KUUSAMO
KUUSAMON KAUPUNKI

LIITE NO 2
KHALL./KVALT. 18/6 2018
§ 140

TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Tämä tietoturva- ja tietosuojapolitiikka kumoaa 8.12.2008 hyväksytyn tietoturvapolitiikan (khall 8.12.2008 §218)

Hyväksytty kaupunginhallituksessa 18.6.2018 § 140

Voimassa 1.7.2018 alkaen

KUUSAMO
KUUSAMON KAUPUNKI

1. JOHDANTO

Tietojen turvaaminen ja hyödyntäminen on oleellinen osa Kuusamon kaupungin toiminnan ja sen järjestämien palvelujen laatua. Tietoturvan ja tietosuojan hyvä hallinta edellyttää toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja resursointia erilaisten uhkatekijöiden ja -tilanteiden varalta. Tietoturvan ja tietosuojan toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja viestintää.

Tietoturva- ja tietosuojapolitiikka on kaupungin johdon kannanotto tietoturvan ja tietosuojan toteuttamiseen Kuusamon kaupungissa. Tietoturva- ja tietosuojapolitiikka määrittelee Kuusamon kaupungin tietoturvan ja tietosuojan tavoitteet, vastuut sekä tietoturva- ja tietosuojatyön organisoinnin ja toteutuskeinot. Tietoturva- ja tietosuojapolitiikkaa täydentävät erikseen laaditut tarkemmat tietoturva- ja tietosuojaohjeet.

Tietoturvallisuuden ja tietosuojan ensisijaisena päämääränä on kaupungin toiminnan ja palveluiden luotettavuuden ja jatkuvuuden turvaaminen toiminnan tietojenkäsittelylle asetettujen vaatimusten mukaisesti.

Tämä politiikka koskee kaikkia Kuusamon kaupungin työntekijöitä ja soveltuvin osin toimittajia ja muita sidosryhmiä.

2. TIETOTURVALLISUUDEN JA TIETOSUOJAN MERKITYS KUUSAMON KAUPUNGIN TOIMINNALLE

Tietojen kasvava määrä ja nopea digitalisoituminen edellyttää tiedon hyvää hallintaa ja turvallista käsittelyä, mikä on tärkeä perusta Kuusamon kaupungin toiminnalle. Tietoturvallisuus- ja tietosuojatoimenpiteillä varmistetaan toiminnan jatkuvuutta uhkaavien riskien hallinta, palvelutoiminnan jatkuvuus ja kehittyminen sekä minimoidaan toimintaan tai asiakkaiden tietoihin liittyvät riskitekijät.

Tietosuoja on osa tietoturvaa ja sillä turvataan ihmisten yksityisyyden kunnioittaminen ja suojeleminen. Tietosuojatyö pitää sisällään velvoittavien tietosuojasäädösten mukaisia toimenpiteitä, joilla varmistetaan henkilön yksityisyyden suojan ja muiden sitä turvaavien oikeuksien toteutuminen Kuusamon kaupungissa ja kaupungin järjestämissä palveluissa henkilötietoja käsiteltäessä. Tietosuojatoimenpiteillä varmistetaan asetuksen edellyttämien rekisterinpitäjän osoitusvelvollisuuden ja rekisteröidyn oikeuksien toteutuminen.

3. TIETOTURVAN JA TIETOSUOJAN TAVOITTEET

Kuusamon kaupungin tietoturva- ja tietosuojatyön tavoitteena on turvata toimintaa tukevien tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta ja tietosuojan täyttyminen. Tavoitteena on myös havaita ja estää tietojen ja tietojärjestelmien luvaton käyttö, tahaton tai tahallinen tiedon tuhoaminen ja vääristäminen sekä minimoida niistä mahdollisesti aiheutuvat vahingot.

