Lapinlahden kunnan tietoturvapolitiikka

1. Johdanto

Tietoturvapolitiikka on kunnan ylimmän johdon hyväksymä strateginen asiakirja, joka on kannanotto tietoturvan kehittämiseen. Tietoturvapolitiikan tavoitteena on luoda yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietoturvatason toteuttamiseksi. Tietoturvapolitiikassa määritellään tietoturvatyön tavoitteet, vastuut, organisointi ja toteutuskeinot. Politiikan toteuttamisella luodaan edellytykset tietoturvallisen toiminnan pitkäjänteiseen kehittämiseen. Kunnanhallitus on hyväksynyt kunnan johtoryhmän tässä tietoturvapolitiikassa kuvaamat periaatteet, tavoitteet ja vastuut. Työssä onnistuminen edellyttää johdon sitoutumista tietoturvatyön tukemiseen.

2. Tietoturvapolitiikan tavoite

Tietoturvallisuuden käsite ja merkitys

Tiedon turvaaminen on merkittävä osa kunnan toiminnan ja sen järjestämien palvelujen laatua, ICT-riskienhallintaa ja kokonaisturvallisuutta. Riskienhallinnan keskeisenä tavoitteena on tunnistaa toimintaan kohdentuvat riskitekijät, arvioida niitä ja ryhtyä tarvittaviin toimenpiteisiin. Tietoturvan hyvä hallinta edellyttää toiminnan pitkäjänteistä suunnittelua, jatkuvaa kehittämistä, seurantaa ja erilaisiin uhkatilanteisiin varautumista. Tietoturvan toteuttaminen vaatii koko henkilöstön tietoturvatietoisuuden parantamista, sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja monikanavaista viestintää.

Määritelmät

Tieto eri muodoissaan on tärkeä perusta kaikelle kunnan toiminnalle. Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen (mm. sähköisesti tallennettu, välitetty tai rekisteröity tieto, suullinen puhuttu, postin kuljettama tai paperilla oleva tieto) suojaamista erilaisilta uhkatekijöiltä varmistaen palvelutoiminnan jatkuvuus minimoiden toimintaan tai asiakkaiden tietoihin liittyvät riskitekijät. Tietosuoja on myös osa tietoturvaa ja se tarkoittaa ihmisten yksityisyyden kunnioittamista ja suojelemista oikeudellisia säännöksiä noudattavien periaattein ja käytännöin.

Tietoturva määritellään kolmen peruskäsitteen kautta seuraavasti:

1) Tietojen luottamuksellisuus: tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeudet.

2) Tietojen eheys: tiedon oikeellisuus ja suojaus on järjestetty niin, että tietoa ei voi tahallisesti tai tahattomasti muuttaa vaarantaen toiminnan luotettavuutta. Lisäksi tietoon sen käsittelyn eri vaiheissa tehdyt muutokset on tarvittaessa kyettävä todentamaan.

3) Palveluiden ja tietojen saatavuus: tieto on saatavissa ja käytettävissä silloin, kun sitä palvelutoiminnassa tarvitaan.

Hyvä tietoturvataso saavutetaan tietoturvapolitiikan ja ohjeiden mukaisilla tietoturvallisilla toimintaperiaatteilla ja erilaisilla turvamekanismeilla, joita hallitaan ja katselmoidaan jatkuvan kehittämisen periaatteita noudattaen.

3. Tietoturvatoimintaa ohjaavat tekijät

Organisaation tietoturvallisuutta velvoittavat ja ohjaavat kansalliset ja kansainväliset yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lisäksi muut

tietoturvallisuutta ohjaavat velvoitteet, määräykset ja ohjeet. Jokaisen kuntakonsernin viranhaltijan, työntekijän ja luottamushenkilön sekä muun kunnan tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä.

4. Tietoriskien hallinta

Tietohallinto ja eri hallintokunnat seuraavat tietohallinto- ja ict-riskien ja uhkien toteutumista osana kunnan sisäistä valvontaa. Tarvittaessa suurimpien riskien vaikutuksia pyritään pienentämään tai ehkäisemään. Tietoriskien hallinta on jatkuvaa aktiivista toimintaa.

5. Tietoturvallisuuden merkitys organisaatiolle

Tietoturvatyön tavoitteena on turvata tietojärjestelmien, tietoverkkojen ja tietojenkäsittelylaitteiden keskeytymätön toiminta, havaita ja estää tietojen luvaton käyttö, tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen ja minimoida niistä aiheutuvat vahingot. Keskeinen tavoite on suojata elintärkeät toiminnot kaikissa häiriötilanteissa varmistaen palveluiden käytettävyys mahdollisimman lyhyellä toipumisajalla.

