TUUSULAN KUNTA

TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Kunnanhallitus xx.xx.xxxx

SISÄLLYS

1. Johdanto

Kunnan johto määrittää tietoturva- ja tietosuojapolitiikassa ne periaatteet, toimintatavat, vastuut ja tavoitteet, joita noudatetaan Tuusulan kunnan tietoturva- ja tietosuojatyön toteuttamisessa ja kehittämisessä.

Politiikka toimii perustana Tuusulan kunnan tietoturvaa ja tietosuojaa koskeville alaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden käytäntöön soveltamisessa.

Tietoturva- ja tietosuojapolitiikka koskee koko kuntaorganisaatiota ja sen henkilöstöä mukaan lukien kuntakonsernin sekä niitä Tuusulan kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Tuusulan kunnan omistamaa tai hallinnoimaa tietoa tietoa tai käyttävät Tuusulan kunnan tietoverkkoa ja sen palveluita. Politiikka kattaa Tuusulan kunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi. Asiasisältöä tarkistetaan ja päivitetään säännöllisesti.

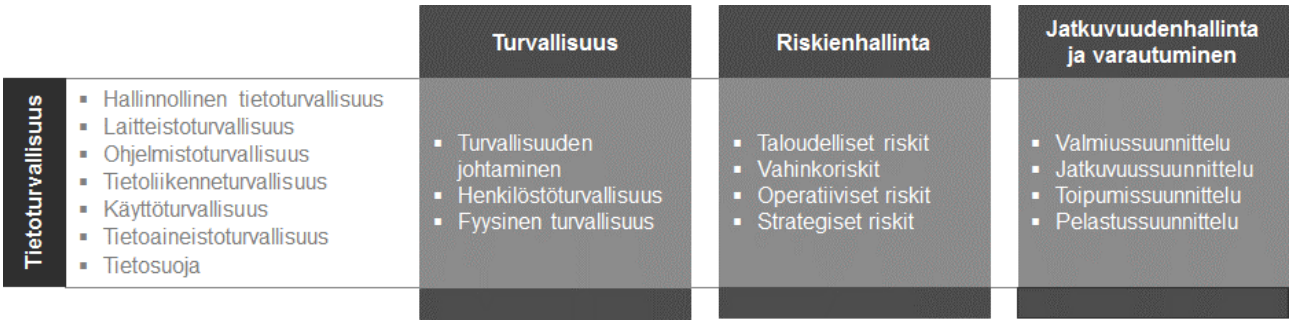
Tietoturva- ja tietosuojapolitiikka on henkilöstön saatavilla Kaiku-Intranetissä.

1.1. Tietoturvan ja tietosuojan määritelmä

Tietosuoja ja tietoturvallisuus liittyvät jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin. Tietoturvalla eli tietoturvallisuudella tarkoitetaan tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä eli niitä teknisiä ja hallinnollisia toimenpiteitä, joilla pyritään tietosuojan toteuttamiseen. Käytännössä tämä tarkoitaa tietoaineistojen, tietojärjestelmien ja tietoliikenteen suojaamista niin, että minimoidaan tietoihin, toimintaan ja palveluihin liittyvät riskit. Tietoturvallisuus on kiinteä osa kunnan johtamista, palveluita ja toimintoja.

Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen.

Tietoturvallisuus integroituu kuvan 1 mukaisesti kaikkiin kokonaisturvallisuuden osa-alueisiin: turvallisuus, riskienhallinta sekä jatkuvuudenhallinta ja varautuminen.



kuva 1. Kunnan kokonaisturvallisuus

Tietosuojalla tarkoitetaan yksilön (rekisteröity) yksityisyyden ja luottamuksen turvaamista eli henkilötietojen oikeaoppista käsittelyä sekä tietojen suojaamista asiattomalta käytöltä. Tietosuojan tarkoituksena on varmistaa yksilön perusoikeuksien säilyminen halki tietojen käsittelyn elinkaaren. Tiivistetysti voidaan todeta, että tietosuoja on perustuslain nojalla turvattu rekisteröidyn oikeus elää omaa elämäänsä ilman kenenkään oikeudetonta puuttumista siihen.

