Janakkala

JANAKKALAN KUNNAN TIETOTURVAPOLITIIKKA

Kunnanhallituksen esityslistan liite
14.8.2023

Sisällysluettelo

Janakkalan kunnan tietoturvapolitiikka

Tämä asiakirja korvaa kunnanhallituksen 13.4.2015 (§ 81) hyväksymän tietoturvapolitiikan.

Johdanto

Tietoturvapolitiikan tarve ja tarkoitus

Janakkalan kunnan toiminta ja palvelutuotanto perustuvat suuressa määrin tietoon ja sen luotettavaan hallintaan. Kunta käsittelee tietoa monessa eri muodossa – muun muassa tietojärjestelmiin tallennettuna ja sähköisillä viestimillä siirtäen, paperille kirjattuna, suullisesti ja joskus jopa vain ihmismuistin varassa. Viranomaisena ja usean eri henkilötietovarannon rekisterinpitäjänä kunnalla on myös monia säädöksissä asetettuja tiedonhallinnan vastuita.

Kunnan vastuulla olevien tietojen käsittely on varsin moninaista. Tietoja käsittelevät oman henkilöstön ja luottamushenkilöiden ohella myös kunnan ulkoiset asiakkaat ja sidosryhmät. Tekoälytekniikan kehitys voi lähitulevaisuudessa lisätä myös täysin automaattisen tiedonkäsittelyn osuutta. Käsittelyä tehdään sekä kunnan tiloissa, että niiden ulkopuolella monenlaisilla välineillä, joista kaikki eivät välttämättä ole kunnan kontrolloitavissa. Tietoja voidaan käsitellä myös tavanomaisten työaikojen ulkopuolella, sillä monet kunnan ja sidosryhmien sähköiset asiointipalvelut ovat käytettävissä mihin aikaan vuorokaudesta tahansa.

Tämä tietoturvapolitiikka on kunnan johdon näkemys ja tahdonilmaisu siitä, miten tietojenkäsittelyn turvallisuus tulee kunnassa varmistaa. Politiikka esittää kunnan olennaiset tietoturvallisuuden tavoitteet ja periaatteet sekä antaa suuntaviivat näiden soveltamiselle erilaisissa käytännön tilanteissa. Samalla politiikka ilmaisee kunnan johdon halun sitoutua tietoturvallisuuteen kunnan toimintaa koskevien säädösten ja hyvien käytäntöjen mukaisesti. Vastaavaa sitoutumista johto edellyttää muiltakin kunnassa ja sen kanssa työskenteleviltä.

Kattavuus ja soveltamisala

Tietoturvapolitiikka koskee kaikkea kunnan omistamaa tai muulla perusteella käsittelemää tietoa riippumatta

- välineestä, jolla tietoa käsitellään
- esitystavasta tai teknisestä muodosta, jossa tietoa käytetään, siirretään tai tallennetaan
- tiedon elinkaaren vaiheesta
- suojausluokituksesta tai muulla tavoin määräytyvästä suojaamisen tarpeesta.

Politiikka kattaa kaiken tyyppiset tietosisällöt estämättä sitä, että joillekin tietosisällöille tai tietojenkäsittelytilanteille voidaan asettaa myös muista poikkeavia tavoitteita tai vaatimuksia. Esimerkiksi henkilötietojen käsittelyyn kohdistuu monia säädöksiin (mm. EU:n yleisen tietosuoja-asetukseen, GDPR) perustuvia vaatimuksia ja rajoituksia, jotka eivät kohdistu kaikkeen tiedonhallintaan.

Tietoturvapolitiikka koskee kunnan koko organisaatiota – ml. henkilöstöä palvelussuhteen kestosta tai tyypistä riippumatta sekä luottamuselinten jäseniä – sekä niitä konserniyhtiöiden tai muiden sidosryhmien edustajia, jotka asiakkuuden, sopimuksen tai muun yhteistyösuhteen nojalla käsittelevät kunnan omistamaa tai hallinnoimaa tietoa. Politiikka on perusta tietoturvallisuutta koskeville soveltaville ohjeille, joiden tehtävänä on konkretisoida ja toteuttaa politiikassa ilmaistujen periaatteiden noudattaminen ja tavoitteiden saavuttaminen käytännössä.