Toiminnan kannalta kriittiset palvelut on kartoitettu ja arvioitu keskeytysten vaikutukset toimintaan. Tietohallinnon varautumissuunnitelmassa käsitellään nämä asiat tarkemmin.

6. Turvatoimien priorisointi

Turvatoimien priorisoinnissa nojaudutaan samaan priorisointiin kun palvelupyyntöjä koskevassa priorisoinnissa. Korkeimmalle prioriteetille asetetaan toiminnoista terveydenhuolto, palkkojen maksu, maksuliikenne ja laskutukset sekä teknisesti suuria käyttäjämääriä koskevat verkon työt kuten palvelimiin ja kytkimiin liittyvät toimenpiteet.

7. Tietoturvavastuut

Kunnan tietoturvallisuuteen liittyvät roolit ja vastuut ovat:

Kunnanhallitus
- Tietoturvapolitiikan ja muiden koko kuntaa koskevien ohjeiden hyväksyminen
- Seuraa tietoturvan tilaa osana sisäistä valvontaa ja riskienhallintaa.

Kunnanjohtaja
- Tietoturvan ja tietosuojan järjestäminen ja toimintaedellytysten luominen sekä seuranta.
- Poikkeusolojen viestinnän johtaminen
- Varautuminen ja jatkuvuudenhallinta yhdessä kunnan johtoryhmän kanssa

Tietohallinto
- Tietoturvallisuuden suunnittelu, ohjaus, seuranta ja kehittäminen
- Teknisen tietoturvallisuuden minimivaatimusten määrittely, toteutus, ohjaus ja valvonta kunnan tietojärjestelmäympäristössä
- Tietoturvallisuuden teknisen valvonnan toteutuminen tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin
- Tietoturvariskien ja -poikkeamien hallinnan koordinointi
- Tietoturvallisuuden tilan raportointi osana sisäisen valvonnan selontekoa

Tietosuojavastaavat

- Auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja mahdollisten erityislakien edellyttämän tietosuojan tason

Osastopäällikkö ja yksiköiden päälliköt
- Osastopäällikkö nimeää jokaiselle rekisterille rekisterin pitäjän edustajan (rekisteriasioista vastaavan henkilön) sekä jokaiselle tietojärjestelmälle vastuuhenkilön/omistajan.
- Tietoturvallisuuden toteutuminen omalla toimialallaan

Tietojärjestelmän vastuuhenkilö/omistaja
- Omistamaansa tai hallinnoimaansa järjestelmään, tietoon tai prosessiin liittyvä:
    - o Pääkäyttäjän nimeäminen ko. järjestelmän osalta
    - o Käyttäjien ja käyttöoikeuksien hyväksyntä ko. järjestelmään
    - o Riskien- ja jatkuvuudenhallintatoimenpiteiden toteuttaminen omalta osaltaan
    - o Tiedon oikeellisuuden ja oikeiden käsittelytapojen varmistaminen
    - oTietojen julkisuuden ja salassapidon määrittely mukaan lukien arkistonmuodostus
    - oVastaa siitä, että tietojärjestelmästä on tehtynä asianmukainen seloste.

Pääkäyttäjä
- Tietoturvan toteutumisen valvonta omalla vastuualueellaan
- Sovelluksen ylläpitotoiminnoista huolehtiminen ja varmistaminen, että järjestelmää käytetään lakien, säädösten ja ohjeiden mukaisesti
- Tietosuojavastaavien avustaminen, henkilöstön neuvonta ja kouluttaminen
- Käyttäjien ja käyttöoikeuksien toteuttaminen

Jokaiselle henkilötietorekisterille on nimettävä rekisteriasioista vastaava henkilö. Tämän henkilön vastuulla on laatia rekisteristä asianmukainen seloste.

Jokaisella tietojärjestelmällä tulee olla yksilöity omistaja, joka vastaa koko järjestelmän elinkaaren hallinnasta, tietosuojasta ja tietoturvan toteuttamisesta. Järjestelmän omistajuuteen liittyvät tiedot dokumentoidaan keskitetysti rekisteri- ja tietojärjestelmäselosteisiin sekä tietohallinnon ylläpitämään tietojärjestelmäluetteloon.

