Savonlinna

TIETOTURVAPOLITIIKKA

Savonlinnan kaupunki

Keskushallinto, hallintopalvelut / Tietohallinto
22.5.2023

Savonlinna

Sisällys

1 JOHDANTO

"Tietoturvapolitiikka toimii perustana kaupungin tietoturvallisuutta koskeville ohjeille"

Savonlinnan kaupungin 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.

Kaupungin johto määrittelee tässä Savonlinnan kaupungin tietoturvapolitiikassa tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet. Politiikka toimii perustana kaupungin tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden käytäntöön soveltamisessa. Politiikka ohjeineen on henkilöstön saatavilla sähköisessä muodossa Santrassa. Tietoturvapolitiikan ja -ohjeiden noudattaminen on tärkeä osa kaupungin sisäistä valvontaa ja riskienhallintaa ja se koskee koko kaupunkikonsernia sekä kaikkia sen sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa. Politiikka kattaa kaupungin käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietoturvapolitiikan liitteinä olevia ohjeita päivitetään tarvittaessa esimerkiksi teknologioiden, lakien ja sopimusten muuttuessa.

ChatGPT-tekoälyohjelmalle 3/2023 toteutetun tietoturvapolitiikka-termiä koskevan kyselyn mukaan *"tietoturvapolitiikka on tärkeä osa organisaation tietoturvastrategiaa ja sen tarkoituksena on määritellä tietoturvan tavoitteet, periaatteet ja käytännöt. Tietoturvapolitiikka auttaa organisaatiota suojaamaan tietojärjestelmiään ja tietojaan mahdollisilta tietoturvauhilta, kuten tietomurroilta, haittaohjelmilta ja tietovarkauksilta. Tietoturvapolitiikan avulla organisaatio varmistaa myös, että sen toiminta on yhteensopiva soveltuvien lainsäädäntöjen ja säädösten kanssa.*

Tietoturvapolitiikassa tulee käsitellä seuraavia asioita:
***Tietoturvavastuu:** Politiikassa tulee määritellä organisaation tietoturvavastaavat ja heidän vastuualueensa.*
***Tietoturvaperiaatteet**: Politiikassa tulee määritellä organisaation tietoturvan keskeiset periaatteet ja niiden noudattamisvelvollisuus.*
***Tietoturvallisuuden hallinta:** Politiikassa tulee määritellä organisaation tietoturvallisuuden hallinnan prosessit, kuten riskienhallinta, tietoturvatarkastukset ja varautuminen tietoturvatapauksiin.*
***Käytännön tietoturvaohjeet:** Politiikassa tulee määritellä käytännön ohjeet, kuten salasanojen hallinta, tietojen luokittelu, tietoturvakoulutus ja tietojen hävittäminen.*
***Tietoturvan seuranta ja raportointi:** Politiikassa tulee määritellä tietoturvan seuranta- ja raportointiprosessit, jotta organisaatio voi arvioida tietoturvan tilaa ja tunnistaa mahdolliset riskit.*

Organisaation tulee varmistaa, että sen tietoturvapolitiikka on käytettävissä kaikille henkilöstöryhmille ja että se päivitetään säännöllisesti vastaamaan muuttuvia tietoturvavaatimuksia. Organisaation tietoturvapolitiikkaa tulee myös arvioida säännöllisesti sen tehokkuuden varmistamiseksi."

Digi- ja väestötietoviraston mukaan digitaalisella turvallisuudella eli digiturvalla pyritään varmistamaan, että digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla. Digitaalinen turvallisuus jakaantuu viiteen eri toteutusalueeseen, jotka on kuvattu oheisessa DVV:n esittämässä kuvassa.

Kuva 1. Digitaalisen turvallisuuden toteutusalueet DVV:N mukaan
(Digitaalisen turvallisuuteen voit tutustua DVV:n sivuilla: linkki, Mitä on digiturva?)

2 TIETOTURVALLISUUS OSANA DIGITURVALLISUUTTA

"Tietoturvallisuus liittyy jokaisen työntekijän/viranhaltijan arkipäivän työtehtäviin ja työtapoihin"

Tietoturvallisuus on kiinteä osa kaupungin johtamista, palveluita, työtehtäviä ja toimintoja. Tietoturva integroituu sekä fyysiseen että digitaalisen turvallisuuteen.

2.1 Tietoturvallisuus

Tietoturvalla varmistetaan tiedon luottamuksellisuus, eheys, saatavuus ja käytettävyys ja tätä kautta kaupungin palvelutuotannon, prosessien ja muiden toimintojen luotettavuus, laatu sekä jatkuvuus. Tietoturvallisuudesta huolehtiminen on myös edellytys tietosuojaperiaatteiden toteutumiselle. Tietosuojaperiaatteet on kuvattu tarkemmin Henkilötiedon käsittelyä koskevassa ohjeistuksessa sekä tämän politiikan liitteessä 8, Tietosuojapolitiikka.

