KIVIJÄRVEN KUNNAN TIETOTURVAPOLITIIKKA

Johdanto

Tieto on keskeisessä roolissa kunnan toiminnassa ja palvelutuotannossa. Ollakseen tehokkaasti hyödynnettävissä tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti. Tietoturvan ja tietosuojan parantaminen on myös osa kunnan toiminnan kehittämistä, jatkuvuuden varmistamista ja valvontaa.

Kunta määrittelee tässä politiikassa tietoturvallisuutta ja tietosuojaa koskevat periaatteensa, linjauksensa, vastuunjaot ja tavoitteensa. Politiikka toimii perustana kunnan tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa.

Tämä politiikka sekä siihen liittyvät ohjeet ja määräykset koskevat kaikkia kunnan työntekijöitä, luottamushenkilöitä, työryhmiä, toimielimiä ja sidosryhmän edustajaa (*palveluntuottaja*), joka työnsä tai toimeksiantonsa puitteissa käsittelee kunnan omistamaa tai hallinnoimaa tietoa.

Kunnan tietoturvatyötä tehdään kiinteässä yhteistyössä kuntien yhdessä omistaman Pohjoisen Keski-Suomen Verkkopalvelut Oy:n kanssa.

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

• Vaatimustenmukaisuus ja tavoitteet

Velvoittavan lainsäädännön lisäksi kunnan tietoturvallisuudelle ja tietosuojalle asettaa vaatimuksia kunnan toimintaympäristö. Kunta on todennut tietoturvallisuutta ja tietosuojaa ohjaaviksi tekijöiksi seuraavat säädöstöt ja soveltuvilta osin ohjeet:

- EU:n yleinen tietosuoja-asetus: (EU) 2016/679 sekä sen johdosta annettava tietosuojalaki
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
- Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän ohjeet (VAHTI, www.vahtiohje.fi)

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.

• 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.

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

• 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 luottamuksellisuus, eheys, saatavuus ja jatkuvuus.
- *Fyysinen turvallisuus*: Toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja, siellä olevia ihmisiä, kuljetuksia, matkatyötä sekä 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.
- *Riskienhallinta*: 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.

Asianmukaisilla ja ajantasaisilla sopimuksilla varmistetaan tässä politiikassa kuvattujen periaatteiden toteutuminen myös sidosryhmien kanssa tehtävässä yhteistyössä.

• Organisointi, roolit ja vastuut

Tietoturvallisuuteen ja tietosuojaan liittyvät roolit vastuineen organisoidaan kunnassa seuraavasti:

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

Kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden, tietosuojan, turvallisuussuunnittelun ja varautumisen toteuttamisesta ja niiden toteutumisen raportoinnista kunnanhallitukselle.

Osastonjohtaja vastaa toimialansa sisäisten toimintojen ja tuottamien palveluiden sekä tietojärjestelmien riskienhallinnasta, varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Pääkäyttäjä vastaa käyttämänsä tietojärjestelmän tietoturvallisuuden ja tietosuojan toteuttamisesta osastonjohtajansa ohjauksessa.

Tytäryhteisöjen 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 työntekijänsä työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin.
- huolehtia työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
    - kunnan tiedon ja muun omaisuuden palauttamisesta
    - ilmoittamisesta ICT-tukihenkilölle työntekijän käyttöoikeuksien ja -valtuuksien poistamiseksi

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

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

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

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 tietoturvassa ja -suojassa.

Kunnan ICT-tukihenkilö vastaa teknisen tietoturvallisuuden suunnittelusta, ohjauksesta ja toteuttamisesta yhteistyössä Pohjoisen Keski-Suomen Verkkopalvelut Oy:n kanssa. Hän raportoi kunnanjohtajalle ja Pohjoisen Keski-Suomen Verkkopalvelut Oy:n toimitusjohtajalle.

Sisäisen tarkastuksen tehtäviin kuuluu tietoturvallisuuden ja tietosuojan toteutumisen asianmukaisuuden ja riittävyyden arviointi.

Esimies ja esimiehen esimies yhdessä henkilöstöhallinnon kanssa vastaa tietoturvallisuuden ja tietosuojan toteutumisesta henkilöstöprosessissa rekrytoinnista työ-/virkasuhteen päättymiseen.

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

• Tiedon ja tietojärjestelmien käyttö

Kunnan tietojärjestelmäympäristössä käytetään kunnan hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Kunnan tietojärjestelmäympäristöön saa tehdä asennuksia ja muutoksia vain kunnan ICT-tukihenkilö tai muu kunnan valtuuttama taho.

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

• 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 kehittää ja 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.

• Dokumentin ylläpito

Tämän politiikan säännöllisestä katselmoinnista ja päivittämisestä vastaa kunnanjohtaja tai hänen nimeämänsä taho. Politiikka ja kunnan muu tietoturva- ja tietosuojadokumentaatio on henkilöstön saatavilla kunnan sisäisissä informaatiokanavissa työtehtävien mukaisessa laajuudessa.