Tietojärjestelmän omistajan on huolehdittava tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsynvalvonnasta sekä tuottamaan lakisääteiset seurantaraportit. Jokaiselle tietojärjestelmälle on nimettävä pääkäyttäjä, jonka vastuulla on huolehtia järjestelmän käyttöoikeuksista.

Pääkäyttäjältä vaaditaan hyvää tietoturva- ja tietosuojaosaamista. Lisäksi tiedon omistajien ja pääkäyttäjien on huolehdittava tiedon koko elinkaaren hallinnasta ja ICT-varautumissuunnitelmista, missä kuvataan vastuuhenkilöt, roolit ja toimintamallit riskien toteutumisen varalta. Tietohallinnon vastuulla on järjestää tukitoimintoja ja tarvittavia koulutuksia edellisten toteuttamiseksi.

Esimiesten vastuulla on huolehtia ja noudattaa työnantajaa koskevien lakisääteistein tietoturva ja tietosuoja velvoitteiden toteutumista. Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa. Lisäksi he huolehtivat loppukäyttäjän riittävästä perehdytyksestä konsernin tietoturvakäytänteisiin varmistaen,

että jokainen ymmärtää niiden merkityksen työtehtävissään. Esimiesten ja pääkäyttäjien vastuulla on myös huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa ja työsuhteen päättyessä työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden sekä käyttöoikeudet tietojärjestelmistä poistetaan.

Esimiehiltä odotetaan esimerkillistä sekä vastuullista tietoturvakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvapoikkeamista tietohallinnon vastuuhenkilölle.

Kunnan työntekijän velvollisuus on allekirjoittaa tietoturva- ja käyttäjäsitoumus. Työntekijällä on vastuu noudattaa hyväksyttyjä tietoturvaohjeita ja huolehtia päivittäisissä työtehtävissä hyvän tiedonhallintatavan käytänteistä. Työntekijän vastuulla on myös huolehtia käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokittelusta sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä. Tietojen säilytys- tai arkistointiajan päätyttyä ne on hävitettävä ohjeiden mukaisesti.

Työntekijällä on velvollisuus raportoida tietoturvaongelmista oman organisaation tietosuojavastaavalle, esimiehelle tai suoraan tietohallinnon vastuuhenkilölle.

Ostopalveluna hankitun ICT–palvelun operatiivisesta ja teknisestä tietoturvasta ja sen ohjeistamisesta vastaavat palveluntuottajat, joille palvelun toteutus on sopimuspohjaisesti luovutettu. ICT-palveluiden tuottajien tehtävänä on laatia ja ylläpitää keskitetysti tietohallinnon hyväksymien palvelukonseptien mukaisia käytännön tietoturvaohjeita.

Tilaajan tulee huolehtia, että kaikkiin tarjouspyyntöihin ja palvelusopimuksiin sisällytetään tietohallinnon ylläpitämät yleiset tietoturvavaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla sekä häiriötilanteiden toimintamallit ja selkeä vastuunjako läpi koko palveluketjun. Tilaajan tehtävä on huolehtia ja vaatia palvelutuottajaa raportoimaan ja tiedottamaan merkittävistä tietoturvaan kohdistuvista poikkeustilanteista, riskitekijöistä sekä uhkatilanteista välittömästi palvelusopimuksessa määritellyille yhteyshenkilöille.

8. Tietojärjestelmien käyttö

Kunnan käytössä olevat ICT-palvelut, -järjestelmät, -laitteet ja -ohjelmistot, on tarkoitettu työtehtävien hoitamista varten. Kunnan tietojärjestelmiä ei tule käyttää toimintaan mikä saattaa, välittömästi tai välillisesti, vaarantaa kunnan vastuulla olevan tiedon ja/tai järjestelmien turvallisuuden ja aiheuttaa haittaa kunnalle, sen toiminnalle tai käyttäjälle itselleen.

Tietojärjestelmien vähäinen käyttö henkilökohtaisiin tarkoituksiin on sallittu omalla ajalla. Henkilökohtainen käyttö ei kuitenkaan saa aiheuttaa ylimääräisiä kustannuksia kunnalle, eikä vaarantaa kunnan tietoa tai tietojärjestelmiä.

Tietojärjestelmiä, laitteita ja ohjelmistoja kunnan tietoverkkoon saa asentaa vain tietohallinto tai sen valtuuttama taho.