2.1.1 Hallinnollinen tietoturvallisuus - johtaminen

Hallinnollisella tietoturvallisuudella tarkoitetaan tietoturvallisuutta koskevien järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Sen tarkoituksena on luoda organisaatioon tietoturvalliset toimintatavat luonnolliseksi osaksi kaikkea toimintaa. Toiminnasta vastaavat henkilöt huolehtivat resurssien riittävyydestä ja oikeasta kohdistamisesta sekä menettelytavoista.

Hallinnollinen tietoturvallisuus on kaikkien muiden tietoturvallisuuden osa-alueiden toteutuksen ja määrittelyn perusta. Sen avulla määritellään tietoturvallisuuden suuntaviivat ja turvallisuutta parantavat toimenpiteet. Tietoturvan kehittäminen ja ylläpito ovat osa organisaation yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietoturvan hallinnassa otetaan huomioon lainsäädännölliset vaatimukset ja vaikutukset. Palveluja ulkoistettaessa palveluntuottajia vaaditaan noudattamaan kaupungin tietoturvapolitiikkaan ja henkilötiedon käsittelyyn liittyviä sopimuksia, käytäntöjä sekä ohjeita.

Hallinnollisen tietoturvan periaatteet:

- Tietoriskit ennakoidaan ja niiden vaikutuksia hallitaan.
- Tiedon luotettavuus, virheettömyys ja laatu varmistetaan johtamisessa, päätöksenteossa, toiminnassa ja viestinnässä.
- Tiedon saatavuus ja käytettävyys varmistetaan riittävillä toimilla.
- Estetään tiedon tahaton tai tahallinen tuhoutuminen ja vääristyminen.
- Kaupungin tietoturvapolitikka viedään käytäntöön ohjeistamalla, kouluttamalla ja tiedottamalla, ja sen toteutuminen näkyy tietojärjestelmien käytössä ja tietojen käsittelyssä.

2.1.2 Henkilöstöturvallisuus

Henkilöstöön liittyvien riskien hallintaa kutsutaan henkilöstöturvallisuudeksi. Sen tavoitteena on ehkäistä henkilökuntaan suuntautuvia ja henkilökunnasta tulevia uhkia. Näitä riskejä voidaan torjua turvakartoituksilla, vastuun ja velvollisuuden selkeällä määrittämisellä, selkeillä ohjeilla toimenpiteistä, kun palvelussuhde päättyy ja sitouttamalla henkilö tietoturvalliseen toimintaan.

Henkilöstön mitoituksessa on huolehdittava siitä, että varmistetaan turvalliselle tietojenkäsittelylle välttämättömien henkilöresurssien riittävyys. Avainhenkilöille nimetään varahenkilöt, joiden osaaminen on sillä tasolla, että avainhenkilön puuttuminen (sairaus, tapaturma, vuosiloma, irtisanoutuminen) ei estä päivittäisiä toimintoja eikä vaaranna tietoturvaa. Oikealla henkilöiden valinnalla, töiden mitoittamisella ja niiden jakamisella sekä koulutuksella huolehditaan työtehtävien vaatiman osaamisen ja siihen liittyvän tietotekniikan osaamisen tasosta.

Lain yhteistoimintamenettelystä yrityksissä (334/2007) tavoitteena on edistää työnantajan ja henkilöstön välistä vuorovaikutusta. Yhteistyötoimikunta muodostuu työntekijöiden/viranhaltijoiden ja työnantajan edustajista. Tietoturvaan liittyvät valvontamenettelyt, ohjeet, sopimukset ja sanktiosäännökset on hyvä saattaa yhteistyötoimikunnan tiedoksi ja myös hyväksyttää ne siellä.

Kaupungin henkilöstöturvallisuus edellyttää, että toimialajohtajat ja esihenkilöt arvioivat mahdollisten tiedonhallintalain (906/2019) 12§:n mukaisten henkilöstöturvallisuusselvitysten tarpeellisuuden niissä työtehtävissä, joissa edellytetään erityistä luotettavuuden varmistamista. Lisäksi esihenkilöt huolehtivat, että kaikki henkilökuntaan kuuluvat suorittavat Navisec -tietosuoja- ja tietoturvaverkkokoulutuksen joka vuosi ja aina uuden palvelussuhteen alkaessa.

