HYRYNSALMEN KUNTA

Tietoturva- ja tietosuojapolitiikka

voimassa 1.9.2018 alkaen

luonnos 9.8.2018

Hyrynsalmen kunta
Tietoturva- ja tietosuojapolitiikka

Sisällysluettelo:

1. Johdanto

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

Tietoturvapolitiikassa kunnan johto määrittelee tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet. Tietoturvapolitiikka toimii perustana kunnan tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa tietoturvapolitiikassa annettuja määräyksiä ja auttaa niiden käytäntöön soveltamisessa. Tietoturvapolitiikka ja sen soveltamisohjeet pidetään käyttäjien saatavilla kaikissa kunnan toimipisteissä.

Tietoturvapolitiikka koskee Hyrynsalmen kunnan organisaatiota – niin työntekijöitä kuin luottamushenkilöitäkin – sekä niitä kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kunnan omistamaa tai hallinnoimaa tietoa. Tietoturvapolitiikka kattaa kunnan käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2. Tietoturvallisuus

Hyrynsalmen kunnassa tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kunnan omistamaa ja hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa että poikkeusoloissa.

Tietoturvallisuus on kiinteä osa kunnan johtamista, palveluita ja toimintoja. Se ulottuu jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin sekä luottamushenkilöiden toimintaan kunnan asioiden käsittelijöinä. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten ihmisten yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä.

Henkilötietoja käsitellään vain perustellun käyttötarkoituksen vuoksi ja vain siinä määrin ja niin kauan, kun se on käyttötarkoituksen kannalta tarpeellista. Käytettävien tietojen oikeellisuus pyritään varmistamaan ja tietoja päivitetään. Henkilötietoja säilytetään ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Tietosuojaa ohjaavina periaatteina on lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä tietojen eheys ja luottamuksellisuus.

Tietoturvallisuuteen liittyvillä vastuutuksilla ja käytännöillä pyritään varmistamaan, että kunnan omistama ja hallinnoima tieto
- on oikeaa ja eheää, eikä ole muuttunut teknisen tai inhimillisen toiminnan seurauksena
- on vain siihen oikeutettujen saatavilla
- on saatavilla, kun sitä tarvitaan.

Tähän liittyen tulee tiedon käsittelyprosessien omistajuus ja käyttöoikeudet määritellä sekä huolehtia tiedon elinkaaren hallinnasta niin, että tietoon sen käsittelyn eri vaiheissa tehdyt muutokset voidaan tarvittaessa jäljittää ja todentaa.

Hyvän tietoturvallisuuden aikaansaaminen ja ylläpito edellyttävät tietoista johtamista ja hyvän hallintotavan noudattamista kaikissa kunnan toiminnoissa. Tietoturvallisuuden osalta tämä kokonaisuus sisältää suunnitteluun, toteutukseen, seurantaan ja ohjaukseen liittyvät prosessit, asiakirjat, kontrollit ja vastuut.

Kunnan tietoturvatyötä ohjaavat, soveltuvilta osin seuraavat viitekehykset:

- Kuntia velvoittavat lait ja asetukset
- EU:n tietosuoja-asetus (GDPR)
- Kunnan voimassa olevat strategiat, hallinto- ja ohjesäännöt, riskienhallinta-, valmius- ja viestintäsuunnitelmat (tietoturvallisuutta koskevilta tai sivuavilta osiltaan)
- Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositukset
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

Tietoturvallisuus on osa Hyrynsalmen kunnan riskienhallintaa, varautumista ja kokonaisturvallisuutta. Riskienhallintaa toteutetaan kunnan sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti. Periaatteena on, että riskienhallintaprosessia käytetään säännöllisesti toteutettavaan sisäisten ja ulkoisten tietoon kohdistuvien ja tiedosta aiheutuvien riskien hallintaan.

Hyrynsalmen kunta varautuu turvaamaan ensisijassa kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia valmius- ja muita suunnitelmia. Varautumiseen liittyvät roolit ja vastuut kuvataan em. suunnitelmissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

3. Tietoturvallisuustavoitteet

Kunnan tavoitteena on saavuttaa Tietoturvallisuusasetuksen (681/2010) kuvaaman tietoturvallisuuden perustason vaatimukset koko kunnan laajuisesti ja korotetun tason vaatimukset lainsäädännön edellyttämissä toiminnoissa tai toiminnan muutoin niin vaatiessa.

4. Organisointi ja tietoturvavastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kunnan sääntöjen mukaisesti.

Kunnanhallitus seuraa tietoturvallisuuden toteutumista kunnassa. Kunnanhallitus hyväksyy tietoturvapolitiikan ja siihen ehdotetut muutokset. Kunnanhallituksella on vastuu kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden toteuttamisesta ja tietoturvallisuuden toteutumisen raportoinnista kunnanhallitukselle. Kunnanjohtaja hyväksyy kunnantasoiset ohjeet ja linjaukset. Kunnanjohtajan tukena tietoturvallisuusasioissa on kunnan johtoryhmä.

