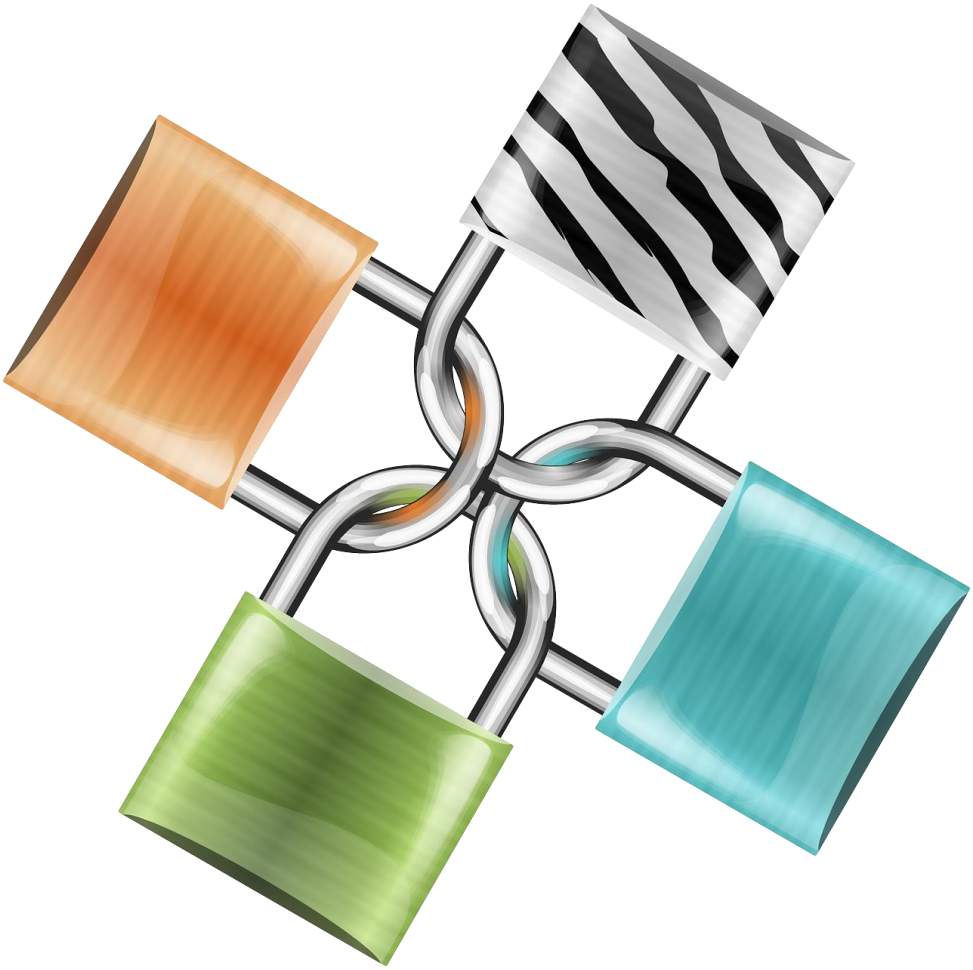
Tietoturva- ja tietosuojapolitiikka



Nurmijärvi

Sisällys

Johdanto

Tietoturva ja tietosuoja ovat yhdessä tärkeä osa Nurmijärven kuntakonsernin (myöh. kunta) toiminnan ja palveluiden laatua. Niihin liittyvä työ kunnassa on päivittäistä kaikille organisaatiotasoille, toimintoihin ja palveluihin sulautettua toimintaa.

Tässä politiikassa ja sen liitteissä määritellään, mitä tietoturva ja tietosuoja Nurmijärven kunnassa tarkoittaa. Lisäksi politiikassa kuvataan kunnan tietoturvan ja tietosuojan keskeiset periaatteet, tavoitteet, roolit ja vastuut. Politiikka toimii perustana kunnan tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa. Tämä politiikka katselmoidaan vuosittain ja on kokonaisuudessaan henkilöstön saatavilla intranetissä. Se julkaistaan myös kunnan kotisivuilla.

