Pyhännän kunnan tietoturvapolitiikka

Kunnanvaltuusto: 17.12.2018 §
Kunnanhallitus: 10.12.2018 § 183

SISÄLTÖ

1. Johdanto

Tietoturva on Pyhännän kunnassa kiinteä osa päivittäistä toimintaa, ja lähtökohta luottamukselliselle viranomaistoiminnalle. Tietoturvapolitiikassa määritellään mitä tietoturva Pyhännän kunnassa tarkoittaa. Lisäksi politiikassa kuvataan kunnan keskeiset tietoturvaperiaatteet, -tavoitteet, -roolit ja –vastuut.

Tietoturvapolitiikka katselmoidaan ja päivitetään tarvittavilta osin vuosittain. Dokumentti on kokonaisuudessaan saatavilla kunnan internet-sivuilla.

2 Tietoturvapolitiikan tarkoitus ja tausta

Tämä politiikka toimii kunnan ylimpänä turvallisuusasiakirjana. Kunnan tietoturvapolitiikka kuvaa tietoturvan roolin kunnan toiminnoissa ja palveluissa, perustuen tehtyihin riskiarvioihin ja toimintaa säätelevien lakien vaatimuksiin.

3. Keitä tietoturvapolitiikka koskee

Tämä tietoturvapolitiikka on kunnanhallituksen hyväksymä ja koskee koko kuntakonsernia (jokaista palvelussuhteessa olevaa viranhaltijaa, työntekijää ja määräaikaista henkilöä, harjoittelijaa sekä luottamushenkilöä) sekä niitä sidosryhmiä (yhteistyö- ja sopimuskumppanit), jotka käsittelevät kunnan omistamaa tai hallinnoimaa tietoa.

Politiikassa esitetyt periaatteet ja käytännöt koskevat kaikissa elinkaaren vaiheissa (luonti, säilytys, siirto, poisto) ja kaikissa muodoissa (mm. paperinen, sähköinen, optinen, puhuttu) olevaa tietoa.

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.

4. Tietoturvallisuus

Tietoturvallisuus kattaa tietoturvaan ja tietosuojaan liittyvät toteutukset. Tietoturvalla kunnassa tarkoitetaan kaikissa muodoissa olevan tiedon (sekä tietojärjestelmien, tietoliikenteen, palveluiden ja niiden käyttöympäristöjen) turvaamista siten, että tiedon luottamuksellisuus, eheys ja saatavuus kyetään varmistamaan.

Tietosuojalla kunnassa tarkoitetaan henkilön yksityisyyden ja henkilötietojen suojaamista niin, että henkilön yksilöivää tietoa ei paljastu siihen oikeudettomille tiedon elinkaaren missään vaiheessa. (Henkilötietolaki 22.4.1999/523).

Periaatteena on, että tietoturvallisuuskäytännöt kattavat kaikki kunnan tietojenkäsittelytehtävät sisältäen myös asiakirjahallinnon sekä arkistoinnin ottaen huomioon toimialojen ja työyksiköiden perusluonteen ja tietoturvatarpeet. Tietoturvallisuus pyritään integroimaan kiinteästi kunnan palveluihin ja toimintaan, sekä jokaisen käyttäjän työtapoihin.

Tietoturvallisuutta toteutetaan käytännössä seuraavilla:

- **Asenne:** Tiedon käsittelijä ymmärtää tietoturvan merkityksen ja omat vastuunsa, sekä on motivoitunut noudattamaan tätä politiikkaa sekä tästä politiikasta johdettuja tietoturvaohjeita ja –määräyksiä.
- **Eheys:** Tieto, tietojärjestelmät ja paperiasiakirjojen arkistot ovat luotettavia, oikeellisia ja ajantasaisia. Toisin sanoen tieto ei ole muuttunut teknisen vian seurauksena tai tietoa ei ole muutettu ihmisen toimesta tahallisesti tai tahattomasti.
- **Kiistämättömyys:** Tiedonkäsittelytoimenpiteiden suorittamista siten, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana että jälkikäteen.
- **Luottamuksellisuus:** Tieto on vain siihen oikeutettujen saatavissa eikä sitä paljasteta tai muutoin saateta sivullisten tietoon. Tiedon käsittelyssä noudatetaan julkisuuslakia sekä erikseen, toiminnottain/järjestelmittäin, hyväksyttyjä tietojen turvaluokituksien mukaisia sääntöjä ja ohjeita.
- **Pääsynvalvonta:** Tietoa ja tietojärjestelmää ei voi käyttää ilman lupaa ja ettei arkistotiloihin tai vastaaviin pääse ilman kontrolloitua pääsynvalvontaa.
- **Saatavuus:** Tieto ja tietojärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille ja tietojärjestelmille, sovituilla tavoilla ja sovittuun aikaan.