Palvelujen päälliköt vastaavat toimialansa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

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

Esimies vastaa tietoturvallisuuden toteutumisesta omalla vastuualueellaan. Esimiehen keskeisimpinä tehtävinä on huolehtia:

- oman organisaationsa perehdyttämisestä kunnan tietoturvaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturvavastuisiin.
- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
    - kunnan tiedon ja muun omaisuuden palauttamisesta
    - ilmoittamisesta Kainuun soten tietohallinnolle työntekijän käyttöoikeuksien ja valtuuksien poistamiseksi.

Henkilöstö vastaa tietoturvan ja -suojan toteuttamisesta omalta osaltaan. Jokaisen vastuulla on lisäksi tietoturvaa ja -suojaa koskevien ohjeiden noudattamien sekä tietoturvallisuuteen liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi tietosuojavastaavalle ja omalle esimiehelleen.

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

Tietojärjestelmän omistaja vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy henkilön esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.

Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Lisäksi hän vastaa prosessin riippuvuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Tietosuojavastaava antaa tietoa ja neuvoja tietosuojaan liittyvissä asioissa, seuraa tietosuoja-asetuksen ja kansallisten tietosuojaa koskevien lakien noudattamista, tekee yhteistyötä valvontaviranomaisten kanssa ja toimii valvontaviranomaisen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaava koordinoi tietosuojaryhmää.

Tietosuojaryhmä toimii tietosuoja-asioissa tietosuojavastaavan tukena organisaation sisäisenä asiantuntijaverkostona. Tietosuojaryhmä ja tietosuojavastaava kehittävät kunnan tietosuoja-asioita yhteistyössä kunnan johtoryhmän kanssa.

Tietohallinto vastaa teknisestä tietoturvallisuudesta, sitä tukevien tietoturvalinjausten tekemisestä ja asetettujen tietoturvavaatimusten toteuttamisesta.

Asiakirjahallinto vastaa asiakirjatiedon hallinnasta ja siihen liittyvästä ohjeistuksesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta asiakirjahallinnossa.

Palvelun tuottajat vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumista tietojärjestelmissä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

5. Tiedon ja tietojärjestelmien käyttö

Kunnan tietojärjestelmäympäristössä käytetään tietohallinnon hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten.

Käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi kunnan ohjeita. Henkilötietojen käsittelyssä noudatetaan voimassaolevaa lakia ja tietosuojaa ohjaavia periaatteita.

6. Tietoturvaosaamisen varmistaminen

Johdon tehtävänä on varmistaa koulutuksen ja ohjeiden avulla, että henkilöstön tietoturvaosaaminen on riittävää. Myös osaamisen ylläpidosta on huolehdittava niin, että se vastaa kulloinkin vallitsevia tilanteita ja toimintaympäristön vaatimuksia.

Jokainen uudessa tehtävässä aloittava työntekijä perehdytetään tietoturvan ja -suojan perusteisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään. Lisäksi tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti, ja tietoturvaohjeet pidetään kaikkien työntekijöiden saatavilla.

Jokaisen Hyrynsalmen kunnan työntekijän on suoritettava omatoiminen tietoturva- ja tietosuojakoulutus ja siihen liittyvä testi. Testi tehdään henkilökohtaisesti, ja esimiehet tarkistavat alaistensa osalta sen suorittamisen.

7. Tietoturvapoikkeamien käsittely ja niistä tiedottaminen

Tietoturva- ja tietosuojaohjeiden noudattamista valvotaan sekä säännöllisin rutiinein tai automaattisesti että pistokokein. Väärinkäytöksiin puututaan. Väärinkäytöksiä tai rikoksia epäiltäessä tietoturvavastaava ja epäillyn esimies ratkaisevat, mikä on oikea ja sopiva tapa käsitellä asiaa.

Sekä odottamattomista että ennalta tiedetyistä palvelukatkoksista ja muista tietojärjestelmien käytön häiriöistä tiedotetaan tiedotussuunnitelman mukaisesti kunnan tavanomaisia tiedotuskanavia hyödyntäen.

Tietoturvapoikkeamat käsitellään ja niistä raportoidaan kunnanjohtajan ja tietosuojavastaavan erikseen tarkemmin ohjeistamalla tavalla. Muulle organisaatiolle havaituista poikkeamista tiedotetaan niiden luonteen ja laajuuden edellyttämällä tavalla. Tietoturvaloukkauksissa noudatetaan EU:n tie-

tosuoja-asetuksen määräyksiä henkilötietojen tietoturvaloukkauksen ilmoittamisesta valvontaviranomaiselle ja rekisteröidylle artiklojen 33 ja 34 mukaisesti.

8. Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Tietoturvallisuustyön tulee olla suunnitelmallista ja käytännön toteutusten tulee vastata toiminnan tarpeisiin, lainsäädännön vaatimuksiin sekä kunnan riskienhallintatyössä asetettuihin muihin tavoitteisiin, ulkoiset toimintaolosuhteet huomioiden.

Seurannan ja muutoshallinnan keinoin varmistetaan, että tietoturvallisuuteen liittyvät kokemukset, palaute ja muutokset vaatimuksissa tai olosuhteissa tulevat oikea-aikaisesti huomioon otetuiksi.

Hyrynsalmen kunnan tietoturvapolitiikka katselmoidaan vuosittain ja päivitetään tarvittaessa.

Hyrynsalmen kuntaa sitoo myös Kainuun soten tietoturvaohjeet silloin, kun käytetään soten hallinnassa olevia tietojärjestelmiä.