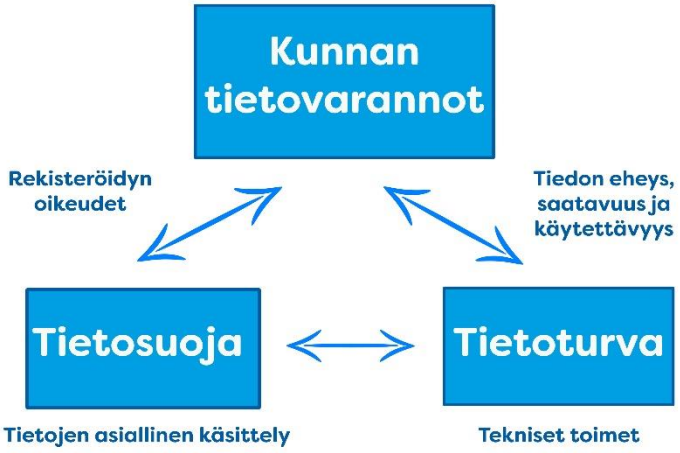
Tämä politiikka on kunnanhallituksen hyväksymä ja korvaa aiemmat erilliset tietoturvapolitiikan ja tietosuojapolitiikan. Se koskee jokaista kunnan työntekijää, viranhaltijaa, luottamushenkilöä ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee Nurmijärven kunnan omistamaa tai hallinnoimaa tietoa. Tätä politiikkaa sovelletaan kaikkeen tietoon ja muuhun dataan (myöh. tieto) riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotavasta.

2. Tietoturvallisuus ja tietoturvatyö

Tietoturvallisuus kattaa tietoturvaan ja tietosuojaan (henkilötietojen suoja) liittyvät toteutukset. Sillä tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kunnan omistamaa tai hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa, että poikkeusoloissa. Sitä noudatetaan kaiken kunnan käsittelemän tiedon suhteen sen tallennusmuodosta riippumatta.

Tietoturvan osa-alueita ovat fyysinen turvallisuus (esim. tilojen suojaaminen), hallinnollinen tietoturvallisuus (ohjeet, linjaukset ja organisointi) ja henkilöstöturvallisuus (osaaminen ja luotettavuus). Teknisiin toteutuksiin liittyvät lisäksi käyttöturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja tietoliikenneturvallisuus.

Tietosuojalla tarkoitetaan järjestelyjä, joilla varmistetaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.



Tietoturvatyö tarkoittaa tiedon suojaamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Nurmijärven kunta toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan ja tietoturvan periaatteita. Se tarkoittaa, että tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua (esim. hankintojen suunnittelu ja sopimukset). Tietojen valtuudeton ja oikeudeton käyttö estetään hyvällä tietojen käsittelyn suunnittelulla sekä ajantasaisella ohjeistuksella, jota henkilöstö noudattaa.

Periaatteena on, että tietoturvallisuuskäytännöt kattavat kaikki kunnan tietojenkäsittelytehtävät, ottaen huomioon toimialojen ja työyksiköiden luonteen ja tietoturvatarpeet. Niitä noudatetaan koko tiedon elinkaaren ajan, tietojen arkistointiin tai turvalliseen hävittämiseen asti. Tietoturvallisuus sisällytetään kaikkiin kunnan palveluihin ja toimintaan, sekä jokaisen käyttäjän työtapoihin.

Tietoturvallisuutta toteutetaan käytännössä seuraavilla:

- **Asenne:** Tiedon käsittelijä ymmärtää tietoturvan merkityksen ja omat vastuunsa, sekä on motivoinut noudattamaan tätä politiikkaa sekä tästä politiikasta johdettuja tietoturvaohjeita ja -määräyksiä.
- **Eheys:** Tieto, tietojärjestelmät ja 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 voimassa olevia lakeja sekä erikseen, toiminnoittain/järjestelmittäin, hyväksyttyjä ohjeita.
- **Pääsynvalvonta:** Tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa eikä 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 toteuttavat kunnan strategiaa (Viihtyisä ja turvallinen Nurmijärvi, Osaavien työntekijöiden hyvin johdettu työpaikka) ja arvoja (vastuullisuus, avoimuus, uudistuminen). Ne pohjautuvat liitteessä 3 mainittuihin lakeihin, ohjeisiin ja suosituksiin.

3. Tietosuojaperiaatteet

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista ja henkilötietojen oikeaoppista käsittelyä niin, että henkilön yksilöivää tietoa ei paljastu siihen oikeudettomille tiedon elinkaaren missään vaiheessa. Nurmijärven kunnalla tämä tarkoittaa asiakkaiden, henkilöstön ja sidosryhmien henkilötietojen suojaamista. Tietosuoja on osa toiminnan vaatimustenmukaisuutta, tietoturvallisuutta ja

riskienhallintaa. Tietosuoja kattaa myös vaitiolovelvollisuuden piiriin kuuluvan ja muunkin puhutun tiedon käsittelyn.