1.2. Tietoturva- ja tietosuojatietoisuus

Tietoturva- ja tietosuojatietoisuus merkitsee kunnan henkilöstön ymmärrystä henkilötietojen käsittelyyn liittyvistä vastuista sekä velvoitteista tiedon hallinnan prosessin kaikissa vaiheissa, sekä sitoutumista organisaation tietosuoja- ja tietoturvaperiaateiden noudattamiseen. Tietoturva- ja tietosuojatietoisuutta ylläpidetään ja kehitetään henkilöstön koulutuksen sekä ajantasaisen ohjeistuksen avulla.

2. Tietoturva ja tietosuoja organisaatiossa

Tässä luvussa määritellään tietoturvan ja tietosuojan vastuiden jakautuminen kunnan organisaatiossa, tietosuojavastaavan ja tietoturvapäällikön tehtävät, sekä tietoturva- ja tietosuojaryhmän muodostaminen.

Kunnan tietosuojatyötä ohjaavat seuraavat lait, asetukset ja ohjeistukset:

- EU:n tietosuoja-asetus (679/2016) ja Tietosuojalaki (1050/2018)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Arkistolaki (831/1994)
- Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositukset
- Kunnan omat strategiat ja niistä johdetut vaatimukset
- Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeet

2.1. Organisointi ja vastuut

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

Kunnanhallitus hyväksyy tietosuoja- ja tietoturvapolitiikan.

Kansliapäällikkö toimii tietoturvallisuuden ja tietosuojan omistajana kunnassa luoden edellytykset niiden asianmukaiselle toteuttamiselle. Kansliapäällikkö asettaa ryhmän seuraamaan tietoturvan ja tietosuojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan järjestelmien pääkäyttäjien tukena.

Toimialuejohtaja vastaa tietoturvallisuuden ja tietosuojan toteutuksesta johtamansa toiminnan osalta ja siitä, että järjestelmien omistajat sekä pääkäyttäjät on nimetty.

Tiedon, tietojärjestelmän tai palvelun omistaja vastaa omistukseensa liittyvästä:

- Käyttäjien ja käyttöoikeuksien määrittelystä ja hyväksynnästä
- Riskienhallinnan toteuttamisesta, sisältäen riittävän dokumentaation varmistamisen järjestelmästä
- Tiedon eheyden varmistamisesta
- Tietojen luokittelusta (julkisuuden ja salassapidon määrittely, arkistonmuodostus)
- Rekisteriselosteen laadinnasta ja nimeää rekisterin yhteyshenkilön

Esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta alaisessaan toiminnassa, sekä erityisesti alaisten ja muun henkilökunnan riittävästä perehdyttämisestä tietoturvapolitiikkaan ja siihen liittyviin tietoturvaohjeisiin.

Jokainen viranhaltija ja työntekijä vastaa omalta osaltaan tietoturvaa sekä tietosuojaa koskevien määräysten ja ohjeiden noudattamisesta, sekä tietosuojasitoumuksen allekirjoittamisesta. Jokaisen vastuulla on lisäksi tietoturvaan ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen viipymättä esimiehelle ja tietosuojavastaavalle tai tietoturvapäällikölle.

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. Tietosuojavastaava raportoi tietosuojan nykytilasta sekä kehittämistoimenpiteistä vuosittain kansliapäällikölle. Tietosuojavastaavan rooli on henkilötietojen käsittelyn erityisasiantuntijana auttaa kunnan johtoa rekisterinpitäjän velvoitteiden toteuttamisessa. Tietosuojavastaavan tulee myös toimia organisaatiossa

henkilötietojen käsittelyä valvovana tahona ja yhdyssiteenä sekä valvontaviranomaiseen että rekisteröityihin.

Tietoturvapäällikkö vastaa tietoturvallisuuden toteutumisesta ja integroitumisesta muihin kokonaisturvallisuuden osa-alueisiin. Vastuuseen sisältyy tarvittava suunnittelu, ohjaus, seuranta ja kehittäminen, sekä tietoturvariskien ja -poikkeamien hallinnan koordinointi. Tietoturvapäällikkö raportoi kunnan johtoryhmälle.