2.1.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan eri tallennusmuodoissa olevien tietojen suojaamista. Se koskee sekä paperiasiakirjoja että digitaalisessa muodossa olevia tallenteita, optisia ja magneettisia muistivälineitä, mikrofilmiä, äänitteitä tai muita vastaavia teknisiä laitteita.

Tietoaineistoturvallisuudella varmistetaan asiakirja- ja tietoaineistojen käytettävyys, oikeellisuus, eheys, luottamuksellisuus ja salassapito elinkaaren kaikissa vaiheissa. Tietoaineistoturvallisuuteen kuuluvat ne ulkoiset normit, jotka rajoittavat tai ohjaavat tietosisällön perusteella tehtävää tietojenkäsittelyä, kuten yleiset ja/tai erityisalan lait, asetukset, viranomaismääräykset ja kansallisarkiston päätökset. Tietoaineistojen käsittelyä on tarkemmin ohjeistettu seuraavissa asiakirjoissa: Asiakirjahallinnon ja arkistotoimen toimintaohje 2021 (linkki) ja Tietojen käsittely pilvipalveluissa -ohje 2023 (politiikan liite 4).

Kaupungilla on käytössä kaikki tietoaineistot kattava arkistonmuodostus- tai tiedonohjaussuunnitelma, josta ilmenee tietoaineiston käsittelysäännöt tietojen synnystä niiden tuhoamiseen asti, turvaluokitus sekä eheyden ja käytettävyyden varmistaminen aineiston elinkaaren kaikissa vaiheissa.

Organisaation johto vastaa henkilöstön perehdyttämisestä tietoaineistojen käsittelyohjeisiin. Tietoaineistojen tietoturvallisuuden varmistaminen koskee koko henkilöstöä ja tietoaineiston koko elinkaarta. Organisaation tietoaineistoturvallisuuden perustason edellytyksenä on, että henkilöstö tuntee ja noudattaa määräyksiä, suosituksia ja ohjeita toiminnassaan.

Tietoaineistoturvallisuuden periaatteet:

- tietoaineistojen luettelointi ja luokitus
- tietoaineistojen käsittelyn ohjeistus
- pääsynhallinta ja käyttöoikeusprosessit
- lukittavat säilytystilat
- tietoaineiston turvallinen hävitys
- salassapitosopimukset
- salaustekniikka
- dokumenttien tunnistetiedot
- henkilötiedon lainmukainen käsittely
- tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen

Riippumatta tiedon olomuodosta tietoturvallisilla toimilla tähdätään tietoaineistojen käytettävyyteen, eheyteen ja luottamuksellisuuden ylläpitämiseen. Edellä mainitut toimet kattavat tiedon koko elinkaaren alkaen tiedon syntymisestä tiedon hävittämiseen.

Tietoja käsiteltäessä on huolehdittava

- luottamuksellisen tiedon salassapidosta
- tiedon oikeellisuudesta siten, että käsiteltävä tieto on oikeaa ilmenemismuodostaan riippumatta
- tiedon käytettävyydestä siten, että tieto on sitä tarvitsevan ja siihen oikeutetun ihmisen tai järjestelmän käytettävissä

Tietoaineisto on suojattava virheiltä, tahattomalta menetykseltä, luvattomalta tai tahalliselta tuhoamiselta, käyttämiseltä, muuttamiselta tai joutumiselta ulkopuolisten käyttöön. Turvallisuusmenettelyt kohdistetaan tiedon käyttöön sen luomisesta käsittelyyn, säilytykseen, arkistointiin ja tietojen hävittämiseen asti.

Henkilöstöllä ja luottamushenkilöstöllä on tietojenkäsittelyn ja asiakirjaturvallisuuden osalta vain heidän työtehtäviensä suorittamisen kannalta välttämättömät käyttö- ja käsittelyoikeudet koskien syöttö-, käsittely- ja tulostusmateriaalia sekä muita asiakirjoja.

2.1.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistautumis- ja suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen määrittelyyn, suunnitteluun, kehittämiseen ja hankintaan sekä ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä (mm. versiointi, lisensointi ja muutoksenhallinta).

Ohjelmistoturvallisuudella varmistetaan ohjelmistojen toimivuus sekä käsiteltävien tietojen eheyden ja luotettavuuden säilyminen. Ohjelmistojen vastuuhenkilöt (järjestelmän omistajat ja pääkäyttäjät) määrittävät ja huolehtivat siitä, että ohjelmistoilla on riittävät suojausominaisuudet. Tietohallinto ja ict-asiantuntijat huolehtivat palvelimille asennettujen ohjelmistojen varmistuksista, palvelinten suojauksen teknisestä toteutuksesta, ylläpidosta ja valvonnasta ja ohjelmistojen vastuuhenkilöt (omistaja,

pääkäyttäjät) määrittelevät tietoturvan vaatimukset ja tason. Pääsynhallinnan suunnittelulla estetään ohjelmien ja järjestelmien luvaton käyttö.