Nurmijärven kunta käsittelee henkilötietoja EU:n tietosuoja-asetuksen (GDPR) periaatteiden mukaisesti:

1. Meillä on selkeä kokonaiskuva hallussamme olevista henkilötiedoista ja niiden käsittelyyn sisältyvistä riskeistä.
2. Keräämme ainoastaan ennalta määriteltyjen käyttötarkoitusten kannalta tarpeellisia henkilötietoja kunnan tehtävien suorittamiseksi ja palveluiden kehittämiseksi.
3. Huolehdimme suunnitelmallisesti ja läpinäkyvästi henkilötietojen elinkaaren hallinnasta ja suojaamisesta.
4. Varmistamme säännöllisten koulutusten avulla, että henkilöstöllämme on riittävä tietosuojaosaaminen tehtävänkuvasta riippuen.
5. Mahdollistamme asiakkaillemme tiedonsaannin omiin henkilötietoihinsa ja informoimme kattavasti henkilötietojen käsittelyperiaatteista.
6. Arvioimme jatkuvasti henkilötietojen käsittelyyn liittyviä riskejä yksilöiden oikeuksille ja vapauksille.
7. Varmistamme, että sopimuskumppanimme noudattavat vähintään lainsäädännön mukaisia tieto-suojaperiaatteita.

Rekisterinpitäjällä on vastuu henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä määrittää, mihin tarkoituksiin ja millä keinoin henkilötietoja käsitellään. Rekisterinpitäjällä on osoitusvelvollisuus toiminnan lainmukaisuudesta, mitä toteutetaan riittävän dokumentaation avulla (mm. tietosuojaselosteet ja selosteet käsittelytoimista). Nurmijärven kunnassa rekisterinpitäjä on tehtävän tai toiminnan järjestämisestä vastaava lautakunta.

4. Tiedonhallintalain vaatimukset

1.1.2020 voimaan astunut tiedonhallintalaki ohjaa laajasti tiedon käsittelyä kunnassa. Se jakaantuu karkeasti kolmeen osa-alueeseen ja tehtäviin:

1) Tiedonhallintayksikön perustaminen ja vastuiden määrittely, tiedonhallintamallin laatiminen ja muutosvaikutusten arviointi.

- Tämä tietoturva- ja tietosuojapolitiikka on osa tiedonhallintalain edellyttämää dokumentointia ja vastuiden määrittelyä.
- Lain edellyttämä ohjeistus tietoturvan ja tietosuojan osalta on kuvattu liitteessä 3.
- Tiedonhallintamallissa kuvataan tiedon käsittelyn, tietojärjestelmien, tietoturvan ja myös tietosuojan hallinta organisaatiossa. Se antaa kuvan tiedon elinkaaresta, sen keruusta tiedon hävittämiseen saakka.

2) Tietoturvavaatimukset (voimaan 1.1.2023).

- Kunnassa tulee olla siihen mennessä lain edellyttämällä tasolla mm. tietojärjestelmien turvallisuus, tietojen turvallinen siirtäminen tietoverkoissa,

tietoaineistoturvallisuus, henkilöstöturvallisuusselvitykset, käyttöoikeuksien hallinta sekä lokien kerääminen.

3) Tietoaineistojen digitalisointi, digitaalisen tiedon käsittely, luovuttaminen ja vastaanottaminen.

- Kunta valmistautuu tiedon sähköiseen siirtoon viranomaisten välillä valtakunnallisen ohjeistuksen mukaisesti ja edistää tiedon säilyttämistä sähköisessä muodossa.

5. Menettely tietoturvallisuuden vaarantuessa

Toimintatapa tietoturvallisuuden vaarantuessa riippuu siitä, koskeeko tapahtuma henkilötietoja vai ei. Tietosuojaloukkaukseksi katsotaan henkilötietojen käsittelyä koskevien lakien ja asetusten, tämän politiikan sekä kunnan tarkempien periaatteiden ja ohjeistusten vastainen toiminta. Jokaisella työntekijällä on velvollisuus ilmoittaa huomatessaan mahdollisen tietosuoja- tai tietoturvaloukkauksen. Ilmoitus tehdään omalle esimiehelle, joka tarvittaessa vie asian eteenpäin tietotekniikan helpdeskiin, tietosuojavastaavalle tai tietoturvapäällikölle.[1] Jo pelkkä epäily tietosuoja- tai tietoturvaloukkauksesta johtaa asian selvittämiseen. Ilmoituskynnyksen tulee olla matalalla ja työntekijöiden tietoisia siitä, miten ja kenelle epäilyistä ilmoitetaan.