Tietoturva- ja tietosuojatyön tulee mukautua tilanteen, palvelun, standardien ja lakien edellyttämiin vaatimuksiin. Lähtökohtana on, että kaupungin tiedot ja tietojärjes-

telmät suojataan asianmukaisesti sekä normaali- että poikkeusoloissa hallinnollisin ja teknisin toimenpitein. Toimintaympäristön riskeihin varaudutaan varustamalla työ- ja laitetilat tarvittavin kulunvalvonta- ja suojausratkaisuin sekä huolellisella henkilötietojen käsittelyn suunnittelulla.

Tietoturva- ja tietosuojatyön tavoitteena on sisällyttää hyväksytyn tietoturva- ja tietosuojapolitiikan ja sitä täydentävien ohjeiden mukainen tietoturva ja tietosuoja luonnollisena osana kaupungin kaikkeen toimintaan. Tämä tarkoittaa henkilökunnan, yhteistyökumppaneiden ja alihankkijoiden sitouttamista noudattamaan kaupungin tietoturva- ja tietosuojakäytäntöjä ja vastuuta huolehtia tietojen tietoturvasta ja tietosuojasta. Tietoturva- ja tietosuojatyön tavoitteena on ylläpitää kuntalaisten ja eri sidosryhmien luottamusta kaupungin tarjoamiin perinteisiin ja sähköisiin palveluihin sekä niiden tietoturvan, tietosuojan ja yksityisyydensuojan toteutumiseen.

4. TIETOTURVALLISUUDEN JA TIETOSUOJAN HALLINTAJÄRJESTELMÄ

Kuusamon kaupungin tietoturvallisuuden ja tietosuojan hallintajärjestelmä koostuu tästä tietoturva- ja tietosuojapolitiikasta ja sitä täydentävistä tarkemmista ohjeista ja menetelmistä. Henkilöstön ajantasainen tietoturva- ja tietosuojaosaaminen varmistetaan kaikki henkilöryhmät kattavalla tietoturva- ja tietosuojakoulutuksella. Kuusamon kaupungin tuottamien palveluiden osalta varmistetaan riittävät tietoturva- ja tietosuojatasot ja niiden lakien, asetusten ja määräystenmukaisuus.

5. TIETOTURVA- JA TIETOSUOJAVASTUUT

Kokonaisvastuu tietoturvallisuuden ja tietosuojan toteuttamisesta on kaupunginhallituksella ja kaupunginjohtajalla. Kaupungin johdon vastuulla on huolehtia tietoturva- ja tietosuojatyön riittävästä resursoinnista. Tietohallintojohtajalla tai kaupunginjohtajan nimeämällä toimialajohtajalla on vastuu koko kaupungin teknisen ja hallinnollisen tietoturvan ja tietosuojan järjestämisestä, kehittämisestä ja seurannasta. Kaupungin tietosuojavastaava vastaa tietosuojan toteutumisesta ja seurannasta voimassa olevan tehtäväkuvauksen mukaisesti.

Toimialat, liikelaitokset ja tytäryhtiöt vastaavat tietoturvan ja tietosuojan toteutumisesta omassa toiminnassaan ja ostopalveluissa. Toimialojen, liikelaitosten ja tytäryhtiöiden johdon ja nimettyjen tietoturva- ja tietosuojavastaavien tulee huomioida toiminnan erikoispiirteet ja lainsäädäntö sekä selventää tietoturva- ja tietosuojavastuut omissa yksiköissään.

Tietojärjestelmien ja tietovarantojen omistajat vastaavat omistamiensa järjestelmien toiminnasta ja tietoturvan ja tietosuojan kehittämisestä ja toteutumisesta. Jokaiselle tietojärjestelmälle määritellään omistaja ja järjestelmästä laaditaan tarvittavat dokumentit ja ohjeet. Omistajien tehtävänä on mm. kartoittaa omistamiinsa tietojärjestelmiin ja henkilötietojen käsittelyyn liittyvät riskit ja suojaamiskeinot, huolehtia tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta, pääsynvalvonnasta, toimitilojen suojaamisesta, toimintojen jatkuvuudesta sekä tietosuojan toteutumisesta.