Tietoturvallisuus ja sen lähikäsitteet

Tieto-, digi- ja kokonaisturvallisuus

Tietoturvallisuudella tarkoitetaan vakiintuneesti seuraavien kolmen tiedon hallintaan liittyvän seikan varmistamista:

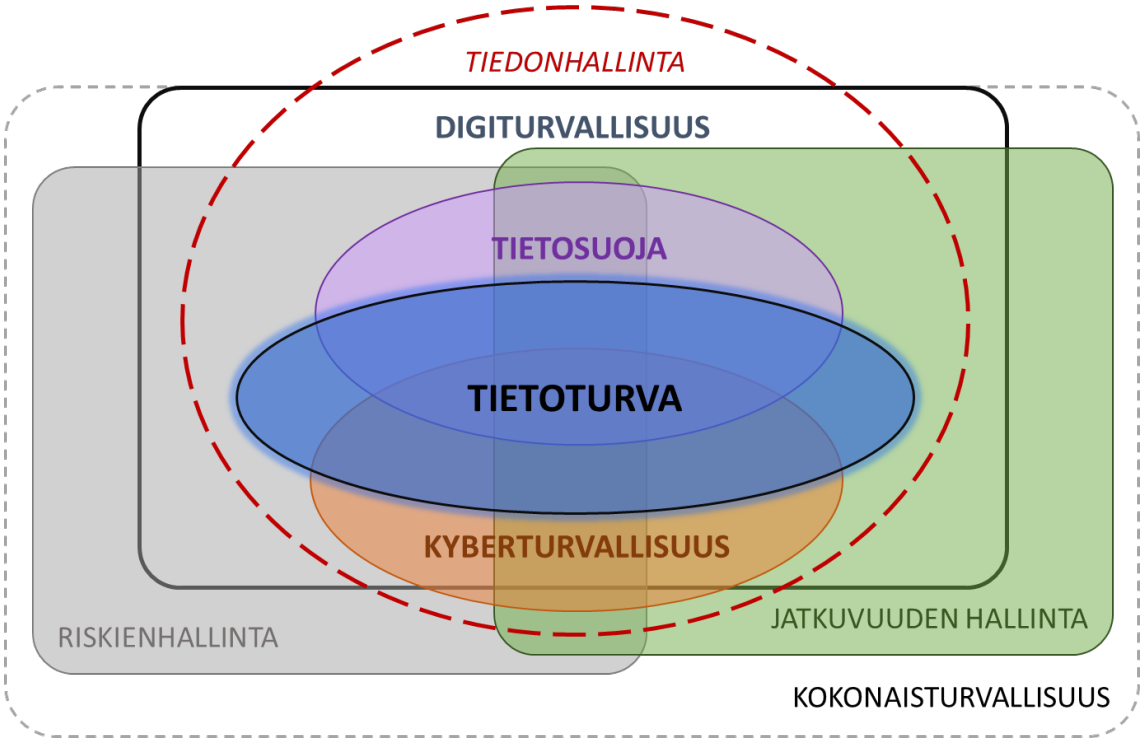
1. **eheys**: että tieto on oikeaa (todenmukaista), ajan tasalla ja käyttötarkoituksensa kannalta sopivassa muodossa
2. **luottamuksellisuus**: että tieto on vain niiden saatavilla, jotka ovat sen käyttöön oikeutettuja
3. **saatavuus**: että tieto on käytettävissä häiriöttömästi silloin, kun sitä tarvitaan

Tietoturvallisuutta on lisäksi se, että tietoon sen käsittelyn eri vaiheissa tehdyt muutokset voidaan tarvittaessa jäljittää ja tietoa käsitelleiden henkilöllisyys tarvittaessa todentaa.

Tietoturvallisuus-käsitteen rinnalla puhutaan usein myös digiturvallisuudesta ja kyberturvallisuudesta. Näiden ja eräiden muiden toisilleen läheisten käsitteiden suhdetta havainnollistaa kuva 1.

Kyberturvallisuudella viitataan yleensä erityyppisistä ja toisistaan riippuvaisista tietoteknisistä järjestelmistä ja palveluista muodostuvan kokonaisuuden turvallisuuteen. Tämä näkökulma sopii esimerkiksi yhteiskunnan elintärkeiden toimintojen tarkasteluun.

