PIEKSÄMÄEN KAUPUNGIN TIETOTURVAPOLITIIKKA

2016

Kh 111§ 31.5.2016

v1.0
19.5.2016, Seija Romo

Dokumentin tila

Versio	Päiväys	Laatija	Muutoksen kuvaus	Muokkauksen vahvistanut

1. Johdanto

Tietoturvapolitiikka on kaupungin ylimmän johdon hyväksymä strateginen asiakirja, joka on kannanotto tietoturvan kehittämiseen. Tietoturvapolitiikan tavoitteena on luoda Pieksämäen kaupungin konserniohjeen mukaisesti yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietoturvatason toteuttamiseksi. Tietoturvapolitiikassa määritellään kaupungin tietoturvatyön visio, tavoitteet, vastuut, organisointi ja toteutuskeinot. Politiikan toteuttamisella luodaan edellytykset tietoturvallisen toiminnan pitkäjänteiseen kehittämiseen. Työssä onnistuminen edellyttää kaupungin johdon sitoutumista tietoturvatyön tukemiseen.

2. Tietoturvapolitiikan tavoite

Tietoturvallisuuden käsite ja merkitys

Tiedon turvaaminen on merkittävä osa kaupungin toiminnan ja sen järjestämien palvelujen laatua, ICT-riskienhallintaa ja kokonaisturvallisuutta. Riskienhallinnan keskeisenä tavoitteena on tunnistaa toimintaan kohdentuvat riskitekijät, arvioida niitä ja ryhtyä tarvittaviin toimenpiteisiin. Tietoturvan hyvä hallinta edellyttää toiminnan pitkäjänteistä suunnittelua, jatkuvaa kehittämistä, seurantaa ja erilaisiin uhkatilanteisiin varautumista. Tietoturvan toteuttaminen vaatii koko henkilöstön tietoturvatietoisuuden parantamista, sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja monikanavaista viestintää.

Määritelmät

Tieto eri muodoissaan on tärkeä perusta kaikelle kaupungin toiminnalle. Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen (mm. sähköisesti tallennettu, välitetty tai rekisteröity tieto, suullinen puhuttu, postin kuljettama tai paperilla oleva tieto) suojaamista erilaisilta uhkatekijöiltä varmistaen palvelutoiminnan jatkuvuus minimoiden toimintaan tai asiakkaiden tietoihin liittyvät riskitekijät. Tietosuoja on myös osa tietoturvaa ja se tarkoittaa ihmisten yksityisyyden kunnioittamista ja suojelemista oikeudellisia säännöksiä noudattavien periaattein ja käytännöin.

Tietoturva määritellään kolmen peruskäsitteen kautta seuraavasti:

1) Tietojen luottamuksellisuus: tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeudet.
2) Tietojen eheys: tiedon oikeellisuus ja suojaus on järjestetty niin, että tietoa ei voi tahallisesti tai tahattomasti muuttaa vaarantaen toiminnan luotettavuutta.
3) Palveluiden ja tietojen saatavuus: tieto on saatavissa ja käytettävissä silloin, kun sitä palvelutoiminnassa tarvitaan.

Hyvä tietoturvataso saavutetaan tietoturvapolitiikan ja ohjeiden mukaisilla tietoturvallisilla toimintaperiaatteilla ja erilaisilla turvamekanismeilla, joita hallitaan ja katselmoidaan jatkuvan kehittämisen periaatteita noudattaen.

3. Tietoturvatoimintaa ohjaavat tekijät

Organisaation tietoturvallisuutta velvoittavat ja ohjaavat kansalliset ja kansainväliset yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lisäksi muut tietoturvallisuutta ohjaavat velvoitteet, määräykset ja ohjeet.

Jokaisen Pieksämäen kaupunkikonsernin viranhaltijan, työntekijän ja luottamushenkilön sekä muun kaupunkikonsernin tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä.

4. Tietoriskien hallinta

Tietohallinnossa käydään vuosittain tietohallinto- ja ict-riskien ja uhkien kartoitus. Saadun tuloksen perusteella suurimpien riskien vaikutuksia pyritään vuoden aikana pienentämään tai ehkäisemään. Seuraavassa riskienkartoituksessa tarkistetaan, miten näihin riskeihin on pystytty vaikuttamaan. Tuloksista raportoidaan hallintojohtajalle. Tietoriskien hallinta on jatkuvaa aktiivista toimintaa.