Tietoturva- ja tietosuojaryhmä seuraa tietoturvallisuuden ja tietosuojan yleistä kehittymistä, toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietoturva- ja tietosuojariskejä. Ryhmä laatii kehitysehdotuksia tietoturvallisuuden parantamiseksi sekä toimii koko kuntaorganisaation tukena tietosuoja-asioissa.

Tietojärjestelmäpalvelut vastaa tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

Tietohallintopäällikkö tukee toimialoja tietoturvapolitiikan toteuttamisessa mm. antamalla uusista järjestelmähankinnoista lausunnon tietoturvaan ja kokonaisarkkitehtuuriin liittyen.

Järjestelmän pääkäyttäjä valvoo tietoturvan ja käyttöoikeuspolitiikan toteutumista omalla vastuualueellaan. Pääkäyttäjä huolehtii sovelluksen ylläpitotoiminnoista ja toimii yhdyshenkilönä järjestelmätoimittajaan. Pääkäyttäjä tiedottaa käyttäjiä, ICT-yksikköä ja esimiehiä vikatilanteista ja käyttökatkoista ja huolehtii käyttökatkojen aikataulutuksista.

2.2. Rekisterinpitäjän velvollisuudet

Tuusulan kunnan rekisterinpitäjänä toimii kunnanhallitus tai lautakunta. Rekisterinpitäjällä on ylin vastuu rekisterissään olevista henkilötiedoista, sekä niiden käsittelyn suunnittelusta ja toteutuksesta. Rekisterinpitäjällä on muun muassa velvollisuus määritellä henkilötietojen käsittelyperuste, sekä informoitava rekisteröityjä heidän henkilötietojensa käsittelyn johdosta. Lisäksi rekisterinpitäjän on pystyttävä osoittamaan, että henkilötietojen käsittelyssä noudatetaan tietosuojalainsäädäntöä.

Jokaisella kunnan rekisterinpitäjällä on oltava dokumentoituna seuraavat asiakirjat:

- rekisterikohtainen tietosuojaseloste
- rekisterikohtainen tietosuojariskienarviointi

Lisäksi tietosuoja huomioidaan kunnan (rekisterinpitäjä) ja henkilötietojen käsittelijän (esim. järjestelmätoimittaja) välisissä sopimuksissa EU:n yleisen tietosuoja-asetuksen mukaisesti, jolloin henkilötietojen käsittelyä ulkoistettettaessa henkilötietojen käsittelijän vastuu määritetään kirjallisella sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa

rekisterinpitäjään. Sopimuksessa on määriteltävä vähintään käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet.

2.3. Tietoturvan ja tietosuojan toteuttamista tukevat käytännöt

Tietoturva- ja tietosuojatyö ovat osa kunnan yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturvan ja tietosuojan toteutuminen varmistetaan käyttämällä tarvittavia teknisiä ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi koko niiden elinkaaren ajan.

Teknisiä ja organisatorisia toimia ovat mm:

- tietosuojavastaavan/tietoturvapäällikön nimeäminen
- tietosuoja- ja tietoturvatyön dokumentoiminen
- henkilöstön kouluttaminen ja ohjeiden laatiminen

3. Tietoturva- ja tietosuojatavoitteet

Kunnan tietoturva- ja tietosuojatyön tavoitteena on edistää hyvää tietojenkäsittelytapaa sekä varmistaa tietojenkäsittelyn turvallisuus sekä tehtävien sujuva toiminta organisaatiossa. Tietoja tulee käsitellä niin, että kaikki osapuolet voivat luottaa käsittelyn asianmukaisuuteen.

Tietoturvan osalta kunnan tavoitteena on saavuttaa Tietoturvallisuusasetuksen (681/2010) kuvaaman tietoturvallisuuden perustason vaatimukset koko kunnan laajuisesti ja korotetun tason vaatimukset lainsäädännön edellyttämissä toiminnoissa tai toiminnan tarpeiden niin vaatiessa.