Esimiehet vastaavat siitä, että työntekijöillä on oikeudet tehtävän edellyttämässä laajuudessa tarvittaviin tietojärjestelmiin ja tietoihin. Esimiehet vastaavat myös siitä, että työtehtävien muutokset huomioidaan tietojärjestelmien käyttöoikeuksissa. Työsuh-

teen päättyessä esimiesten on huolehdittava kaiken työnantajalle kuuluvan omaisuuden palauttamisesta ja järjestelmien käyttöoikeuksien poistamisesta.

Esimiesten tulee huolehtia siitä, että työntekijät saavat riittävän perehdytyksen ja koulutuksen tietoturvaan ja tietosuojaan ja siitä, että työntekijät ymmärtävät tietoturvan ja tietosuojan merkityksen. Esimiehiltä odotetaan esimerkillistä ja vastuullista tietoturva- ja tietosuojakäyttäytymistä.

Työntekijöiden vastuulla on huolehtia siitä, että heidän työtehtävissään käsittelemät, organisaatiolle kuuluvat tiedot jäävät organisaation haltuun, ellei niitä muilla määräyksillä ole määrätty hävitettäväksi tai muuten käsiteltäviksi. Jokaisen työntekijän on tunnettava voimassa olevat ohjeet ja ottaa ne toiminnassaan huomioon.

Kaupungin toimeksiannosta ja lukuun toimivat vastaavat omalta osaltaan tietojen käsittelyn oikeellisuudesta ja lainmukaisuudesta sekä kaupungin antamien tarkentavien ohjeiden noudattamisesta tietojenkäsittelyssään.

6. TIETOTURVA- JA TIETOSUOJATYÖN ORGANISOINTI JA TOTEUTUSKEINOT

Tietoturvan ja tietosuojan toteuttamisen perustana on kaupungin tietoturva- ja tietosuojapolitiikka, joka on perehdytetty koko organisaatiolle. Tietoturvan ja tietosuojan kehittämistä ja ylläpitoa koordinoi tietoturva -asiantuntija ja tietosuojavastaava yhdessä kaupunginjohtajan tarvittaessa asettaman työryhmän kanssa. Tietoturva-asiantuntijan ja tietosuojavastaavan tehtävänä on ylläpitää tietoturva- ja tietosuojapolitiikkaa sekä laatia tietoturvaan ja tietosuojaan liittyvät esityksiä, ohjeita ja toimintamalleja.

Käytännön teknisestä tietoturvasta ja sen ohjeistuksesta vastaavat palveluntuottajat, joille palvelun toteutus on sopimuspohjaisesti luovutettu. Kaikkiin palvelutasosopimuksiin sisällytetään tietoturvaan ja tietosuojaan liittyvät vaatimukset, velvoitteet ja häiriötilanteiden toimintamallit sekä määritellään vastuuhenkilöt läpi koko palveluketjun. Palvelutuottajan vastuulla on raportoida tietoturvaan ja tietosuojaan kohdistuvista merkittävistä riskeistä ja uhkista välittömästi määritellylle yhteyshenkilölle.

Jokaisen Kuusamon kaupungin tietoja käsittelevän työntekijän ja kaupungin tietoverkkojen ja järjestelmien käyttäjän on noudatettava hyväksyttyä tietoturva- ja tietosuojapolitiikkaa sekä sitä täydentäviä ohjeita. Esimiesten vastuulla on valvoa tietoturva- ja tietosuojaohjeiden noudattamista sekä tietoturvan ja tietosuojan toteutumista yksikkö- ja työntekijätasolla. Tietoturva-asiantuntijan ja tietosuojavastaavan tehtävänä on kommunikoida tietoturva- ja tietosuoja -asioista läpi koko organisaation ja koordinoida tietoturvan ja tietosuojan kehittämistoimia. Jokaisella työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietoturvallisuuteen ja tietosuojaan liittyvistä puutteista tai väärinkäytöksistä esimiehelleen tai tietoturva -asiantuntijalle tai tietosuojavastaavalle.