Käyttöoikeudet kunnan tietojärjestelmiin ja tietoon myönnetään vain kunnan tehtävien hoitoon liittyen. Pääsääntöisesti tarvittavat oikeudet määrittelee esimies.

Tietojärjestelmien turvallinen käyttäminen etätyötä tehdessä vaati etätyöntekijältä erityistä huolellisuutta ja sitoutumista tietoturvaohjeiden noudattamiseen.

Väärinkäytöksiin puututaan välittömästi kunnan normaalein kurinpitomenettelyin.

Kunnan tietoverkkojen toimintaa valvotaan erityisillä valvontamenetelmillä ja -ohjelmistoilla. Toiminnan ja turvallisuuden takaamiseksi tietoliikenteestä suodatetaan palomuurijärjestelmän avulla haittaohjelmat ja muu asiaton sisältö sekä estetään pääsy haitalliseksi luokitelluille sivustoille.

9. Tietoturvakoulutus ja –ohjeet sekä selosteet
Esimiehen vastuulla on huolehtia, että kaikilla työntekijöillä on riittävä koulutus tietoturvasta. Mikäli henkilön työtehtäviin kuuluu olennaisena osana henkilötietojen käsittely, niin osastopäällikön tulee edellyttää, että työntekijä suorittaa hyväksytysti kulloinkin voimassa oleva tietoturva- tai tietosuojakoulutuksen säännöllisin väliajoin.

Tietoturvallisuuteen liittyvät oppaat, säännöt ja materiaalit ovat työntekijöiden luettavissa sisäverkossa sekä kunnan kotisivuilla. Hyvällä perehdyttämisellä luodaan työviihtyvyyttä ja -turvallisuutta. Uuden henkilön perehdyttämisestä huolehtii lähin esimies.

Tietojärjestelmien ja henkilörekistereiden selosteet on toimitettava asianhallintasihteerille. Selosteet on nähtävissä kunnan sisäisessä verkossa.

10. Tietoturvallisuudesta tiedottaminen ja sen toteutumisen valvonta
Ennalta tiedetyistä palvelukatkoksista tiedotetaan hyvissä ajoin ennen katkosta.

Havaitusta väärinkäytöksestä tai pistokokeena havaitusta väärinkäytöksestä raportoidaan ja tiedotetaan lähintä esimiestä.

Tietoturvallisuuden toteutumista valvotaan osana sisäistä valvontaa.

11. Henkilötietojen tietoturvaloukkaus
Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi hävinnyt USB-tikku, varastettu tietokone, hakkerointi, haittaohjelmatartunta, kyberhyökkäys, tulipalo datakeskuksessa tai tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkaus edellyttää rekisterinpitäjän edustajalta kykyä arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu tietoturvaloukkauksen kohteena olleille henkilöille. Arvion johtopäätös voi olla esimerkiksi se, että tietoturvaloukkauksesta ei aiheudu riskiä, aiheutuu riski tai aiheutuu korkea riski. Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä (esimerkiksi tietoturvaloukkauksen dokumentointi, ilmoitus valvontaviranomaiselle tai ilmoitus rekisteröidylle).

Rekisterinpitäjän edustajan on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa.

Rekisterinpitäjän edustajan on ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle, jos siitä voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Henkilötietojen käsittelijän tulee ilmoittaa tietoturvaloukkauksesta rekisterinpitäjälle, jollei ole erikseen sovittu, että käsittelijä voi ilmoittaa tietoturvaloukkauksista suoraan valvontaviranomaiselle asetuksen edellyttämällä tavalla. Vastuu ilmoitusvelvollisuuden toteuttamisesta on rekisterin vastuuhenkilöllä.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Rekisterin vastuuhenkilön on ilmoitettava asiasta silloin ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojata itseään esimerkiksi sulkemalla luottokorttinsa.

12. Toiminta normaaliolojen häiriötilanteissa, poikkeustilanteissa ja -oloissa

Kunta pyrkii varmistamaan toimintansa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Poikkeusoloja varten kunta ylläpitää valmiussuunnitelmaa.

Normaaliolojen häiriötilanteita pyritään ennaltaehkäisemään ja toipumisaikoja lyhentämään pitämällä järjestelmiä ja laitteita mahdollisimman ajantasaisina. Kriittisille laitteille hankitaan varalaitteita.

Poikkeustilanteessa varautumista johtaa ja valvoo valtioneuvosto sekä kukin ministeriö toimialallaan. Tietohallinnon osalta poikkeusolojen valmiussuunnitelmaa päivitetään säännön mukaisesti.