Jos tietosuojaloukkauksesta todennäköisesti aiheutuu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski, rekisterinpitäjän on ilmoitettava siitä rekisteröidyille ja valvontaviranomaiselle ilman aiheetonta viivytystä (72 h). Nurmijärven kunnan tietosuojavastaava toimii yhteyshenkilönä valvontaviranomaiselle (tietosuojavaltuutettu). Ilmoittaminen rekisteröidyille, joita tietosuojaloukkaus koskee, tapahtuu tietosuojavastaavan, rekisterin vastuuhenkilön ja tietojärjestelmän pääkäyttäjän yhdessä sopimalla tavalla.

Poikkeamisen tai rikkomuksen käsittelyssä ei tule pysähtyä siihen, mikä meni pieleen tai kuka toimi väärin. Virheiden paljastuminen on pienempi paha kuin niiden huomaamatta tai ilmoittamatta jääminen. On muistettava kysyä myös, mitä olisimme voineet tehdä paremmin ja mitä opittiin tapahtumasta, sillä virheet voivat ohjata kohti toiminnan kehittämistä jatkossa.

Tietoturvarikkomuksista ja tietosuojaloukkauksista voi olla seurauksena käyttöoikeuksien rajoituksia, palvelussuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia. Palvelussuhteeseen vaikuttavista seuraamuksista on säädetty ensi sijassa työsopimuslaissa ja viranhaltijalaissa. Sovellettavaksi voivat tulla myös rikos- ja vahingonkorvauslainsäädäntö. Seuraamuksia arvioitaessa moitittava toiminta, sen vaikutukset ja seuraukset käsitellään kokonaisuutena.

Kunnan tietosuojavastaava, tietoturvapäällikkö, turvallisuuspäällikkö ja toimialojen tietosuojan yhdyshenkilöt osallistuvat tietoturva- ja tietosuojapoikkeamien, väärinkäytös-

[1] Ks. intranetistä löytyvä ohje *Miten toimit henkilötietojen tietoturvaloukkauksen tapahduttua*.

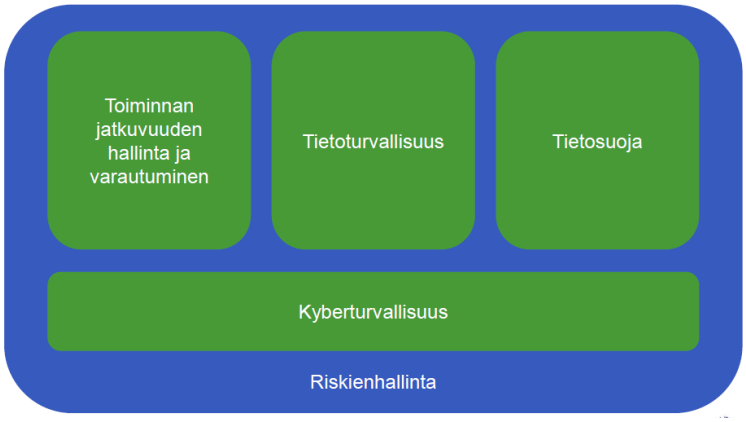
ten sekä nykytilan arviointiin oman työroolinsa rajoissa. Näiden työtehtävien suorittamiseksi edellä mainituille henkilöille mahdollistetaan pääsy tehtävän edellyttämään tietoon.

6. Tietoturvallisuus osana kokonaisturvallisuutta

Tietoturvallisuus on osa kunnan kokonaisturvallisuutta, ja sitä kehitetään yhteistyössä kunnan turvallisuusorganisaation kanssa, huomioiden mm. rakenteellinen turvallisuus, tilaturvallisuus ja henkilöturvallisuus.

Kunnan johtoryhmän organisoima ja kuvaama riskienhallintaprosessi toimii kunnan turvallisuusjärjestelyiden ja varautumisen perustana. Riskienhallinnan tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että riskienhallintakeinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen. Riskienhallinta kattaa kaikki tunnistetut riskit, mukaan lukien tietoon kohdistuvat ja tiedosta aiheutuvat riskit – digitaalisen tiedon osalta asiaa on kuvattu näin[2]:

Digitaalinen turvallisuus



Kaikissa varautumiseen ja jatkuvuudenhallintaan liittyvissä suunnitelmissa huomioidaan tietoturvallisuusnäkökulma.

- Jatkuvuussuunnitelmat toiminnan kannalta elintärkeille palveluille, toiminnoille ja tietojärjestelmille niiden jatkuvuuden turvaamiseksi.
- Toipumissuunnitelmat kriittisille tietojärjestelmille ja -verkoille niiden mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi.
- Valmiussuunnitelma toiminnan, palveluiden ja järjestelmien hallinnoimiseksi häiriö- ja poikkeusoloissa (kriittiset tietojärjestelmät nimetään valmiussuunnitelmassa).
- Lakisääteiset pelastussuunnitelmat ihmisten ja omaisuuden suojelemiseksi, sekä vahinkojen minimoimiseksi onnettomuustilanteissa.