Digiturvallisuus-käsitteen piiriin luetaan perinteisen tietoturvallisuuden ohella tietosuoja ja kyberturvallisuus sekä näiden huomiointi organisaation riskienhallinnassa ja toiminnan jatkuvuuden hallinnassa. *Digi*-etuliitteestä huolimatta digiturvallisuuden käsite on siis varsin laaja, eikä sitä pidä rajata vain digitaalisessa muodossa olevan tiedon käsittelyyn. Sen sijaan se voidaan ajatella laaja-alaiseksi tiedonhallinnan turvallisuuden varmistamiseksi *digitalisoituvassa toimintaympäristössä*.



Kuva 1. Tietoturva lähikäsitteineen.

Digitaalisen tiedonhallinnan turvallisuuden varmistamisessa keskeisiä osa-alueita ovat

- ohjelmistoturvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- tietoaineistojen turvallisuus

Tieto- ja digiturvallisuus ovat myös erottamaton osa modernin organisaation ***kokonaisturvallisuutta***, johon kuuluu muutakin kuin tiedonhallinnallisia elementtejä ja tavoitteita. Näitä ovat esimerkiksi

- *turvallisuusjohtaminen*: turvallisuuden toteutumisen ohjaus ja valvonta kaikilla turvallisuuden osa-alueilla, mukaan lukien riskienhallinta ja varautuminen
- *henkilöstöturvallisuus*: henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa
- *työturvallisuus ja -suojelu*: henkilöstöön kohdistuvien tai henkilöstön (tahallisesti tai tahattomasti) aiheuttamien vahingontekojen estämiseen tähtäävät toimenpiteet
- *fyysinen turvallisuus*: 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.
- *tietosuoja* (ks. kohta 2.2).

Tietosuoja ja yksityisyyden suoja

Tietosuoja tarkoittaa erityisesti henkilötietojen käsittelyyn liittyvää yksityisyyden kunnioittamista, jota toteutetaan suojaamalla henkilötiedot oikeudettomalta ja tarpeettomalta käsittelyltä. Tietosuojan keskeisiä käsitteitä ovat *rekisteröity* eli henkilö, jota koskevia tietoja käsitellään, ja *rekisterinpitäjä* eli organisaatio tai muu toimija, joka näiden henkilötietojen käsittelyä tekee tai teettää. *Henkilötietojen käsittelijäksi* sanotaan sitä, joka käsittelee henkilötietoja varsinaisen rekisterinpitäjän lukuun. Nämä roolit ja rooleihin liittyvät oikeudet ja velvollisuudet on määritelty varsin tarkasti EU:n yleisessä tietosuoja-asetuksessa (GDPR), jota Suomen kansallinen tietosuojalaki (1050/2018) täsmentää ja täydentää.

Tietoturva ja tietosuoja liittyvät tiukasti toisiinsa, mutta ne eivät ole tarkasti sama asia. Tietoturva liittyy kaikkeen tietojenkäsittelyyn – ei vain

henkilötietojen. Toisaalta erilaiset hallinnolliset ja tekniset tietoturvajärjestelyt ovat tärkeitä keinoja säädösten edellyttämälle tietosuojalle eli sen varmistamiselle, että henkilötietoja käsiteltäessä rekisteröityjen lakisääteiset oikeudet toteutuvat. Tästä seuraa eräänlainen keskinäisriippuvuus: ei voida saavuttaa kattavaa tietoturvaa ilman, että tietosuoja toteutuu, eikä tietosuojaa voi toteuttaa ilman riittäviä tietoturvatoimenpiteitä.

Tietoturva ja riskienhallinta

Kunnan riskienhallintatyössä palveluihin, toimintaan ja tietoon kohdistuvia riskejä kartoitetaan, analysoidaan ja hallitaan tietoisesti valituin toimenpitein ja kontrollein. Tietoturvapolitiikka täydentää, soveltaa ja toteuttaa kunnan riskienhallintapolitiikkaa *tietoriskien* eli tietoaineistoihin tai tietojärjestelmiin kohdistuvien saatavuus-, eheys- ja luottamuksellisuusriskien osalta.

Päävastuu riskienhallinnan ohjauksesta ja järjestämisestä on kunnanhallituksella ja kunnanjohtajalla. Toimeenpanovastuu kuuluu jokaiselle esimiehelle ja työntekijälle hänen omalla tehtäväalueellaan.

