TUUSULAN KUNNANSÄÄDÖSKOKOELMA

TIETOTURVAPOLITIIKKA

Kunnanhallitus XX.X.2018 § XXX Voimaantulopv. X.X.2018

Tuusulan kunta
PL60
04301 Tuusula
www.tuusula.fi
puh. (09) 87 181

Sisällys

1 Johdanto

Tuusulan kunnan toiminta ja palvelut perustuvat enenevässä määrin tietoon. Ollakseen tehokkaasti hyödynnettävissä, tietoa tukevien järjestelyjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tämä edellyttää tehokasta johtamista luotettavien toteutusten ja osaavan henkilöstön tueksi.

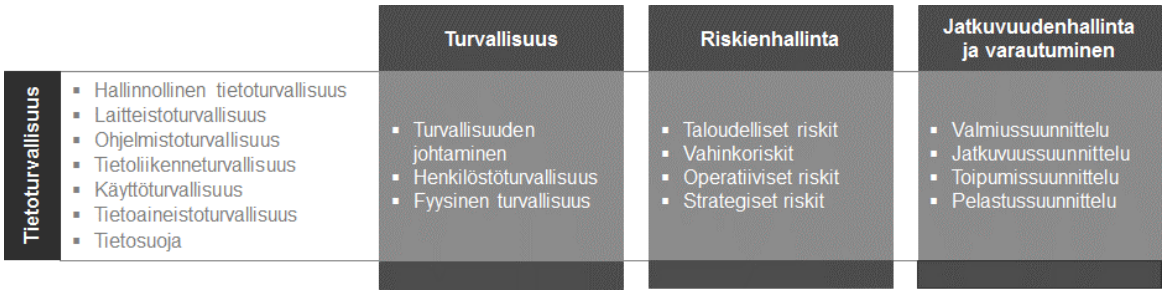
Kunnan johto määrittelee tässä Tuusulan kunnan tietoturvapolitiikassa tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet. Politiikka toimii perustana kunnan tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden käytäntöön soveltamisessa. Tietoturvapolitiikka ja sen soveltamisohjeet pidetään käyttäjien saatavilla intranetissä.

Tietoturvapolitiikka koskee koko kuntaorganisaatiota sekä kaikkia sen sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kunnan omistamaa tai hallinnoimaa tietoa. Politiikka kattaa kunnan käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2 Mitä tietoturvallisuus on?

Tietoturvallisuus on kiinteä osa kunnan johtamista, palveluita ja toimintoja. Lisäksi tietoturvallisuus liittyy jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin.

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



Kuva 1. Kunnan kokonaisturvallisuus

Tietoturvallisuuteen liittyvillä vastuilla ja käytännöillä pyritään varmistamaan, että kunnan omistama ja hallinnoima:

- tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena
- tieto on vain siihen oikeutettujen saatavilla
- tieto on saatavilla aina sitä tarvittaessa
- tietoon tehdyt muutokset sen käsittelyn eri vaiheissa on tarvittaessa kyettävä todentamaan.

2.1 Tietoturvallisuuden hallinta

Kunnan tietoturvallisuuteen liittyvää toimintaa johdetaan ja kehitetään osana kunnan johtamisjärjestelmää. Tietoturvallisuuden osalta kokonaisuus sisältää suunnitteluun, toteutukseen, seurantaan ja ohjaukseen liittyvät prosessit, asiakirjat, kontrollit ja vastuut.

Kunnan tietoturvatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- Kuntaa velvoittavat lait ja asetukset
- Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositukset
- Kunnan omat strategiat ja niistä johdetut vaatimukset
- Valtionhallinnon Tietoturvallisuuden johtoryhmän (VAHTI) ohjeet
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010).

2.2 Riskienhallinta sekä jatkuvuuden hallinta ja varautuminen

Kunnanvaltuuston hyväksymä ja kunnan johtoryhmän organisoima riskienhallintaprosessi toimii kunnan turvallisuusjärjestelyiden ja varautumisen perustan.

Riskienhallinnan tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että riskienhallintakeinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen. Riskienhallinta kattaa kaikki riskit, mukaan lukien tietoon kohdistuvat ja tiedosta aiheutuvat riskit.

Kunnan tulee varautua turvaamaan sen toiminnan ja palveluiden jatkuvuus normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Tätä varten kunta voi tarvittaessa laatia erillisiä suunnitelmia prosessien ja tietojärjestelmien tueksi.

