Laatija	pvm
Päivi Vauhkonen	3.9.2019
Päivittäjä	pvm
IT-ryhmä	13.9.2019
Hyväksyjä	pvm
Kunnanhallitus	23.9.2019 § 207
Asiakirjan sijainti	

Tietoturvapolitiikka

1 Johdanto

Pelkosenniemen kunnan palvelutuotannon ja muun toiminnan ja keskeisimpiä resursseja on tieto. Kunnan tiloissa ja niiden ulkopuolella tietoa käsittelevät kunnan henkilöstön lisäksi ulkoiset sidosryhmät ja asiakkaat. Tietoa esiintyy muiden muassa paperille tulostettuna, tallennettuna tietojärjestelmiin, kannettaviin laitteisiin ja muistivälineille sekä käyttäjien muistiin tallentuneena. Tiedon sijainnista ja olomuodosta riippuen, sitä pyritään turvaamaan hallinnollisin ja/tai teknisin menetelmin.

Kunnanhallitus on hyväksynyt kunnan johtoryhmän tässä tietoturvapolitiikassa kuvaamat, kunnan strategian mukaiset periaatteet, tavoitteet ja vastuut. Tietoturvapolitiikan onnistuneen käyttöönoton edellytyksenä on, että kunnan ylin johto sitoutuu toteuttamaan tätä politiikkaa yhdessä osaavan ja tietoturvallisuuteen perehdytetyn henkilöstön sekä sidosryhmien kanssa.

2 Tietoturvapolitiikan kattavuus ja sen soveltaminen

Tämä tietoturvapolitiikka kattaa kaiken kunnan käyttämän tiedon riippumatta esitystavasta tai elinkaaren vaiheesta ja toimii perustana muille tietoturvaan liittyville ohjeille ja määräyksille.

Lisäksi politiikka koskee jokaista kunnan kanssa palvelussuhteessa olevaa viranhaltijaa, työntekijää ja määräaikaista henkilöä, harjoittelijaa sekä luottamushenkilöä ja tarvittavilta osin yhteistyökumppania.

Politiikka saatetaan koko henkilöstön tietoon kunnan perehdytys- ja koulutuskäytäntöjen avulla. Yhteistyökumppanien ohjeistamisesta vastaa tilaaja. Periaatteena on, että kaikki jotka käsittelevät kunnan tietoa, ovat saaneet riittävän perehdytyksen tiedon turvallisen käsittelyn varmistamiseksi.

3 Tietoturvallisuus

Kunnassa tietoturvallisuudella tarkoitetaan tiedon, tietojärjestelmien, tietoliikenteen ja palveluiden, sekä niiden käyttöympäristöjen ja käyttäjän itsensä turvaamista siten, että niihin kohdistuvat uhat eivät aiheuta merkittävää riskiä tiedon elinkaaren missään vaiheessa.

Periaatteena on, että tietoturvallisuus on luonnollinen, sisäänrakennettu osa kunnan palveluita ja toimintaa sekä jokaisen käyttäjän työtapoja. Tietoturvallisuuteen liittyvillä käytännöillä pyritään varmistamaan, että kunnan käyttämä tieto on:

- oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena
- vain siihen oikeutettujen saatavilla
- saatavilla aina sitä tarvittaessa.

Lisäksi tietoon sen käsittelyn eri vaiheissa tehdyt muutokset on tarvittaessa kyettävä todentamaan. Kunnan tietoturvallisuuteen liittyvää toimintaa johdetaan ja kehitetään osana kunnan hallintojärjestelmää ja se liittyy kiinteästi kunnan kokonaisturvallisuuteen, joka muodostuu seuraavista osa-alueista:

- **Turvallisuusjohtaminen** on turvallisuuden toteutumisen ohjaamista ja valvomista kaikilla turvallisuuden osa-alueilla, mukaan lukien riskienhallinta ja varautuminen.

- **Henkilöstöturvallisuus** on henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa. Henkilöstöturvallisuuden perustana on osaava ja sitoutunut henkilöstö, jolle tietoturvavastuut ja -tehtävät on selkeästi perehdytetty. Henkilöstöturvallisuuteen pyritään vaikuttamaan palvelussuhteen kaikissa vaiheissa – rekrytointivaiheessa, työsuhteen aikana ja työsuhteen päätyttyä tehtävillä toi-menpiteillä.
- **Fyysinen turvallisuus** käsittää toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja, ja siellä olevia ihmisiä, tietoa ja muuta omaisuutta, suojataan fyysisiltä vahingoilta, vahingoittamisyrityksiltä, oikeudettomilta henkilöiltä ja erilaisilta kiinteistövahingoilta. Fyysistä turvallisuutta toteute-taan mm. vartioinnilla, kameravalvonnalla, kulunvalvonnalla ja turvallisilla rakenteilla.
- **Tietosuoja** tarkoittaa henkilön yksityisyyden ja henkilötietojen suojaamista niin, että henkilön yksilöiviä tietoja ei paljastu asiattomille käsittelyprosessin missään vaiheessa. Kuntalaisia koskevat yksilöivät henkilötiedot ovat kunnan keskeisimpiä suojattavia tietoja ja vaativat siten käsittelijöiltä erityistä huomiota.
- **Työturvallisuus ja -suojelu** kattavat sekä henkilöstöön kohdistuvien että henkilöstön aiheuttamien, tahallisten ja tahattomien, vahingontekojen estämiseen tähtäävät toimenpiteet.
- Perustana kunnan tietoturvatyössä käytetään ensisijassa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) suosituksia ja Tietoturvatasojen kuvaaman Perustason vaatimuksia (LIITE 1: Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010).