[2] Kuvan lähde: Päivi Nerg: *Kuntien digitaalinen turvallisuus.* Kuntien ja maakuntien kyberturvallisuuspäivät 2020.

Varautumista toteutetaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia valmius- ja muita suunnitelmia myös tietoturvallisuuden osalta (esim. valtakunnalliset TAISTO-harjoitukset). Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

EU:n yleinen tietosuoja-asetus edellyttää vaikutuksen arvioinnin (DPIA) tekemistä. Vaikutustenarvioinnin tarkoituksena on kuvata henkilötietojen käsittelyä, arvioida käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä arvioida henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutusten arviointia on tehtävä, kun henkilötietojen käsittelyyn kohdistuu korkea riski, esimerkiksi silloin, kun käsitellään suuria määriä arkaluonteisia tietoja tai käytetään uutta teknologiaa. Vaikutustenarviointi tulee ottaa osaksi toiminnan ja hankintojen suunnittelua niin, että tiedostetaan varhaisessa vaiheessa, milloin vaikutustenarviointi on tarpeen.

7. Roolit ja vastuut

Tietoturvan ja tietosuojan toteuttaminen on jatkuvaa ja kuuluu kaikille. Sen toteuttamiseen osallistuvat kunnan ja sidosryhmien henkilöstö, osana omaa yleistä toimintavastuutaan. Tämä tarkoittaa hyvien periaatteiden ja yhteisten ohjeiden noudattamista sekä tietoturvan ja tietosuojan huomioimista kaikessa tekemisessä. Kunnan tietoturva- ja tietosuojaperiaatteita sovelletaan yhtä lailla myös kokeiluhankkeisiin ja pilotteihin.

Ylin vastuu tietoturvasta, tietosuojasta, riskienhallinnasta ja varautumisesta on kunnanhallituksella ja kunnanjohtajalla. Ohjaus- ja kehittämistyössä tarvittava muu erityisasiantuntemus ja nimetyt turvallisuusvastuut kuvataan liitteessä 1.

8. Tiedon ja tietojärjestelmien käyttö

Käyttäjien toimintaa ohjataan tästä politiikasta johdetuilla periaatteilla ja ohjeilla.

Kunnan tietojärjestelmäympäristössä käytetään tietohallinnon hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja. Otettaessa käyttöön uusia ratkaisuja tulee varmistua, että ne ovat tietohallinnon tiedossa ja hyväksymiä.

Kunnan toimintaa ja palveluita tukevat tietojärjestelmät tunnistetaan ja luokitellaan kriittisyyden perusteella. Jokaiselle järjestelmälle nimetään omistaja ja pääkäyttäjä, ja järjestelmien kriittisyys ja riskit arvioidaan. Käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään esimiehen hyväksynnällä ja työtehtävien hoitoon tarvittavassa laajuudessa.

Käytettävät tietojärjestelmät ja laitteet on tarkoitettu työtehtävien hoitamiseen, eikä niitä tule käyttää kunnan omistaman tai hallinnoiman tiedon vaarantumiseen johtavaan toimintaan. Kunnalle tai sen toiminnalle mahdollisesti aiheutetun haitan korvausvastuussa on ensi sijassa vaarantumisen aiheuttaja.

9. Tietoturva- ja tietosuojatietoisuus

Tietoturva- ja tietosuojatietoisuus merkitsee kunnan henkilöstön ymmärrystä tiedon – ja etenkin henkilötietojen – käsittelyyn liittyvistä vastuista sekä velvoitteista tiedon elinkaaren kaikissa vaiheissa, sekä sitoutumista organisaation tietosuoja- ja tietoturvaperiaatteiden noudattamiseen. Tietoturva- ja tietosuojatietoisuutta ylläpidetään ja kehitetään aktiivisen viestinnän, henkilöstön koulutuksen (vuosittainen koulutussuunnitelma ja sen seuranta) sekä ajantasaisen ohjeistuksen avulla.

Keskeinen tietoturva- ja tietosuojaohjeistus sisällytetään koko kunnan henkilöstön perehdytysprosessiin. Tarvittavien ulkoisten sidosryhmien tietoturva- ja tietosuojaosaamisesta vastaa kyseisen toimialan johto. Periaate on, että kaikki, jotka käsittelevät kunnan omistamaa tai hallinnoimaa tietoa, saavat riittävät edellytykset tiedon asianmukaiseen käsittelyyn.