3 Tietoturvallisuustavoitteet

Kunnan tavoitteena on saavuttaa valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) kuvaaman tietoturvallisuuden perustason vaatimukset koko kunnan laajuisesti ja korotetun tason vaatimukset lainsäädännön edellyttämissä toiminnoissa tai toiminnan tarpeiden niin vaatiessa.

4 Organisointi 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 kansliapäällikkö vastuussa sopivimman henkilön nimeämisestä kyseiseen rooliin. Kaikki roolit ja vastuut kuvataan liitteessä 1.

Kunnanhallitus hyväksyy kunnassa noudatettavan tietoturvapolitiikan (ja valvoo tietoturvapolitiikan toteutumista).

Kansliapäällikkö toimii tietoturvallisuuden ja tietosuojan omistajana kunnassa luoden edellytykset niiden asianmukaiselle toteuttamiselle. Tarvittaessa kansliapäällikkö nimeää vastuuhenkilöitä seuraamaan tietoturvan ja tietosuojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan tietosuojavastaavien sekä järjestelmien pääkäyttäjien tukena.

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

Tietojärjestelmän **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 tai tietoturvaselosteen laadinnasta ja nimeää rekisterin yhteyshenkilön

ICT-johtoryhmä 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 vikatilanteista ja käyttökatkoista ja huolehtii käyttökatkojen aikataulutuksista.

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

Tiedon ja tietojärjestelmien **käyttäjä** vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokaisen käyttäjän vastuulla on lisäksi tietoturvaan ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen viipymättä joko esimiehelle tai Tietojärjestelmäpalveluiden Helpdeskiin tai muuten virallisesti sovitulla tavalla.

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 kansliapäällikölle.

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

Tietosuojavastaava toimii kunnan erityisasiantuntijana henkilötietojen käsittelyyn liittyvissä asioissa. Tietosuojavastaava antaa asiantuntija-apua sekä kunnan henkilöstölle, että ennen kaikkea johdolle, jolla on rekisterinpitäjän vastuu henkilötietojen käsittelystä. Tietosuojavastaava raportoi kansliapäällikölle. Kunnassa on erillinen ohjeistus tietosuoja-asioista. Tarvittaessa toimialoilla nimetään toimialakohtainen tietosuojavastaava, jos lainsäädäntö tai toiminnan tarpeet niin edellyttävät.

5 Tiedon ja tietojärjestelmien käyttö

Kunnassa noudatetaan lainsäädännön tarkoittamaa hyvää tietojenkäsittelyn ja –hallinnan tapaa. Kunnan tietoja ja tietojärjestelmiä käytettäessä tulee noudattaa seuraavia tietoturvallisuutta edistäviä periaatteita ja sääntöjä.

1. Kunnan käytössä oleva tieto sekä tietojärjestelmät, laitteet ja ohjelmistot on tarkoitettu ensisijaisesti työtehtäviä varten.
2. Kunnan tietojärjestelmäympäristössä saa käyttää ainoastaan tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja.
3. Asennustyön saa suorittaa vain tietohallinto tai sen valtuuttama taho.
4. Kunnan toimintaa ja palveluita tukevat tietojärjestelmät tunnistetaan, luokitellaan kriittisyyden perusteella ja niille nimetään omistaja.
5. Käyttöoikeudet kunnan tietoon ja tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Toteutuksesta riippuen käyttöoikeudet hyväksyy käyttäjän esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.
6. Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi kunnan normaalein kurinpidollisin keinoin tai lainsäädännön edellyttämällä tavalla.
7. Tiedon turvalliset käsittelytavat ja tietoturvapoikkeamien hallintakäytännöt kuvataan erillisissä ohjeissa.

Tietoturvarikkomuksista voi olla seurauksena käyttöoikeuksien rajoituksia, työsuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia. Työsuhteeseen vaikuttavista seuraamuksista on säädetty ensisijassa työsopimuslaissa ja viranhaltijalaissa. Sovellettavaksi voivat tulla myös rikos- ja vahingonkorvauslainsäädäntö. Tietoturvarikkomuksista ilmoitetaan aina esimiehelle.

6 Tietoturvaosaamisen ja -tietoisuuden ylläpito

Jokainen uudessa tehtävässä aloittava työntekijä perehdytetään kunnan perehdytyskäytäntöjen mukaisesti tietoturvan perusteisiin ja tietoturvan toteuttamiseen hänen omissa työtehtävissään. Lisäksi tietoturvallisuuden peruskoulutusta on tarjolla säännöllisesti ja tietoturvaohjeet ovat kaikkien työntekijöiden saatavilla.