Tietoturvan yhteys jatkuvuudenhallintaan, varautumiseen ja valmiussuunnitteluun

Jatkuvuuden hallinnalla turvataan kunnan kyky hoitaa tehtäviään kaikissa oloissa sekä tarvittaessa toipua häiriöistä ja toiminnan katkoksista mahdollisimman vähin haittavaikutuksin. Tähän liittyy myös lakisääteinen valmiussuunnittelu eriasteisiin poikkeusoloihin varautumiseksi. Koska kunnan toiminta on yhä kriittisemmin riippuvaista tiedoista ja tiedonhallinnasta, on myös tietoturvallisuudesta huolehtiminen keskeinen osa sekä jatkuvuudenhallintaa että tavallisesta poikkeaviin oloihin varautumista.

Tarpeelliset toimet kunnan toimintaa uhkaavien häiriöiden ja poikkeusolojen ennakoimiseksi ja niistä selviytymiseksi määritellään kunnan ja sen toimialojen jatkuvuus-, toipumis- ja valmiussuunnitelmissa. Tietoturvapolitiikka on näitä tukeva ja täydentävä asiakirja.

Yleiset tietoturva- ja tietosuojatavoitteet

Kunnan toiminnan suuri riippuvuus tietojen saatavuudesta, eheydestä ja luottamuksellisina pysymisestä merkitsee sitä, että tietoturvallisuus on kunnalle kriittinen menestystekijä. Siksi se on välttämätön näkökulma kaikessa toiminnan suunnittelussa ja päätöksenteossa ja siten erottamaton osa kunnan johtamista, hallintoa ja palvelutoimintaa. Tietoturvallisuudesta ja tietosuojasta huolehtimisen tulee olla myös osa jokaisen työntekijän työtehtäviä.

Tietoturvan ja tietosuojan hyvällä hoitamisella tavoitellaan mm. seuraavia hyötyjä:

- häiriötön ja suunnitelmien mukaan onnistuva palvelutoiminta (asiakas-näkökulma)
- arkisen työn häiriötön sujuminen (työnteon näkökulma)
- suunnittelun ja päätöksenteon onnistuminen luotettavan tiedon pohjalta (tarkoituksenmukaisuus, virheettömyys)
- ennakoitavissa oleva talouskehitys
- kuntalaisten, asiakkaiden, yhteistyökumppanien ja muiden sidosryhmien luottamus ja arvostus
- yleiset hyvän maineen tuomat hyödyt (kunnan vetovoimaisuus ja kilpailukyky)

Tietoturvan tai tietosuojan pettäminen voisi merkitä toiminnan keskeytyksiä ja palvelujen epäonnistumista sekä näihin liittyviä taloudellisia menetyksiä ja mainehaittoja. Asiakkaat ja sidosryhmät voisivat kärsiä palvelujen tai päätöksenteon viivästymisistä. Työaikaa voisi kulua hukkaan kadotetun tiedon etsinnän ja korvaamisen vuoksi. Näitä kaikkia kunnan tulee tietenkin välttää.

Edellä mainittujen hyötyjen saavuttamiseksi ja haittojen välttämiseksi kunnalle tärkeitä **yleisiä tietoturvatavoitteita** ovat seuraavat:

- Kunnan henkilöstöllä on tehtäviensä ja tiedonhallinnan vastuidensa kannalta riittävän laaja ja ajantasainen tietoturva- ja tietosuojaosaaminen.
- Kunnan tiedonhallintaprosesseista vastaavat tuntevat lakien tiedon-hallinnalle kohdistamat vaatimukset ja osaavat soveltaa niitä tehtävä- ja vastuualueellaan.
- Kunnalle tarpeelliset tiedot ovat kunnan perustehtävien hoitamisen sekä hyvän hallinnon ja hyvän palvelutuotannon toteuttamisen kannalta riittävän eheät ja kattavat sekä saatavilla toiminnallisten tarpeiden mukaisesti.