Ohjelmistoturvallisuuden periaatteet:

- Käyttäjätunnukset ja salasanat ovat henkilökohtaisia.
- Järjestelmän omistaja päättää käyttöoikeuksista ja teknisen luvituksen tekee pääkäyttäjä tai keskitetysti tietohallinto.
- Ohjelmistojen ja järjestelmien käyttöön tulee aina saada perehdytys, josta vastaa järjestelmän vastuuhenkilöt.
- Ohjelmiston tietoturvallisuus ja tietosuoja tulee konsultoida ja hyväksyttää jo hankintavaiheessa tietoturva- ja tietosuojavastaavalla voimassaolevien lakien mukaisesti (mm. Tiedonhallintalaki, GDPR, Tietosuojalaki).
- Ohjelmistoista tulee olla olemassa varmuuskopiot.
- Ohjelmistojen tulee olla edelleen tuettuja mm. tietoturvapäivitysten osalta. Elinkaaren loputtua ei-tuettuja ohjelmistoja ei saa käyttää tietoturvariskien vuoksi vaan ne on korvattava ennen tuen päättymistä. Järjestelmän omistaja vastaa osaltaan järjestelmän ja tiedon elinkaaresta yhteistyössä tietohallinnon, arkistosihteerin ja tietosuojavastaavan kanssa.

Muita huomioitavia asioita:

- ajantasaiset käyttöoikeudet järjestelmiin
- käyttäjien hallinta, pääsyoikeudet, käyttäjien todennus
- tiedon elinkaaren hallinta, mukaan lukien arkistointi
- asianmukaiset päivitykset
- lisenssien hallinta
- arkkitehtuuriyhteensopivuus
- tietoturvalliset asennukset
- huolellinen ylläpito
- tukipalvelut
- varmistukset
- jäljitettävyys
- haittaohjelmien torjunta

Keskeisimmät tietojärjestelmät ja verkkosovellukset sekä niiden vastuuhenkilöt on kuvattu pääkäyttäjien/vastuuhenkilöiden ylläpitämässä tietojärjestelmäluettelossa, jonka ylläpito toteutetaan it-palvelunhallintajärjestelmässä (Efecte ITSM).

2.1.5 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan ict-laitteistojen (ml. mobiililaitteet) rakenteeseen, käyttöjärjestelmiin, ohjelmistoihin, laite- ja ohjelmistohuoltoon, keskitettyyn operointiin, varmistuksiin ja ict-laitteisiin pääsyn suojaukseen liittyvää turvallisuutta. Laitteistoturvallisuudella turvataan myös kaupungin laitteiston elinkaarta.

Laitteistoista on huolehdittava niin, että ne ovat niihin oikeutettujen henkilöiden käytettävissä sovittujen periaatteiden mukaisesti. Vierailijoilta on evätty pääsy henkilökunnan käytössä oleville laitteille. Laitteistohankinnassa kiinnitetään huomiota niiden yhteensopivuuteen, ylläpitoon ja saatavuuteen. Laitteistoturvallisuuteen kuuluvat laitteiston suojauksen, asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.

Lisäksi:

- Huolehditaan laitteiston elinkaareen liittyvistä palvelusopimuksista (esimerkiksi, että laitteistojen poistossa tietojen tuhoaminen hoidetaan lopullisesti).

- Huolehditaan sopimuksilla erityisesti tilanteita, joissa koko palvelu sijaitsee palveluntarjoajalla tai osa organisaation laitteista sijaitsee fyysisesti kaupungin tilojen ulkopuolella (ja vaaditaan selvityksiä).
- Huolehditaan, että järjestelmien tietoturvapäivityksiä varten on selkeät suunnitelmat ja ohjeet.
- Huolehditaan hankinnoissa ja sopimuksissa tietojärjestelmätoimittajien ja tietoinfrastruktuurin ylläpitäjän vastuut laitteistoturvallisuuden osalta.
- Laitteistojen ja niiden ohjelmistojen tulee olla edelleen tuettuja mm. tietoturvapäivitysten osalta. Elinkaaren loputtua ei-tuettuja laitteistoja ei saa käyttää tietoturvariskien vuoksi vaan ne on korvattava ennen tuen päättymistä.