Jokaisella kaupungin järjestelmällä tulee olla nimetty omistaja, joka vastaa järjestelmän tietoturvan ja tietosuojan toteutumisesta. Järjestelmän omistajuuteen ja järjestelmän sisältämien tietojen käyttöön liittyvät tiedot dokumentoidaan tarvittavissa selosteissa. Kaikki tietojärjestelmät ja tietovarannot luokitellaan niissä käsiteltävien tietojen ja tunnistettujen tietoturva- ja tietosuojariskien mukaisesti. Tietojen ja tietojärjestelmien omistajien on tehtävä luokittelua vastaavat tietojärjestelmiä koskevat riskikar-

toitukset ja tietoturva- ja tietosuojaohjeet käyttäjille sekä huolehdittava, että työtekijät saavat riittävän koulutuksen. Riskikartoitusten toteuttamista ja ohjeiden noudattamista on seurattava aktiivisesti. Omistajien on ylläpidettävä ajantasaisia varautumissuunnitelmia, joissa kuvataan vastuuhenkilöt, roolit ja toimintamallit riskien toteutumisen varalta.

7. SEURANTA JA ONGELMATILANTEET

Tietoturva- ja tietosuojapolitiikan ja -ohjeiden noudattamisen valvonta on tärkeä osa kaupungin sisäistä valvontaa. Toimialojen, liikelaitosten ja tytäryhtiöiden vastuussa oleva johto, tietoturva -asiantuntija ja tietosuojavastaava seuraavat teknisen ja hallinnollisen tietoturvan sekä tietosuojan toteutumista.

IT -palveluiden tuottajilla on velvollisuus raportoida säännöllisesti tietoturvaan ja tietosuojaan liittyvistä palvelutasojen täyttymisestä ja riskeistä määritellyille yhteyshenkilöille. Esimiesten tulee raportoida tietoturvapoikkeamista toimialajohtajalle ja tietoturva -asiantuntijalle sekä tietosuojaloukkauksista toimialajohtajalle ja tietosuojavastaavalle huomioiden mm. asetuksen asettamat aikarajat.

Tietoturvapoikkeamissa ja tietosuojaloukkauksissa tai niihin liittyvässä uhkatilanteessa nimetyllä toimialajohtajalla ja/tai tietohallintojohtajalla sekä tietoturva -asiantuntijalla on oikeus sulkea tietty tietoliikenneyhteys, järjestelmä, tunnus tai laite. Edellä mainittujen on viipymättä tai heti kun se on mahdollista informoitava asianomaisia tahoja tehdyistä toimenpiteistä ja mahdollisista jatkotoimista.

8. TIEDOTTAMINEN

Tietoturva- ja tietosuoja-asioiden sisäisestä tiedottamisesta vastaavat tietoturva -asiantuntija ja tietosuojavastaava sekä kaupungin johtoryhmä. Hallintokunnat, liikelaitokset ja tytäryhtiöt hoitavat itse sisäisen tiedottamisen. Toimialajohtaja, tietoturva -asiantuntija, tietosuojavastaava ja IT -palveluiden tuottajat ylläpitävät käyttäjien saatavilla käytännön tietoturva- ja tietosuojaohjeita ja tiedottavat työntekijöitä ja muita sidosryhmiä akuuteista tietoturva- ja tietosuojariskeistä sekä suojautumiskeinoista tarvittavassa laajuudessa.

Ulkoisesta tietoturvaan ja tietosuojaan liittyvästä tiedottamisesta vastaa tietohallintojohtaja tai nimetty toimialajohtaja yhdessä kaupunginjohtajan kanssa. Poikkeusolojen tiedottamisesta vastaa kaupunginjohtaja.