5. Tietoturvallisuuden merkitys organisaatiolle

Tietoturvatyön tavoitteena on turvata tietojärjestelmien, tietoverkkojen ja tietojenkäsittelylaitteiden keskeytymätön toiminta, havaita ja estää tietojen luvaton käyttö, tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen ja minimoida niistä aiheutuvat vahingot. Keskeinen tavoite on suojata elintärkeät toiminnot kaikissa häiriötilanteissa varmistaen palveluiden käytettävyys mahdollisimman lyhyellä toipumisajalla.

Toiminnan kannalta kriittiset palvelut on kartoitettu ja arvioitu keskeytysten vaikutukset toimintaan. Tietohallinnon varautumissuunnitelmassa käsitellään nämä asiat tarkemmin.

6. Turvatoimien priorisointi

Turvatoimien priorisoinnissa nojaudutaan samaan priorisointiin kun palvelupyyntöjä koskevassa priorisoinnissa. Korkeimmalle prioriteetille asetetaan toiminnoista terveydenhuolto, palkkojen maksu, maksuliikenne ja laskutukset sekä teknisesti suuria käyttäjämääriä koskevat verkon työt kuten palvelimiin ja kytkimiin liittyvät toimenpiteet.

7. Tietoturvavastuut

Jokaisella tietojärjestelmällä tulee olla yksilöity omistaja, joka vastaa koko järjestelmän elinkaaren hallinnasta, tietosuojasta ja tietoturvan toteuttamisesta. Järjestelmän omistajuuteen liittyvät tiedot dokumentoidaan keskitetysti rekisteri- ja tietojärjestelmäselosteisiin sekä tietohallinnon ylläpitämään tietojärjestelmäluetteloon. Tietojärjestelmän omistajan on huolehdittava tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsynvalvonnasta sekä tuottamaan lakisääteiset seurantaraportit.

Jokaiselle tietojärjestelmälle on nimettävä pääkäyttäjä, jonka vastuulla on huolehtia järjestelmän käyttöoikeuksista. Pääkäyttäjältä vaaditaan hyvää tietoturva- ja tietosuojaosaamista. Lisäksi tiedon omistajien ja pääkäyttäjien on huolehdittava tiedon koko elinkaaren hallinnasta ja ICT-varautumissuunnitelmista, missä kuvataan vastuuhenkilöt, roolit ja toimintamallit riskien toteutumisen varalta. Tietohallinnon vastuulla on järjestää tukitoimintoja ja tarvittavia koulutuksia edellisten toteuttamiseksi.

Esimiesten vastuulla on huolehtia ja noudattaa työnantajaa koskevien lakisääteistein tietoturva ja tietosuoja velvoitteiden toteutumista. Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa. He huolehtivat loppukäyttäjän riittävästä perehdytyksestä konsernin tietoturvakäytänteisiin varmistaen, että jokainen ymmärtää niiden merkityksen työtehtävissään. Esimiesten ja pääkäyttäjien vastuulla on myös huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa ja työsuhteen päättyessä työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden sekä käyttöoikeudet tietojärjestelmistä poistetaan. Esimiehiltä odotetaan esimerkillistä sekä vastuullista tietoturvakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvapoikkeamista tietohallinnon vastuuhenkilölle.

Kaupungin työntekijän velvollisuus on allekirjoittaa tietoturva- ja käyttäjäsitoumus sekä suorittaa hyväksytysti kulloinkin voimassa oleva tietoturva- tai tietosuojakoulutus säännöllisin väliajoin. Työntekijällä on vastuu noudattaa hyväksyttyjä tietoturvaohjeita ja huolehtia päivittäisissä työtehtävissä hyvän tiedonhallintatavan käytänteistä. Työntekijän vastuulla on myös huolehtia käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokittelusta sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä. Tietojen säilytys- tai arkistointiajan päätyttyä ne on hävitettävä ohjeiden mukaisesti. Työntekijällä on velvollisuus raportoida tietoturvaongelmista oman organisaation tietoturvavastaavalle tai suoraan tietohallinnon vastuuhenkilölle.

Ostopalveluna hankitun ICT–palvelun operatiivisesta ja teknisestä tietoturvasta ja sen ohjeistamisesta vastaavat palveluntuottajat, joille palvelun toteutus on sopimuspohjaisesti luovutettu. ICT-palveluiden tuottajien tehtävänä on laatia ja ylläpitää keskitetysti tietohallinnon hyväksymien palvelukonseptien mukaisia käytännön tietoturvaohjeita.

