatiokanavissa työtehtävien edellyttämässä laajuudessa.

11 Tietoturvallisuuden toteuttaminen, seuranta, ylläpito ja kehittäminen

Kuopion kaupungin tietoturvallisuustyö perustuu toiminnan, teknologian ja osaamisen jatkuvaan kehittämiseen tietoturvan hallinnan prosessin kuvauksen mukaisesti noudattaen jatkuvan kehittämisen periaatteita.

Tietoturvallisuutta toteutetaan tietoturvallisuuden parantamiseen tähtäävillä johtamis- ja muilla käytännöillä. Keskeistä toteuttamisessa on, että kaupungilla on riittävät keinot ja käytännöt aktiivisesti

- johtaa tietoturvallisuutta
- seurata ja arvioida toimintaympäristön tilaa
- havaita ja tunnistaa uhkat
- varautua poikkeamiin ja häiriöihin ennakolta sekä reagoida tilanteen edellyttämällä tavalla.