- Kunnan omistamat ja käyttämät tiedot eivät paljastu tahoille, joilla ei ole kyseiseen tietoon oikeutta.
- Kunnan tekniset ja hallinnolliset tietoturvajärjestelyt ovat riittäviä ja oikeasuhtaisia siihen nähden, millaisia säädös- tai sopimuspohjaisia vaatimuksia kunnan tiedonhallintaan kohdistuu. Minimitavoite on, että lakisääteiset tietoturvavaatimukset täytetään kaikessa tiedonhallinnassa.
- Tietoriskien hallinnan perustavoite on rajoittaa riskit sellaiselle tasolle, jossa toteutuu hyväksyttävä tasapaino riskin suuruuden (vaikutusten ja todennäköisyyden) ja hallintakeinoihin liittyvien kustannusten tai muiden haittojen välillä.
- Vakavat tietoturvapoikkeamat vältetään.
- Kaikki tietoturvapoikkeamat tai sellaisten epäilyt tulevat asianmukaisesti ja viivytyksettä käsitellyiksi, ja mahdollisista virheistä otetaan opiksi.

Erityisesti **tietosuojaan eli henkilötietojen käsittelyyn liittyviä lisätavoitteita** ovat

- Rekisteröityjen (eli niiden, joiden henkilötietoja käsitellään, vrt. 2.2) oikeudet tulevat toteutetuiksi tietosuojasäädösten edellyttämällä tavalla.
- Tietosuojasäädösten vaatimia tiedonhallinnan vastuumäärittelyjä ja toimintatapoja noudatetaan, ja tämä toiminta dokumentoidaan niin, että vaatimusten täyttyminen voidaan tarvittaessa myös osoittaa.

Tietosuojasäädöksissä määriteltyjä rekisteröityjen oikeuksia toteutetaan kunnan kaikessa tiedonhallinnassa mm. noudattamalla seuraavia **periaatteita**:

- Henkilötietoja käsitellään lainmukaisesti, suunnitellun laillisen käyttö-tarkoituksen mukaisesti ja laillisen käsittelyperusteen nojalla.
- Henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää.
- Henkilötietojen käsittely toteutetaan täsmällisesti ja siinä noudatetaan tietojen eheyden ja luottamuksellisuuden periaatetta sekä hyviä tietoturvakäytäntöjä.
- Henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika.
- Henkilötietojen luovuttamisessa huomioidaan EU tietosuoja-asetuksen ja kansallisen lainsäädännön vaatimukset.
- Henkilötietojen käsittelystä ja sen perusteesta, käsittelyn tarkoituksesta ja tavasta sekä laajuudesta ja kestosta informoidaan rekisteröidyille (läpinäkyvyysperiaate).

- Rekisteröidyille varataan mahdollisuus käyttää heille säädöksissä määriteltyjä oikeuksia liittyen omien henkilötietojensa käsittelyyn.

Janakkalan kunta sitoutuu – kunnan konsernirakenne huomioiden – kaikessa toiminnassaan ja siihen liittyvässä tiedonhallinnassa edellä kuvattuihin tietoturva- ja tietosuojatavoitteisiin. Kunnan eri toimialat sekä prosessien ja tietovarantojen tai tietojärjestelmien omistajat voivat asettaa myös tarkempia tietoturvatavoitteita toimiala- ja tietovarantokohtaisesti. Vrt. kohdassa 4 esitetyt vastuut toimijoittain.

Organisointi, roolit ja vastuut

Eri toimijoiden vastuut tietoturvallisuuden ja tietosuojan toteutumisesta ovat seuraavat:

Kunnanhallitus

- Tietoturvapolitiikan hyväksyminen/vahvistaminen ja toteutumisen seuranta

Kunnanjohtaja

- Toimintaedellytysten luominen tietoturvapolitiikan mukaiselle tietoturvan ja tietosuojan toteuttamiselle
- Poikkeusolojen ja häiriötilanteiden viestinnän johtaminen kunnan kriisiviestintäohjeiden mukaisesti
- Varautuminen ja jatkuvuudenhallinta yhdessä kunnan johtoryhmän kanssa
- Koko kuntaa ja kuntakonsernia koskevien tietoturvaohjeiden vahvistaminen

Toimialajohtajat

- Omistajan nimeäminen toimialan tietovarannoille ja tietojärjestelmille
- Tietoturvallisuuden toteutuminen omalla toimialallaan
- Toimialakohtaisten (kunnan yleisiä ohjeita tarkentavien) tietoturvaohjeiden vahvistaminen

