1 Johdanto

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

Kunnan johto määrittelee tässä politiikassa tietoturvallisuutta ja tietosuojaa koskevat periaatteet, linjaukset, vastuut ja tavoitteet. Politiikka toimii perustana kunnan tietoturvallisuutta ja tietosuojaa 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 tietoturvallisuudelle ja tietosuojalle asettaa vaatimuksia kunnan toimintaympäristö. Kunta on valinnut tietoturvallisuutta ja tietosuojaa ohjaaviksi tekijöiksi, soveltuvilta osin, seuraavat:

- EU:n Yleinen Tietosuoja-asetus: (EU) 2016/679
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa: 681/2010, 5§
- Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeet

Kunnan tietoturva- ja tietosuojatyön 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 Tietoturvallisuus ja tietosuoja

Tietoturvallisuudella tarkoitetaan kunnassa hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kunnan omistamaa tai hallinnoimaa tietoa normaali- ja häiriötilanteissa sekä poikkeusoloissa. 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: Todisteiden keräämistä sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen.

Tietosuojalla tarkoitetaan kunnassa velvoittavien tietosuojasäädösten mukaisia toimenpiteitä, joilla varmistetaan henkilön riittävä yksityisyyden suoja, ja muut sitä turvaavat oikeudet, henkilötietoja käsiteltäessä.

Henkilötiedot, joita kunta kerää ja käsittelee, on kuvattu tietosuojaselosteissa, jotka ovat julkisesti saatavilla kunnan verkkosivuilla.

Tietoturvallisuus ja tietosuoja, sekä niihin liittyvät kunnan määrittelemät vaatimukset, tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan, hankintojen ja teknisten järjestelmien suunnittelua.

4 Kokonaisturvallisuus

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

- Kybertuvallisuus: Toimenpiteet, joilla turvataan kybertoimintaympäristön[1] 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.
- Sopimushallinta: Sopimustekniset toimenpiteet, joilla varmistetaan tässä politiikassa kuvattujen periaatteiden toteutuminen myös sidosryhmien kanssa tehtävässä yhteistyössä.
- 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.

5 Organisointi, roolit ja vastuut

Tietoturvallisuuteen ja tietosuojaan liittyvät roolit vastuineen on organisoitu kunnassa seuraavasti.

Kunnanhallitus seuraa tietoturvallisuuden ja tietosuojan toteutumista kunnassa. Kunnanhallitus hyväksyy tietoturvapolitiikan. Lisäksi hallituksella on vastuu kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden ja tietosuojan toteuttamisesta ja niiden toteutumisen raportoinnista hallitukselle. Kunnanjohtaja omistaa tietoturvapolitiikan ja hyväksyy siitä johdetut tarkentavat ohjeet ja määräykset.

[1] Toistensa kanssa eri teknologioiden avulla vuorovaikutuksessa olevien henkilöiden, järjestelmien sekä palveluiden muodostama ympäristö.

Toimialajohtaja vastaa toimialansa tietoturvallisuuden ja tietosuojan toteutumisesta sekä omistamiensa prosessien kokonaisturvallisuudesta.

Tytäryhtiöiden hallitukset ja toimitusjohtajat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta sekä kokonaisturvallisuuden toteutumisesta omissa organisaatioissaan.

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

- oman organisaationsa perehdyttämisestä kunnan tietoturva- ja tietosuojaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin.
- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
    - kunnan tiedon ja muun omaisuuden palauttamisesta
    - ilmoittamisesta IT-vastuuhenkilölle työntekijän käyttöoikeuksien ja -valtuuksien poistamiseksi.

Henkilöstö vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokaisen vastuulla on lisäksi poikkeamien, uhkien ja riskien ilmoittaminen välittömästi omalle esimiehelleen, tietosuojavastaavalle tai IT-vastuuhenkilölle.

Tietojärjestelmän tai muun teknisen kokonaisuuden **omistaja** vastaa järjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Pääkäyttäjä vastaa järjestelmänsä osalta tietoturvallisuuden ja tietosuojan toteuttamisesta tietojärjestelmän omistajan ohjauksessa.

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

Seudullinen 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 kunnanjohtajalle ja Keski-Suomen Verkkopalvelut Oy:n toimitusjohtajalle, sekä vastaa tietoturvallisuuteen ja tietosuojaan liittyvästä viestinnästä yhdessä viestintätoimen kanssa.

Tietosuojaryhmä toimii tietosuojavastaavan tukena kunnassa. Tietosuojaryhmä 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 tietotuojan parantamiseksi. Lisäksi ryhmä toimii, yhdessä tietosuojavastaavan kanssa, kunnan tukena tietoturva- ja tietosuoja -asioissa.

Pohjoisen Keski-Suomen kuntien ja kaupunkien IT **(Seutu-IT)** vastaa teknisen tietoturvallisuuden suunnittelusta, ohjauksesta ja toteuttamisesta sekä toteutumisen raportoinnista Pohjoisen Keski-Suomen Verkkopalvelut Oy:n hallitukselle ja tiedottamisesta kunnanjohtajalle.

Sisäinen tarkastus vastaa tietoturvallisuuden toteutumisen asianmukaisuudesta ja riittävyyden arvioinnista sekä tarkastamisesta.

Henkilöstöhallinto vastaa tietoturvallisuuden ja tietosuojan toteutumisesta henkilöstöhallinnon kaikissa vaiheissa työ-/virkasuhteen alkamisesta sen päättymiseen.

Kunnanjohtaja vastaa kunnan turvallisuussuunnittelusta ja varautumisesta.

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

6 Tiedon ja tietojärjestelmien käyttö

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

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

7 Tietoturvallisuuden ja tietosuojan toteuttaminen

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

- Tietoturvallisuutta ja tietosuojaa johdetaan järjestelmällisesti
- Henkilöstön osaamisesta huolehditaan jatkuvilla koulutuskäytännöillä
- Toimintaympäristön tilaa seurataan aktiivisesti
- Uhka- ja riskiympäristöä arvioidaan säännöllisesti ja reagoidaan tilanteen edellyttämällä tavalla
- Poikkeamiin ja häiriöihin varaudutaan ennakolta ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuus- ja muita suunnitelmia.

8 Dokumentin ylläpito

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