Jokainen työntekijä allekirjoittaa palvelussuhteen alkaessa tietoturva- ja tietosuojasitoumuksen.[3] Esimies huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin sekä työntekijän omissa työtehtävissä tarvittavaan erityisosaamiseen. Esimiesten vastuulla on, että työntekijät suorittavat vuosittain tietoturvan ja tietosuojan perusteista Navisec-verkkokoulutuksen ja -testin sekä osallistuvat heille suunnattuihin tietosuojakoulutuksiin. Lisäksi tietoturva- ja tietosuojaohjeet ovat kaikkien työntekijöiden saatavilla intranetissä. Tietoturvallisuuden ja tietosuojan ylläpidosta, kehittämisestä ja johtamisesta vastaaville tarjotaan riittävä hallinnollinen ja tekninen koulutus.

10. Tietoturvan ja tietosuojan seuranta, ylläpito ja kehittäminen

Kunnan tietoturva- ja tietosuojatavoitteiden toteutumista seurataan säännöllisesti laaditun vuosikellon mukaisesti. Tietoturva- ja suojapolitiikan ajantasaisuus katselmoidaan vuosittain ja sitä päivitetään tarvittaessa. Päivitykset hyväksytään tietoturva- ja tietosuojaryhmässä. Merkittävät sisällölliset muutokset hyväksyy kunnanhallitus.

Liitteet

1. Tietoturvan ja tietosuojan huoneentaulu
2. Roolit ja vastuut
3. Lainsäädäntö ja ohjaavat asiakirjat

[3] Sitoumusta säilytetään työsopimuksen yhteydessä henkilöaktissa.

Liite 1 Tietoturvan ja tietosuojan huoneentaulu

1.
Noudata annettuja tietoturvaohjeita ja -käytäntöjä.

2.
Lukitse tietokoneesi tai kirjaudu ulos aina kun poistut sen läheisyydestä. Käytä eri salasanaa eri järjestelmissä. Säilytä salasanat ja muut kirjautumisessa käytettävät tunnisteet, kuten toimikorttisi ja PIN-koodit huolellisesti.

3.
Varo paljastamasta luottamuksellisia tietoja sivullisille työpaikalla tai sen ulkopuolella esim. sosiaalisessa mediassa.

4.
Älä surffaa arveluttavilla nettisivuilla. Älä avaa outoja sähköpostiviestejä tai niiden liitteitä.

5.
Huolehdi papereiden, muistitikkujen, puhelinten, salasanojen, avainten, kulkukorttien ym. asianmukaisesta käsittelystä ja säilyttämisestä.

6.
Hävitä henkilötietoja sisältävät paperit ja muu tietosuojattava jäte asianmukaisesti – käytä tietoturvasäiliötä.

7.
Huolehdi erityisesti etätyössä kannettavan tietokoneen ja sen tietojen suojaamisesta. Hanki kannettavaan tietokoneeseen suojakalvo, joka estää sivulta tapahtuvan salakatselun.

8.
Muista kunnioittaa asiakkaiden ja työkavereiden yksityisyyttä.
Näin ylläpidät luottamusta.

9.
Kerro esimiehellesi, mikäli havaitset tietoturva- tai tietosuojapoikkeamia tai -rikkomuksia.

10.
Älä hätäänny, jos jotain poikkeavaa tapahtuu. Soita rohkeasti helpdeskiin.

+Bonus:
- **Kysyn, jos en tiedä!**
- **Varmistan, jos epäilen että asia ei etene!**
- **En hölmöile!**

Liite 2 Roolit ja vastuut

Kunnan keskeisimmät tietoturvallisuuteen liittyvät toimijat ja roolit vastuineen on määritelty alla. Mikäli kunnan hallinto- tai muissa säännöissä ei ole määritelty kenelle roolin vastuu kuuluu, on kunnanjohtaja vastuussa sopivimman henkilön nimeämisestä kyseiseen rooliin.

Luottamushenkilöstö

- Vastaa tietoturvallisuuden toteuttamisesta omissa luottamustehtävissään

Kunnanhallitus

- Toimii kunnan ylimpänä kokonaisturvallisuudesta päättävänä tahona ja omistajana
- Politiikkatason asiakirjojen hyväksyntä
- Kokonaisturvallisuuden toteutumisen seuranta ja ohjaus

Kunnanjohtaja

- Edellytysten luominen tietoturvallisuuden toteutumiselle
- Raportointi ja kehitysehdotukset kunnanhallitukselle