Konsernipalvelut

- Kunnan tietouden ylläpitäminen koskien tietoturvallisuuteen ja tietosuojaan vaikuttavia lakeja, säädöksiä ja määräyksiä sekä siitä huolehtiminen, että näitä noudatetaan kunnan kaikessa toiminnassa
- Henkilöstöturvallisuuden ja henkilöstötietojen käytön ohjaus ja koordinointi työntekijän palvelussuhteen kaikissa vaiheissa

Tietohallinto (ICT-suunnittelija)

- Teknisten tietoturvallisuusjärjestelyjen vaatimusmäärittely, toteutus tai sen ohjaus sekä valvonta kunnan tietojärjestelmäympäristössä
- Tietoturvallisuutta edistävän teknisen valvonnan toteutukset tietojärjestelmäympäristössä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin

Tietoturvavastaava (rooli, johon kunnanjohtaja nimeää henkilön) *

- Tietoturvallisuutta edistävän toiminnan yleinen suunnittelu, ohjaus, seuranta ja kehittäminen
- Tietoturvariskien ja -poikkeamien hallinnan koordinointi; vakavissa tapaukissa yhdessä valmiuspäällikön tai valmiustiimin kanssa
- Tietoturvallisuuden tilan raportointi kunnanjohtajalle
- Tietoturvallisuutta koskeva asiantuntijatuki kunnan johdolle ja toimialoille

Tietosuojavastaava */**

- Tietosuojatoiminnan yleinen suunnittelu, ohjaus, seuranta ja kehittäminen sekä tietosuojan toteutumiseen liittyvä raportointi kunnan johdolle
- Auttaa rekisterinpitäjiä ja tietovarantojen omistajia toteuttamaan lakisääteiset rekisteröityjen oikeudet henkilötietojen käsittelyssä sekä muutoinkin noudattamaan henkilötietojen käsittelyyn liittyviä vaatimuksia ja kunnan itselleen asettamia tietosuojatavoitteita
- Asiantuntijatuki kunnan johdolle ja rekisterinpitäjälle mahdollisten tietosuojaloukkausten käsittelyssä
- Tietosuojasäädösten tietosuojavastaavalle osoittamat tehtävät ja vastuut (kunnan tietosuojavastaava), ml. tarpeiden mukainen yhteydenpito muihin viranomaisiin

Valmiuspäällikkö (ja valmiustiimi)

- Kunnan valmiussuunnittelun ja varautumisen koordinointi erikseen määritellyn tehtävänkuvan ja toimivallan sekä kunnanjohtajan ohjeiden mukaisesti
- Tilannekohtainen kunta- tai toimialakohtaisen toiminnan koordinointivastuu vakavissa tietoturvallisuuden poikkeamatilanteissa (esimerkiksi laajan kyberhyökkäyksen aikana); ml. ennalta määritellyn tai kunnanjohtajan tapauskohtaisesti koolle kutsuman valmiustiimin työn johtaminen sekä tarpeelliset ilmoitukset muille viranomaisille

Tietovarantojen ja -järjestelmien tai prosessien omistajat (hallinnoimaansa järjestelmään, tietoon tai prosessiin liittyen) **

- Tiedon luottamuksellisuuden (julkisuuden tai salassapidon) ja suojaus-tarpeiden määrittely sekä tietojen käsittelyä koskevien ohjeiden antaminen
- Kriteerit käyttäjien ja käyttöoikeuksien hyväksynnälle ko. tietovarantoon tai järjestelmään
- Pääkäyttäjän nimeäminen kullekin tietojärjestelmälle
- Riskien- ja jatkuvuudenhallintatoimenpiteiden toteuttaminen omalta osaltaan
- Tiedon elinkaaren suunnittelu ja arkistonmuodostus

Tietojärjestelmien pääkäyttäjät

- Tietoturvan ja tietosuojan käytännön toteuttaminen tiedon tai tietojärjestelmän omistajan antamien tavoitteiden ja ohjeiden mukaisesti; ml. käyttäjätilien ja käyttöoikeuksien määrittäminen
- Tietojärjestelmän käyttäjien ohjeistus ja neuvonta sekä tietojärjestelmän ylläpito ja käytön seuranta tavalla, joka varmistaa, että järjestelmä on suojattu ja että sitä käytetään lakien, säädösten ja ohjeiden mukaisesti
- Omistajan, tietosuojavastaavien ja tietohallinnon avustaminen järjestelmän tietoturvallisuutta ja tietosuojaa tarkasteltaessa