Tietoturvallisuuden ja tietosuojan ylläpidosta, kehittämisestä ja johtamisesta vastaaville tarjotaan riittävä hallinnollinen ja tekninen koulutus.

25.5.2018 lähtien sovellettavaksi astuva GDPR (General Data Protection Regulation) eli EU:n yleinen tietosuoja-asetus (2016/679) lisää rekisterinpitäjän vastuuta sen lukuun tapahtuvan henkilötietojen käsittelyn osalta. Tämä lisää kunnan johdon ja esimiesten vastuuta henkilöstön kouluttamisesta, jotta tietoturvaan ja tietosuojaan liittyvä osaaminen vastaa asetuksen edellyttämää tasoa.

Toimialan johto vastaa siitä, että henkilöstö noudattaa tietoturva- ja tietosuojaohjeistuksia ja esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta alaisessaan toiminnassa.

7 Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

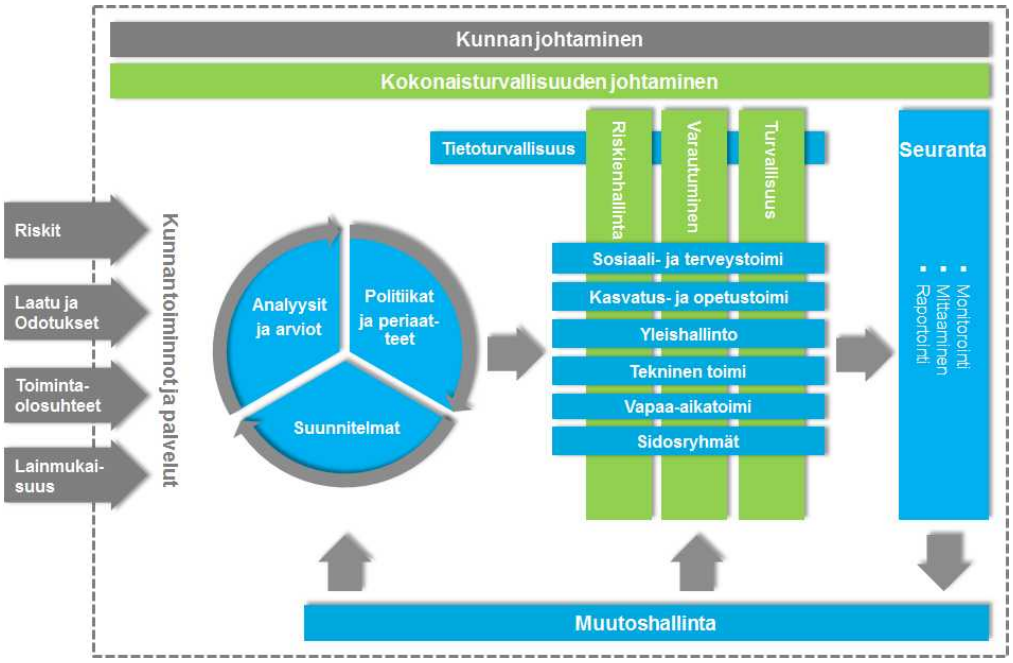
Kunnan tietoturvallisuustyö perustuu toiminnan, teknologian ja osaamisen jatkuvaan kehittämiseen seuraavassa kokonaisturvallisuusprosessissa kuvattujen vaiheiden mukaisesti:

SUUNNITTELU -vaiheessa tuotetaan analyysien ja arvioiden perusteella politiikkoja, periaatteita ja suunnitelmia. Tässä vaiheessa vaatimuksia asettavat mm. lainmukaisuus, riskienhallinnan tulokset, vaatimukset (asukkaat, asiakkaat, henkilökunta, sidosryhmät) ja toimintaolosuhteet.

TOTEUTUS -vaiheessa edellisen vaiheen tuotokset otetaan käyttöön kunnan toiminnassa.

SEURANTA -vaiheessa suoritetaan teknistä valvontaa ja hallinnollista seurantaa.

MUUTOSHALLINTA -vaiheessa seurantavaiheen tuloksista opitun perusteella toteutetaan muutoshallintaa kunnan normaalin muutoshallintaprosessin mukaisesti.



Kuva 2. Kunnan kokonaisturvallisuusprosessi

Kunnan tietoturvapolitiikka katselmoidaan lainsäädännön muuttuessa ja päivitetään tarvittaessa.

8 Liitteet

- LIITE 1: Käsitteet ja roolit
- LIITE 2: Lait, asetukset ja direktiivit
- LIITE 3: Tietoturvallisuuden perustason toteuttaminen (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa)