JULKINEN

**WIITAUNIONIN DIGITURVAPOLITIIKKA**

 **1 Johdanto**

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

Kunnan johto määrittelee tässä politiikassa digitaalista turvallisuutta koskevat periaatteet, linjaukset, vastuut ja tavoitteet. Politiikka toimii perustana digitaalista turvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa.

Tämä politiikka koskee jokaista kunnan työntekijää ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee kunnan omistamaa tai hallinnoimaa tietoa.

Tätä politiikkaa sovelletaan kaikkeen tietoon ja muuhun dataan (myöh. tieto) riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotiestä.

**2 Vaatimustenmukaisuus ja tavoitteet**

Velvoittavan lainsäädännön lisäksi kunnan digitaaliselle turvallisuudelle asettaa vaatimuksia kunnan toimintaympäristö. Kunta on valinnut digitaalista turvallisuutta ohjaaviksi tekijöiksi, soveltuvilta osin, seuraavat:

EU:n Yleinen Tietosuoja-asetus: (EU) 2016/679 ja tietosuojalaki 1050/2018

 Laki julkisen hallinnon tiedonhallinnasta 906/ 2019

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeet

Kunnan digitaalisen turvallisuuden tavoitteena on:

yhdenmukaistaa kunnan sisäisiä turvallisuuskäytäntöjä kehittämällä kunnan turvallisuuskulttuuria

varmistaa seudullinen turvallisuuskäytäntöjen yhteensopivuus tekemällä yhteistyötä Pohjoisen Keski-Suomen seutuverkon kuntien ja Pohjoisen Keski-Suomen Verkkopalvelut Oy:n kanssa

Tavoitteiden saavuttamiseksi toteutetut ja suunnitellut toimenpiteet, kuvataan erillisissä suunnitelmissa.

**3 Digitaalinen turvallisuus**

Digitaalisella turvallisuudella tarkoitetaan keskeisiä kunnan määrittelemiä turvallisuuden, riskienhallinnan ja varautumisen osa-alueita, jotka yhdessä tietoturvallisuuden ja tietosuojan kanssa muodostavat eheän kokonaisuuden kunnan tiedon suojaksi:

Kybertuvallisuus: Toimenpiteet, joilla turvataan kybertoimintaympäristön1 luottamuksellisuus, eheys, saatavuus ja jatkuvuus.

Fyysinen turvallisuus: Toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja, siellä olevia ihmisiä, tietoa ja muuta omaisuutta suojataan fyysisiltä ja kiinteistö- ja ympäristövahingoilta, vahingoittamisyrityksiltä ja oikeudettomilta henkilöiltä.

Henkilöstöturvallisuus: Tietoturvallisuuteen vaikuttavat toimenpiteet, joita suoritetaan henkilöstöprosessissa ennen palvelussuhdetta, sen aikana ja sen päättymisen yhteydessä.

Riskien hallinta: Järjestelmällistä toimintaa riskien hallitsemiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun kunnan toiminnalle asetetut tavoitteet voidaan saavuttaa.

Varautuminen: Tekniset järjestelyt ja toimintatavat, joilla kunnan toimintojen ja palveluiden jatkuvuus turvataan normaalioloissa, häiriötilanteissa sekä poikkeusoloissa.

 Tietoturvallisuus: Hallinnolliset, tekniset ja muut keinot, joilla suojataan kunnan omistamaa tai hallinnoimaa tietoa normaali- ja häiriötilanteissa sekä poikkeusoloissa

 Tietosuoja: Velvoittavien tietosuojasäädösten mukaiset toimenpiteet, joilla varmistetaan henkilön riittävä yksityisyyden suoja, ja muut sitä turvaavat oikeudet, henkilötietoja käsiteltäessä.

Sopimushallinnan keinoin pidetään huolta siitä, että digitaalinen turvallisuus toteutuu myös sidosryhmien toiminnassa.

**4 Organisointi, roolit ja vastuut**

Digitaaliseen turvallisuuteen liittyvät roolit vastuineen on organisoitu kunnassa seuraavasti.

**Kunnan-/kaupunginhallitus** seuraa digitaalisen turvallisuuden toteutumista kunnassa. Kunnan-/kaupunginhallitus hyväksyy digiturvapolitiikan. Lisäksi hallituksella on vastuu kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä.

**Kunnan-/kaupunginjohtajalla** on kokonaisvastuu digitaalisen turvallisuuden toteuttamisesta ja sen toteutumisen raportoinnista hallitukselle. Kunnan-/kaupunginjohtaja omistaa digiturvapolitiikan ja hyväksyy siitä johdetut tarkentavat ohjeet ja määräykset sekä vastaa säännöllisestä digiturvallisuuden katselmuksesta.

**Toimialajohtaja** vastaa toimialansa digitaalisen turvallisuuden toteutumisesta.

**Tytäryhtiöiden hallitukset ja toimitusjohtajat** vastaavat digitaalisen turvallisuuden toteutumisesta omissa organisaatioissaan.

**Esimies** vastaa digitaalisen turvallisuuden toteutumisesta omalla vastuualueellaan.



**Henkilöstö** vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokainen on lisäksi velvollinen ilmoittamaan poikkeamista, uhkista ja riskeistä välittömästi omalle esimiehelleen, tietosuojavastaavalle tai IT-vastuuhenkilölle.

**Tietojärjestelmästä tai muusta teknisestä kokonaisuudesta vastaava** viranomainen päättää järjestelmänsä ja sen sisältämän tiedon digitaalisen turvallisuuden toteutumisesta.

**Pääkäyttäjä** vastaa järjestelmänsä osalta digitaalisen turvallisuuden toteuttamisesta tietojärjestelmän omistajan ohjauksessa.

**Tiedosta** vastaava viranomainen päättää tiedon luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

**Digiturvakoordinaattori** vastaa digiturvapolitiikan jalkauttamisen tukemisesta kunnassa sekä tähän sisältyvästä tietosuojavastaavan tehtävästä.

**Tietosuojavastaava** edistää tietoturvallisuuden ja tietosuojan toteutumista kunnassa. Tietosuojavastaava on riippumaton toimija, joka seuraa tietosuojaa ohjaavan lainsäädännön noudattamista kunnassa. Lisäksi tietosuojavastaava tekee yhteistyötä valvonta- ja muiden viranomaisten kanssa sekä tukee ja neuvoo tietoturva- ja tietosuoja -asioissa. Tietosuojavastaava raportoi tietoturvallisuuden ja tietosuojan toteutumisesta kaupunginjohtajalle ja vastaa tieto-turvallisuuteen ja tietosuojaan liittyvästä viestinnästä yhdessä viestintätoimen kanssa.

**Wiitaunionin johtoryhmä** johtaa,koordinoi, ohjaa toimialakohtaista tietoturva- ja tietosuojatyötä ja seuraa työtä johdon katselmuksin.

**Digiturvaryhmä** toimii tietosuojavastaavan tukena kunnassa. Ryhmä seuraa tietoturvallisuuden ja tietosuojan yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden ja tietosuojan toteutumista kunnassa. Ryhmä analysoi ja arvioi em. kokonaisuutta ja tekee siihen perustuen kehitysehdotuksia kunnan tietoturvallisuuden ja tietosuojan parantamiseksi. Lisäksi ryhmä toimii, yhdessä digiturvakoordinaattorin

/tietosuojavastaavan kanssa, kunnan tukena tietoturva- ja tietosuoja -asioissa.

**Henkilöstöjohtaja** vastaa digitaalisen turvallisuuden ohjeistamisesta ja toteutumisesta henkilöstöprosessin kaikissa vaiheissa työ-/virkasuhteen alkamisesta sen päättymiseen.

**Ulkoiset sidosryhmät** vastaavat omalta osaltaan tietoturvallisuuden ja tietosuojan toteuttamisesta, sopimuksissa kuvattujen kunnan asettamien vaatimusten mukaisesti.

**5 Tiedon ja tietojärjestelmien käyttö**

Kunnan tietojärjestelmäympäristössä käytetään kunnan hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Kunnan tietojärjestelmäympäristöön saa tehdä muutoksia vain kunnan IT tai sen valtuuttama taho.

Pääsyoikeudet kunnan tietoverkkoon ja -järjestelmiin sekä käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon myönnetään työtehtävien hoitoon tarvittavassa laajuudessa.

**6 Digitaalisen turvallisuuden toteuttaminen**

Digitaalista turvallisuutta toteutetaan kunnan hallintojärjestelmässä kuvattavilla jatkuvaan parantamiseen tähtäävillä johtamis- ja muilla käytännöillä. Keskeistä toteuttamisessa on, että kunnalla on riittävät kyvykkyydet ylläpitää turvallisuuskulttuuriaan mm. seuraavasti:

Digitaalista turvallisuutta johdetaan järjestelmällisesti

Henkilöstön osaamisesta huolehditaan jatkuvilla koulutuskäytännöillä

Toimintaympäristön tilaa seurataan

Uhka- ja riskiympäristöä arvioidaan säännöllisesti ja reagoidaan tilanteen edellyttämällä tavalla

Poikkeamiin ja häiriöihin varaudutaan ennakolta ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuus- ja muita suunnitelmia.

**7 Dokumentin ylläpito**

Tämän politiikan säännöllisestä katselmoinnista ja päivittämisestä vastaa kaupungin-/kunnanjohtaja tai hänen nimeämänsä taho. Politiikka on julkisesti saatavilla kunnan verkkosivuilla. Kunnan digiturvadokumentaatiota kokonaisuudessaan pidetään henkilöstön saatavilla kunnan sisäisissä informaatiokanavissa työtehtävien edellyttämässä laajuudessa.