Kunnan tietoturvatyön periaatteet ja toteutukset perustuvat ensisijassa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeisiin ja suosituksiin, Tietoturvatasojen määrittelemiin Perustaso –vaatimuksiin (Tietoturvallisuusasetus 681/2010) ja tietosuojavaltuutetun toimiston antamiin ohjeisiin. Tietoturvatoteutukset koskien henkilöstö-, tietoaineisto-, tietoliikenne-, laitteisto-, ohjelmisto, käyttö- ja fyysistä turvallisuutta kuvataan tietoturvallisuussuunnitelmassa. (tietosuoja direktiivi (EU) 2016/680 ja tietosuoja-asetus (EU) 2016/679)

5. Kokonaisturvallisuus

Kunnan kokonaisturvallisuus koostuu riskienhallintaan, varautumiseen ja turvallisuuteen liittyvistä prosesseista ja niiden toteutuksista. Tietoturvapolitiikka on osa kunnan kokonaisturvallisuuden hallintaa.

6. Riskienhallinta

Riskienhallinta toimii kunnan kokonaisturvallisuuden perustana. Riskienhallinnan avulla kunnan palveluihin ja toimintoihin kohdistuvia riskejä hallitaan järjestelmällisesti ja koko organisaation laajuisesti. Riskienhallinta kuuluu jokaisen työntekijän vastuulle.

7. Varautuminen ja jatkuvuudenhallinta

Pyhännän kunta on varautunut erilaisiin, toimintaa häiritseviin tai toiminnan keskeyttäviin uhkatilanteisiin, kriiseihin ja niistä toipumiseen ennakolta. Tämä tapahtuu kehittämällä ja ylläpitämällä seuraavia varautumiseen ja jatkuvuudenhallintaan liittyviä suunnitelmia:

- **Valmiussuunnitelma** toiminnan, palveluiden ja järjestelmien hallinnoimiseksi poikkeusoloissa joka sisältää:
    - **Jatkuvuussuunnitelmat** toiminnan kannalta kriittisille palveluille ja toiminnoille niiden jatkuvuuden turvaamiseksi
    - **Toipumissuunnitelmat** kriittisille tietojärjestelmille ja –verkoille niiden mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi
    - **Lakisääteiset pelastussuunnitelmat** ihmisten ja omaisuuden suojelemiseksi, sekä vahinkojen minimoimiseksi onnettomuustilanteissa.

8. Turvallisuus

Tietoturvan ja tietosuojan ohella keskeisempiä turvallisuuden osa-alueita kunnassa ovat:

Turvallisuusjohtaminen on turvallisuuden toteutumisen ohjaamista ja valvomista kaikilla tietoturvaprosessin kuvaamilla osa-alueilla.

Henkilöstöturvallisuus on kunnan ja sidosryhmien henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskienhallintaa. Periaatteena on, että tietoturva huomioidaan työ- / virkasuhteen kaikissa vaiheissa.

Fyysinen turvallisuus koostuu järjestelyistä, joilla kunnan tiloja, ihmisiä, tietoa ja muuta omaisuutta suojataan vahingoilta ja vahingoittamisyrityksiltä.

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.

9. Tietoturvatavoitteet

Hyväksyessään tietoturvapolitiikan kunnanhallitus asettaa seuraavat, kuntastrategiaa tukevat ja koko organisaatiota koskevat pitkän tähtäimen tietoturvatavoitteet:

1. Osaava ja hyvinvoiva henkilöstö: Koko kunnan henkilökunta ja luottamushenkilöstö on osallistunut ”Arjen Tietosuoja” –koulutukseen.
2. Kuntalaiset ja sidosryhmät asiakkaina ja toimijoina: Salassa pidettävää tai luottamuksellista tietoa ei paljastu tietoon oikeudettomille
3. Tietoturvan hallinnolliset ja tekniset järjestelyt täyttyvät keskeisiltä osin Tietoturvatasojen Perustaso –vaatimukset (Tietoturvallisuusasetus 681/2010).