Esimiehet

- Riittävän tietoturva- ja tietosuojatietouden varmistaminen osana alaisen henkilöstön perehdytystä ja osaamisen kehittämistä
- Tietoturvallisuuden toteutumisen seuranta ja mahdollisiin poikkeamiin reagointi alaisessaan toiminnassa

Henkilöstö (~ tiedon ja tietojärjestelmien käyttäjät)

- Tietoturvallisuutta tai tietosuojaa sekä kunnan tiedonhallintaa yleisesti koskevien määräysten ja ohjeiden noudattaminen omassa työssä
- Henkilöstölle tarkoitettuihin tietoturva- ja tietosuojakoulutuksiin osallistuminen sekä sisäisen tiedottamisen seuranta ja huomioon ottaminen
- Tietoturvaan tai tietosuojaan liittyvien poikkeuksien, uhkien ja riskien välitön ilmoittaminen omalle esimiehelle, tietohallintoon tai tietosuojavastaavalle

Asianhallintasihteeri

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

Luottamushenkilöt

- Kunnan antamien tietoturvallisuutta ja tietosuojaa koskevien sekä toiminta- ja käyttöohjeiden noudattaminen luottamustoimen hoidossa sekä kunnan tietoja ja tietojärjestelmiä käsitellessä

Muut kunnan tietojen tai tietojärjestelmien käyttäjät (esimerkiksi sopimussuhteiset yhteistyökumppanit, konserniyhtiöiden edustajat tms.)

- Kunnan antamien tietoturvallisuutta ja tietosuojaa koskevien sekä toiminta- ja käyttöohjeiden noudattaminen kunnan tietoja ja tietojärjestelmiä käsitellessä

Kaikki edellä mainitut:

- Havaitsemiensa tietoturvallisuutta tai tietosuojaa koskevien epäkohtien (esim. puutteiden tai poikkeamien) viivytyksetön ilmoittaminen asianomaisen tiedon omistajalle, kunnan tietoturvavastaavalle, tietosuojavastaavalle tai muulle kyseisen tilanteen kannalta sopivalle toimijalle kunnassa, jotta kunta voi ryhtyä tarpeelliseksi katsomiinsa jatkotoimiin

* Kunnan tietoturvavastaava ja tietosuojavastaava nimetään hallintosäännössä tai kunnanjohtajan erillisellä päätöksellä.

** Toimialajohtajat nimeävät vastuualueellaan tietovarannoille ja tietojärjestelmille omistajat. He voivat tarvittaessa erillisellä päätöksellään nimetä myös toimiala- tai palvelualuekohtaisia tietosuojavastaavia omalle vastuualueelleen.

Tiedon ja tietojärjestelmien käyttö

Kunnan käytössä olevat tietotekniset palvelut, järjestelmät, laitteet ja ohjelmistot on tarkoitettu työtehtävien hoitamista varten.[1] Tietojärjestelmiä ei saa käyttää tavalla, joka voisi välittömästi tai välillisesti vaarantaa kunnan vastuulla olevan tiedon tai tietojärjestelmien turvallisuuden ja aiheuttaa haittaa kunnalle tai sen toiminnalle, kunnan sidosryhmille, kuntalaisille tai käyttäjälle itselleen.

Käyttöoikeudet kunnan tietojärjestelmiin ja tietoon voidaan myöntää vain kunnan tehtävien hoitamiseksi. Jollei järjestelmäkohtaisesti ole erikseen toisin määrätty, tarvittavat oikeudet pyytää ja perustelee tietojen käyttäjän esimies, ja niiden myöntämisestä päättää tietoaineiston tai -järjestelmän nimetty vastuuhenkilö.

Tietojärjestelmiä, laitteita ja ohjelmistoja kunnan tietoverkkoon saa asentaa vain kunnan oma tietohallinto tai sen valtuuttama taho. Tietojärjestelmien käyttäminen kunnan verkon ulkopuolelta edellyttää kunnan tietohallinnon hyväksymän etäyhteystekniikan käyttämistä ja vaati käyttäjältä erityistä huolellisuutta sekä etäkäyttöä koskevien tietoturvaohjeiden noudattamista. Nämä ohjeet voivat olla osa kunnan yleisiä etätyö- ja matkustusohjeita tai tällaisia täydentäen erikseen annettuja.