Tietoturva- ja tietosuojaryhmä

- Kehittää ja edistää organisaation tietoturvan ja tietosuojan toteutumista ja seuraa sitä vuosikellon mukaisesti
- Seuraa tietoturvallisuuden ja tietosuojan yleistä kehittymistä, toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietoturva- ja tietosuojariskejä
- Toimii koko kuntaorganisaation tukena tietoturvallisuusasioissa.
- Tietoriskien ja tietoturvapoikkeamien hallinnan koordinointi
- Tietoturvallisuuteen liittyvän viestinnän tukeminen ja toteuttaminen yhdessä tietoturvapäällikön ja tietosuojavastaavan kanssa

Tietohallinnon kehittämisryhmä

- Huolehtii, että tietojärjestelmähankinnoissa noudatetaan tietoturva- ja tietosuojapolitiikkaa

Tietoturvapäällikkö (rooli)

- Tietoturvapolitiikan ja -periaatteiden määrittelyyn osallistuminen
- Tietoturvan kehittäminen tietoturvapolitiikan mukaisesti
- Henkilöstön tietoturvatietouden ylläpito ja tietoturvakoulutuksen järjestelyt
- Tietoturvan toteutuksen ohjaus
- Johdolle raportointi tietoturvan toteutumisesta, vuosikellon mukaisesti
- Yhteisten tietoturvaperiaatteiden ja käytäntöjen valmistelu, sekä tietoturvasuunnitelman omistajuus
- Yhteistyö ulkoisten sidosryhmien kanssa

Tietosuojavastaava

- Vastaa tietosuojatyön organisoinnista, suunnittelusta ja toteuttamisesta kunnassa yhdessä tietoturva- ja tietosuojaryhmän kanssa
- Vastuuseen sisältyy tarvittava ohjaus, seuranta ja kehittäminen, sekä tietosuojariskien ja -poikkeamien hallinnan koordinointi
- Raportoi tietosuojan nykytilasta sekä kehittämistoimenpiteistä johdolle vuosittain
- Auttaa henkilötietojen käsittelyn erityisasiantuntijana kunnan johtoa rekisterinpitäjän velvoitteiden toteuttamisessa
- Toimii organisaatiossa henkilötietojen käsittelyä valvovana tahona ja yhdyssiteenä sekä valvontaviranomaiseen että rekisteröityihin

Toimialojen johto (toimialajohtajat ja liikelaitosten johtajat)

- Vastaa tietoturvallisuuden ja tietosuojan toteutuksesta johtamansa toiminnan osalta
- Nimeää omistajat vastuualueellaan oleville tietojärjestelmille
- Ylläpitää tietoutta tietoturvallisuuteen ja tietosuojaan vaikuttavista laeista, säädöksistä ja määräyksistä, sekä huolehtii niiden huomioimisesta johtamansa toiminnan osalta

Esimies

- Vastaa oman yksikkönsä tai tulosalueensa osalta annettujen määräysten ja ohjeistusten noudattamisesta. Tähän sisältyy niin työntekijöiden perehdyttäminen kuin toteutumisen seuranta.
- Ilmoittaa mahdollisista tietosuojapoikkeamista tietosuojavastaavalle
- Ilmoittaa mahdollisista tietoturvapoikkeamista tietotekniikan helpdeskiin tai tietoturvapäällikölle
- Tietojärjestelmien käyttöoikeuksien hakeminen, hyväksyminen, muuttaminen ja poistopyyntöjen tekeminen

Tiedon tai tietojärjestelmän omistaja

- Omistamansa tiedon tai tietojärjestelmän suojaamistarpeen määrittäminen, sekä käyttöoikeuksien myöntämisen periaatteet ja säännöllisestä katselmoinnista huolehtiminen (mm. toipumis- ja jatkuvuussuunnitelmat)
- Tietojärjestelmän ja tiedon riskienhallinta
- Vastaa järjestelmien turvajärjestelyjen asianmukaisesta totetuttamisesta käyttäen apuna kulloinkin tarvittavia asiantuntijoita (esim. tietosuojavastaava, tietoturvapäällikkö, turvallisuuspäällikkö, ulkoinen auditointi)

Henkilöstöpalvelut

- Henkilöstöturvallisuuden (tietoturvallisuuden osa-alueena) ohjaaminen ja toteutumisen tuki virka- / työsuhteen kaikissa vaiheissa

Hankintoja ja sopimuksia tekevät

- Vastaavat siitä, että tietoturvallisuuden taso vastaa hankittavien tuotteiden, palveluiden ja kumppanuus- ja ulkoistusratkaisujen osalta kunnan vaatimuksia, määräyksiä ja ohjeita.