Tietosuojan osalta tavoitteena on saavuttaa korkea henkilötietojen käsittelyn taso. Tavoitteeseen päästään toteuttamalla tietosuoja-asetuksen rekisterinpitäjälle osoittamat velvollisuudet ja todentamalla, että kunnassa noudatetaan tietosuoja-asetuksessa määriteltyjä seuraavia henkilötietojen käsittelyn periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään ainoastaan käyttötarkoituksen mukainen määrä
- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

3.1. Tietoturvallisuuden ja tietosuojan hallinta

Kunnan tietoturvallisuuteen ja tietosuojaan liittyvää toimintaa johdetaan ja kehitetään osana kunnan johtamisjärjestelmää. Tietosuojan ja tietoturvan hallinnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tämä tarkoittaa sitä, että tietosuojaan ja tietoturvaan liittyvät näkökohdat otetaan jo varhaisessa vaiheessa huomioon esimerkiksi erilaisissa hankinnoissa, sekä henkilötietojen käsittelyyn liittyvien toimintaprosessien suunnittelussa ja kehittämisessä.

3.2. Tietoturva- ja tietosuojatyön dokumentoiminen

Tietosuojan hallintamallin avulla kuvataan, miten tietosuojan ja tietoturvan hallinta on kunnassa organisoitu ja mitkä ovat ne kuvaukset, ohjeet ja dokumentit, joiden avulla rekisterinpitäjän osoitusvelvollisuutta todennetaan.

Kunnan tietosuoja- ja tietoturvatyöstä on dokumentoitu seuraavat kokonaisuudet:

- tietosuojatehtävät
- tietosuoja- ja tietoturvapolitiikka
- henkilötietojen käsittelyyn liittyvä ohjeistus
- seloste henkilötietojen käsittelytoimista
- henkilörekisterit
- tietosuojan vuosikello
- tietosuojavastaavan asema ja tehtävät
- tietojärjestelmä- ja tietovirtakuvaukset
- tietosuojariskit ja tietosuojaprosessit
- tietotilinpäätös

3.3. Henkilöstön osaaminen

Tuusulan kunta huolehtii henkilöstön riittävästä tietosuoja- ja tietoturvaosaamisesta
a) vuosittaisten henkilöstökoulutusten avulla
b) jokaisen työntekijän joka toinen vuosi suorittaman verkkokoulutuksen ja testin avulla

Lisäksi jokainen uudessa tehtävässä aloittava työntekijä perehdytetään kunnan perehdytyskäytäntöjen mukaisesti tietosuojan perusteisiin ja tietoturvan toteuttamiseen omassa työtehtävässään. Tietoturva- ja tietosuojaohjeet ovat kaikkien kunnan työntekijöiden saatavilla Intranetissä.

4. Tietoturvan ja / tai tietosuojan vaarantuessa - ilmoitusvelvollisuus

Tietoturvaloukkaus on oikeudeton puuttuminen tietoon tai tietojärjestelmään. Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Henkilötietojen tietoturvaloukkauksen (tietosuojaloukkaus) tapahtuessa Tuusulan kunta on rekisterinpitäjänä velvollinen ilmoittamaan poikkeamasta valvontaviranomaiselle ja tarvittaessa rekisteröidylle.

Valvontaviranomaiselle (Tietosuojavaltuutetun toimisto) tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä. Myös henkilötietojen käsittelijän on ilmoitettava kuntaan havaitsemastaan henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä.

4.1. Prosessi ja menettelytavat tietoturvaloukkaustilanteessa

Jos havaitset tietoturvaloukkauksen tai epäilet sellaisen tapahtuneen, ilmoita siitä välittömästi esimiehellesi ja turvallisuuspäällikölle.

4.2. Prosessi ja menettelytavat henkilötietojen tietoturvaloukkaustilanteessa

Jos havaitset henkilötietojen tietoturvaloukkauksen tai epäilet sellaisen tapahtuneen, ilmoita siitä välittömästi esimiehellesi ja tietosuojavastaavalle tai turvallisuuspäällikölle.

Lisätietoja saat Tuusulan kunnan Intranetistä löytyvästä dokumentista *Menettelytapaohje henkilötietojen tietoturvaloukkaustilanteissa.*