Kunnan tietoverkon ja tietojärjestelmien toimintaa voidaan valvoa teknisillä valvontamenetelmillä ja -ohjelmistoilla lakisääteinen käyttäjien yksityisyyden suoja huomioiden. Tietohallinnolla on oikeus kunnan toiminnan ja tietoturvallisuuden takaamiseksi suodattaa ulkoisesta ja sisäisestä tietoliikenteestä haittaohjelmat ja muu asiaton sisältö sekä pääsy haitalliseksi luokitelluille verkkosivustoille, tällaiseen soveltuvien tekniikoiden avulla.

[1] Kunnan tietojenkäsittelylaitteiden ja tietoverkon *vähäinen käyttö henkilökohtaisiin* tarkoituksiin on sallittu omalla ajalla. Se ei kuitenkaan saa vaarantaa kunnan tietoa tai tietojärjestelmiä eikä aiheuttaa kunnalle ylimääräisiä kustannuksia tai työkuormitusta.

Tietoturvaosaamisen ja -kyvykkyyden ylläpito

Jokainen uusi tai uudessa tehtävässä aloittava työntekijä perehdytetään tietoturvan ja tietosuojan perusteisiin, kunnan tietoturva- ja tietosuojaohjeisiin (ml. tämä tietoturvapolitiikka) sekä siihen, miten nämä tulee huomioida hänen omissa työtehtävissään. Vastuu perehdytyksestä on esimiehellä. Lisäksi henkilöstölle tarjotaan tietoturvallisuuden ja tietosuojan peruskoulutusta, ja tällaiseen osallistumista valvotaan säännöllisesti. Ajantasaiset tietoturva- ja tietosuojaohjeet pidetään kaikkien työntekijöiden saatavilla kunnan sisäisessä tietoverkossa.

Tietoturvallisuuden ja tietosuojan toteuttamisesta, kehittämisestä ja johtamisesta vastaaville tarjotaan hallinnollista ja teknistä koulutusta ammattitaidon ylläpitämiseksi.

Tietoturvapolitiikan toimeenpano, seuranta ja ylläpito

Tämä tietoturvapolitiikka saatetaan kunnan koko henkilöstön, luottamuselinten sekä konserniyhtiöiden ja muiden tiedonhallinnan kannalta keskeisten sidosryhmien tietoon kunnassa hyväksi tunnettuja perehdytys- ja koulutuskäytäntöjä käyttäen. Yksittäisten yhteistyökumppanien ohjeistamisesta vastaa asianomaisen palvelun tilaaja. Tavoite on, että kaikki, jotka käsittelevät kunnan tietoa, saavat sitä varten riittävän perehdytyksen ja ohjeet tiedon turvallisen käsittelyn varmistamiseksi.

Kunnan tietoturvallisuustavoitteiden toteutumista ja turvajärjestelyjen riittävyyttä ohjataan ja seurataan säännöllisesti kunnan johtamis- ja hallintokäytäntöjen mukaisesti. Tietoturvallisuuden ylläpito ja kehittäminen tulee huomioida kaikessa palveluiden, toimintatapojen ja teknisten ratkaisujen kehittämisessä. Tietoturvapolitiikasta ja sen nojalla annetuista soveltamisohjeista poikkeavia ratkaisuja saa toteuttaa vain erityisen painavin perustein, ja poikkeamiselle on saatava etukäteen kunnanjohtajan kirjallinen hyväksyntä.

Tietoturvallisuus ja tietosuoja tulee huomioida ja tarpeen mukaan käsitellä myös osana kunnan sisäistä ja ulkoista tiedottamista ja raportointia.

Tietoturvallisuutta tai tietosuojaa koskeviin laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi kunnan normaalein kurinpitomenettelyin ja tarvittaessa lainsäädännön edellyttämällä tavalla.

Kunnanjohtaja katselmoi tämän tietoturvapolitiikan vuosittain yhdessä kunnan tietoturvavastaavan ja tietosuojavastaavan kanssa. Katselmoinnin perusteella aloitetaan tarvittaessa politiikan päivittämisen valmistelu.