4 Tietoturvallisuustavoitteet

Kunnan tietoturvallisuustavoitteet ovat tärkeysjärjestyksessä seuraavat:

1. Kunnan henkilökunnalla on vähintään Tietoturvatasojen Perustason tietoturva- ja tietosuoja-osaaminen tehtäviensä suorittamiseksi.
2. Tekniset ja hallinnolliset tietoturvajärjestelyt täyttävät keskeisiltä osin Perustason vaatimukset.
3. Kunnan käyttämää tietoa ei paljastu tietoon oikeudettomille tahoille.

5 Roolit ja vastuut

Kunnan tietoturvallisuuteen liittyvät roolit ja vastuut ovat seuraavat:

Kunnanhallitus

- Tietoturvapolitiikan hyväksyminen

Kunnanjohtaja

- Tietoturvan ja tietosuojan järjestäminen ja toimintaedellytysten luominen
- Poikkeusolojen viestinnän johtaminen
- Varautuminen ja jatkuvuudenhallinta yhdessä kunnan johtoryhmän kanssa
- Tietoturvaohjeiden ja muiden vastaavien ohjeiden vahvistaminen

Toimialajohtajat

- Omistajan nimeäminen tietojärjestelmille
- Tietoturvallisuuden toteutuminen omalla toimialallaan

IT-ryhmä

- 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 kunnanjohtajalle

Hallintojohtaja
- Kunnan tietouden ylläpitäminen koskien tietoturvallisuuteen vaikuttavia lakeja, säädöksiä ja määräyksiä, sekä huolehtiminen niiden huomioimisesta tietoturvallisuustoiminnassa
- Henkilöstöturvallisuuden ja henkilöstötietojen käytön ohjaus ja koordinointi työntekijän palvelussuhteen kaikissa vaiheissa

Tietosuojavastaava ja tietosuojavastuuhenkilöt
- Auttavat rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja mahdollisten erityislakien edellyttämän tietosuojan tason
- Tietosuojavastaava toimii yhteyshenkilönä valtakunnalliseen tietosuojavaltuutettuun ja tekee tarvittaessa ilmoitukset tietosuojaloukkauksista

Tietojärjestelmän, tiedon tai prosessin omistaja
- Omistamaansa tai hallinnoimaansa järjestelmään, tietoon tai prosessiin liittyvä:
- Pääkäyttäjän nimeäminen ko. järjestelmän osalta
- Käyttäjien ja käyttöoikeuksien hyväksyntä ko. järjestelmään
- Riskien- ja jatkuvuudenhallintatoimenpiteiden toteuttaminen omalta osaltaan
- Tiedon oikeellisuuden ja oikeiden käsittelytapojen varmistaminen
- Tietojen julkisuuden ja salassapidon määrittely mukaan lukien arkistonmuodostus

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

Esimies
- Tietoturvallisuuden toteutuminen alaisessaan toiminnassa

Tiedon ja tietojärjestelmien käyttäjä
- Määräysten ja ohjeiden noudattaminen sekä tietoturvaan liittyvien poikkeuksien, uhkien ja riskien välitön ilmoittaminen joko esimiehelle, tietohallintoon tai tietosuojavastaaville

Asianhallintatiimi
- Yksiköiden arkistonmuodostuksen ohjaaminen ja neuvonta
- Kunnanarkistoon siirretyistä asiakirjoista huolehtiminen ja niistä tietojen antaminen

6 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 hallinnon käytössä olevaan 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.

7 Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Tietoturvallisuuden ylläpito ja kehittäminen sovitetaan yhteen palveluiden, toimintatapojen ja teknisten ratkaisujen kehittämisen kanssa. Lisäksi säännöllinen tiedottaminen, osaamisen ylläpito ja koulutus ovat olennaisessa roolissa tietoturvallisuuden kehittämisessä.

8 Riskienhallinta

Tietoturvallisuus on kiinteä osa kunnan riskienhallinta-käytäntöjä ja kuuluu jokaisen työntekijän vastuulle. Riskienhallinnan avulla palveluihin, toimintaan ja tietoon kohdistuvia riskejä kartoitetaan, analysoidaan ja hallitaan järjestelmällisesti.

Riskienhallintakäytäntöjen tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että käy-tetyt keinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen.

9 Jatkuvuudenhallinta ja varautuminen

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