10. Roolit ja vastuut

Tietoturvan toteuttaminen on jatkuvaa, laaja-alaista ja kaikille toimijoille kuuluvaa toimintaa. Periaatteena on, että tietoturvan toteuttamiseen osallistuvat kunnan ja sidosryhmien henkilöstö, osana omaa yleistä toimintavastuutaan. Käytännössä tämä tarkoittaa hyvien tiedonhallintatapojen, tietoturvamääräysten ja –ohjeiden noudattamista, sekä tietoturvan huomioimista kaikessa tekemisessä.

Ylin vastuu tietoturvasta, riskienhallinnasta ja varautumisesta on kunnanhallituksella. Tietoturvan ohjaus- ja kehittämistyössä tarvittava muu erityisasiantuntemus ja nimetyt turvallisuusvastuut kuvataan alla.

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.

Osastojen/Yksiköiden päälliköt: Tietoturvallisuuden toteutuminen omalla toimialallaan.

Tietoturvatyöryhmä: 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.

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

Tietojärjestelmän, tiedon tai prosessin omistaja: Omistamaansa tai hallinnoimaansa järjestelmään, tietoon tai prosessiin liittyvä: Pääkäyttäjän nimeäminen ko. järjestelmän osalta, Käyttäjien ja käyttö-

oikeuksien 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 käytetään 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, tietoturvatyöryhmä, ICT-vastuuhenkilöille tai tietosuojavastaavalle

Keskusarkistonhoitaja: Yksiköiden arkistonmuodostuksen ohjaaminen ja neuvonta, kunnanarkistoon siirretyistä asiakirjoista huolehtiminen ja niistä tietojen antaminen

11. Tietojärjestelmien käyttö

Kunnan periaatteiden mukaisesti tietojärjestelmät ovat tarkoitettu työtehtävien hoitamiseen eikä niitä tule käyttää kunnan omistaman tai hallinnoiman tiedon vaarantumiseen johtavaan toimintaan. Kunnalle tai sen toiminnalle mahdollisesti aiheutetun haitan korvausvastuussa on ensisijassa vaarantumisen aiheuttaja.

Käyttäjien toimintaa ohjataan tästä politiikasta johdetuilla tietoturvamääräyksillä ja –ohjeilla. Tiedon ja tietojärjestelmien väärinkäyttöön puututaan kunnan normaalein kurinpitomenettelyin.

12. Tietoturvan seuranta, ylläpito ja kehittäminen

Kunnan tietoturvatavoitteiden toteutumista seurataan säännöllisesti. Seuranta perustuu talousarvio- ja toimintasuunnitelman mukaisiin mitattaviin tavoitteisiin ja raportointikäytäntöihin, sekä yhteisesti sovittuihin teknisen valvonnan keinoihin. Organisaatiolle laaditaan tietotilinpäätös, joka on osa tietojohtamista, riskienhallintaa ja sisäistä valvontaa. Tietotilinpäätös toimitetaan vuosittaisena tiedoksiantona tarkastuslautakunnalle, kunnanhallitukselle ja kunnanjohtajalle.

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.

Tietoturvan ylläpidossa ja kehittämisessä keskeisessä roolissa on osaaminen, mitä toteutetaan säännöllisillä koulutus- ja viestintäkäytännöillä. Tässä politiikassa kuvatut määräykset ja periaatteet koulutetaan koko kunnan henkilöstölle ja luottamushenkilöstölle perehdytysprosessien mukaisesti.

Tarvittavien ulkoisten sidosryhmien tietoturvaosaamisesta vastaa kyseisen toimialan johto. Periaate on, että kaikki jotka käsittelevät kunnan omistamaa tai hallinnoimaa tietoa saavat riittävät edellytykset tiedon asianmukaiseen käsittelyyn.

Tietoturvatoteutukset sekä asetettujen tietoturvatavoitteiden edellyttämät hallinnolliset, fyysiset ja tekniset ratkaisut kuvataan tietoturvallisuussuunnitelma ja –ohjeessa.