Tilaajan tulee huolehtia, että kaikkiin tarjouspyyntöihin ja palvelusopimuksiin sisällytetään tietohallinnon ylläpitämät yleiset tietoturvavaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla sekä häiriötilanteiden toimintamallit ja selkeä vastuunjako läpi koko palveluketjun. Tilaajan tehtävä on huolehtia ja vaatia palvelutuottajaa raportoimaan ja tiedottamaan merkittävistä tietoturvaan kohdistuvista poikkeustilanteista, riskitekijöistä sekä uhkatilanteista välittömästi palvelusopimuksessa määritellyille yhteyshenkilöille.

8. Tietoturvakoulutus ja -ohjeet

Omatoiminen toimialakohtainen tietoturvakoulutus ja -testi tapahtuvat extranetissä henkilökohtaisilla tunnuksilla. Esimiehet seuraavat alaistensa kouluttautumista ja testien suorittamista. Testi on uusittava kerran vuodessa.

Tietoturvallisuuteen liittyvät oppaat, säännöt ja materiaalit ovat työntekijöiden luettavissa sisäverkossa.

Hyvällä perehdyttämisellä luodaan työviihtyvyyttä ja -turvallisuutta. Uuden henkilön perehdyttämisestä huolehtii lähin esimies. Perehdytystä varten on intranetissä esimerkkikaavake, jonka kukin toimialue voi muokata vastaamaan omia tarpeitaan.

9. Tietoturvallisuudesta tiedottaminen ja sen toteutumisen valvonta

Ennalta tiedetyistä palvelukatkoksista tiedotetaan tietohallinnon Tiedotussuunnitelman mukaisesti.

Häiriötilanteen tiedottaminen, tapahtumaraportti (selvitys tapahtumasta ja miten vastaava voidaan estää) ja sen jakelu, häiriöiden tiedottaminen jälkikäteen atk-ryhmille tiedotetaan Tiedotussuunnitelman mukaisesti.

Havaitusta väärinkäytöksestä tai pistokokeena havaitusta väärinkäytöksestä raportoidaan ja tiedotetaan lähintä esimiestä. Väärinkäytökset on sanktioitu, ja tieto niistä on osa tietoturvakäsikirjan liitteitä.

Muusta perussyystä johtuvasta häiriötilanteesta tiedottamisessa noudatetaan kaupungin yleistä tiedottamisohjetta.

10. Toiminta normaaliolojen häiriötilanteissa, poikkeustilanteissa ja -oloissa

Normaaliolojen häiriötilanteita pyritään ennaltaehkäisemään ja toipumisaikoja lyhentämään pitämällä järjestelmien ja laitteiden mahdollisimman ajantasaisina. Tietohallinto päivittää vuosittain jatkuvuus- ja toipumissuunnitelmansa.

Poikkeustilanteessa varautumista johtaa ja valvoo valtioneuvosto sekä kukin ministeriö toimialallaan (1552/2011) 13 §). Tietohallinnon osalta poikkeusolojen valmiussuunnitelmaa pidetään yllä ja se on viimeksi päivitetty 2015.

TIETOTURVAAN LIITTYVÄÄ LAINSÄÄDÄNTÖÄ JA OHJEITA

Arkistolaki (831/1994)

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)

Hallintolaki (434/2003)

Henkilötietolaki (523/1999)

Julkisuus ja tietosuoja opetustoimessa (opas koulujen ja oppilaitosten käyttöön 2013:7)

Kuntalaki (410/2015)

Laki julkisista hankinnoista (348/2007, laki on uudistumassa 2016)

Laki kansainvälisistä tietoturvavelvoitteista (588/2004)

Laki kunnallisesta viranhaltijasta (304/2003)

Laki potilaan asemasta ja oikeuksista (785/1992)

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)

Laki sosiaali- ja terveydenhuollon palvelusetelistä (569/2009)

Laki sähköisistä allekirjoituksista (14/2003)

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)

Laki sähköisestä lääkemääräyksestä (61/2007)

Laki terveydenhuollon ammattihenkilöstä (559/1994)

Laki toimeentulotuesta (1997/1412)

Laki yksityisyyden suojasta työelämässä (759/2004)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)

Laki viranomaisen toiminnan julkisuudesta (621/1999)

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009)

Lukiolaki (629/1998)

Perustuslaki (731/1999)

Perusopetuslaki (628/1998)

Rikoslaki (39/1889)

Sosiaalihuoltolaki (1301/2014)

Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (298/2009)

Sähköisen viestinnän tietosuojalaki (516/2004)

Tekijänoikeuslaki (4040/1961)

Terveydenhuoltolaki (1326/2010)

Tietosuovaltuutetun toimiston ohjeet ja kannanotot

Työsopimuslaki (55/2001)

Vahti-ohjeet

Valmiuslaki (1080/1991)

Viestintämarkkinalaki (393/2003)