Asiakirjahallinnosta vastaava

- Ohjaa ja kehittää asiakirjahallintoa osana koko kunnan tiedonhallintaa, huomioiden tietoturvallisuuden
- Ohjaa toimialoja asiakirjahallinnon hoidossa, jotta arkistolain 7§ toteutuu oikeusturva ja tietosuoja huomioiden
- Hyväksyy asiakirjallisten tietoaineistojen hallinnan edellyttämät arkistonmuodostus- ja tiedonohjaussuunnitelmat
- Vastaa päätearkistoon luovutetusta pysyvästi säilytettävästä tietoaineistosta ja sen tietoturvallisuudesta ja tietosuojasta

Toimialojen asiakirjahallinnon vastuuhenkilöt (vastuualueet määritellään tehtävänkuvissa)

- Koordinoivat vastuualueellaan asiakirjahallinnon hoitoa arkistolain 7 § ja kunnan tietoturvallisuusohjeet huomioiden
- Huolehtivat vastuualueellaan lähiarkistojen tietoaineistojen säilyttämisestä ja niiden tietoturvallisuudesta ja tietosuojasta

Tietotekniikan henkilöstö

- Tietoturva- ja tietosuojapolitiikan soveltaminen ja toteuttaminen
- Vastaa tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

Tietojärjestelmän pää- ja varapääkäyttäjä

- Valvoo tietoturvan ja käyttöoikeuspolitiikan toteutumista omalla vastuualueellaan
- Käyttöoikeuksien hallinta tietojärjestelmän omistajan valtuuttamana
- Tietojärjestelmien dokumentaation ylläpito (mm. tietosuojaseloste), yhdessä tiedon tai tietojärjestelmän omistajan kanssa
- Huolehtii sovelluksen ylläpitotoiminnoista ja toimii yhdyshenkilönä järjestelmätoimittajaan
- Tiedottaa käyttäjiä, tietotekniikkayksikköä ja esimiehiä vikatilanteista ja käyttökatkoista ja huolehtii käyttökatkojen aikataulutuksista

Henkilöstö/jokainen työntekijä

- Käsittelee tietoja annettujen ohjeiden ja määräysten mukaisesti
- Allekirjoittaa tietosuojasitoumuksen
- Ilmoittaa viipymättä havaitsemistaan tietoturvaan ja tietosuojaan liittyvistä ongelmista, poikkeamista tai ohjeiden vastaisesta menettelystä tietotekniikan helpdeskiin, esimiehelle ja tietosuojavastaavalle tai tietoturvapäällikölle.

Rekisteröidyt

- Ovat tietoisia oikeuksistaan sekä vastuussa antamiensa tietojen oikeellisuudesta

Ulkoiset palveluntuottajat

- Sitoutuvat noudattamaan kunnan tietoturva- ja tietosuojaohjeistusta

- Palveluntuottajien vastuut henkilötietojen käsittelyssä sovitaan palvelukohtaisissa sopimuksissa
- Palveluntuottajien tulee nimetä tietoturva- ja tietosuoja-asioihin yhteyshenkilö

Liite 3 Lainsäädäntö ja ohjaavat asiakirjat

Kunnan strategiat ja päätökset

- Nurmijärvi - positiivinen ilmiö - kuntastrategia 2018 - 2025
- Nurmijärven kunnan hallintosääntö 2020
- Kunnanjohtajan päätös tietoturva- ja tietosuojaryhmien yhdistämisestä 29.11.2018

Tärkeimmät lait, asetukset ja valtakunnalliset ohjeistukset:

- EU:n yleinen tietosuoja-asetus (679/2016)
- Tietosuojalaki (1050/2018)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Arkistolaki (831/1994)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- Laki digitaalisten palvelujen tarjoamisesta (306/2019)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- VAHTI-ohjeet
- Tiedonhallintalautakunnan suositukset ja ohjeet https://vm.fi/tiedonhallintalautakunta

Uudistuvat säädöstekstit löytyvät ajantasaisina mm. Valtion säädöstietopankki – sivustolta (www.finlex.fi)

Nurmijärven tietoturva- ja tietosuojapolitiikkaa toteuttavaa ohjeistusta (https://nurmijarvikunta.sharepoint.com/sites/tuki/SitePages/Tietoturva-ja-tietosuoja.aspx):

- Tietoturva pähkinänkuoressa
- Tietoturva – henkilöstön ohje
- Tietojärjestelmän omistajan tietoturvaohje
- Pääkäyttäjän tietoturvaohje
- Esimiehen tietoturvaohje
- Yleisohje henkilötietojen käsittelystä
- Toimintaohje – henkilötietojen tietoturvaloukkaus
- Tietoturva ja tietosuoja etätyössä
- O365-sähköpostiohje
- Päätösten julkaiseminen verkossa ja tietosuoja