2.1.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittää tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen ja verkon varmistamiseen liittyvät turvallisuustoimenpiteet. Tavoitteena on estää luvaton tunkeutuminen järjestelmiin tietoverkon kautta, paljastaa tunkeutumisyritykset, estää siirrettävän tiedon joutuminen sivullisten haltuun ja tarvittaessa estää sen käyttö sekä estää väärän tiedon syöttö tietojärjestelmiin.

Kaikki tietoliikenteeseen liittyvät tekniset toteutukset tulee hyväksyttää tietohallinnolla ennen hankintapäätöksiä.

2.1.7 Käyttöturvallisuus

Käyttöturvallisuus koostuu järjestelmien turvallisista käyttöperiaatteista, tiedonkäytön valvonnasta sekä jatkuvuuden turvaamisesta. Käyttöturvallisuuden avulla luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat olosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuus- ja suojauskopioinnista sekä häiriöraportoinnista. Periaatteena on luoda sellaiset menettelytavat, joilla päivittäisessä toiminnassa säilytetään tietojärjestelmien käytössä tietoturvallisuuden taso mahdollisimman hyvänä sekä asiakkaan että työntekijän/viranhaltijan kannalta.

Tietojärjestelmän käyttövaltuudet on määritelty ja dokumentoitu asianmukaisesti, haittaohjelmien torjunnassa noudatetaan annettuja ohjeita, tietojen sisällön käyttökelpoisuus ja saatavuus sekä atk-ohjelmien ylläpidon ja huollon saatavuus on varmistettu. Tietoturvallisuuden taso ml. käyttöoikeudet määritellään tietovarannoittain yhdessä järjestelmän omistajan/vastuuhenkilön ja tietohallinnon kesken ja toteutetaan Helpdeskin, järjestelmän pääkäyttäjän ja ict-palveluntuottajan toimesta. Ict-laitteiden käyttötiedostojen (datan) varmistuksista huolehtivat asianomaiset sovellusten käyttäjät. Käytännössä pääkäyttäjät, projektin vetäjät ja esihenkilöt huolehtivat sovellusten käyttötuen hankkimisesta ja tarvittavien kehitys- ja ylläpitotoimenpiteiden tekemisestä ohjelmistotoimittajien kanssa tietohallinnon konsultoimana ja hyväksyminä.

Käyttäjät vastaavat käyttöturvallisuudesta omalta osaltaan huolehtimalla, ettei työasema ole ulkopuolisen käytössä eikä muut käyttäjät tai ulkopuoliset henkilöt saa tietoonsa käyttäjän henkilökohtaisia salasanoja. Tietoturvapoikkeamiin kuten salasanojen ja käyttäjätunnusten kalasteluun, haittaohjelmiin ja muuhun sellaiseen tulee suhtautua vakavasti.

Tietohallinto ja/tai ict-palveluntuottaja vastaa laitteistojen ja ohjelmistojen huollosta ja korjauksista.

2.1.8 Fyysinen turvallisuus

Fyysisen turvallisuuden tavoitteena on tietojenkäsittelyn käyttöympäristön ja sen tilojen suojaaminen fyysisiltä vahingoilta ja häiriöiltä sekä luvattomalta pääsyltä tiloihin, laitteille ja tietoihin sekä ympärystekniikan toiminnan varmistaminen. Fyysinen turvallisuus käsittää kiinteistöjen rakenteellisen turvallisuuden, valvontatekniikan kuten kulunvalvonta-, paloilmoitus-, rikosilmoitus- ja kameravalvontajärjestelmät sekä valvonnan ja vartioinnin.

Käyttöympäristöllä tarkoitetaan niitä tiloja, joissa sijaitsevat palvelimet, mikrotietokoneet, lähiverkot, tietoliikennelaitteet, suunnittelu-, kehitys-, tulostus- ja jälkikäsittelytilat, tietojenkäsittelyn toimistotilat ja teletilat. Ympärystekniikka käsittää toimintaa tukevat ja sitä varmistavat tekniset järjestelmät kuten sähkönsyötön, ilmastoinnin ja lämmityksen.

2.2 Tietoturvallisuuden tavoitteet

Kaupungin tietoturvatyön päämäärä on turvata kaupungin toiminnalle tärkeiden palveluiden ja prosessien sekä niitä tukevien tietojärjestelmien ja tietoverkkojen riittävä toiminta (saavutettavuus), estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille (luottamuksellisuus) sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot (eheys).

Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen. Kaupungin toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Suunnittelussa ja ohjaamisessa tulee varautua niin pieneen, keskisuureen, kuin suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin.

Hyväksytyn tietoturvapolitiikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa kaupungin yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Kaupungin tavoitteena on saavuttaa Valtiohallinnon tietoturvallisuusasetuksen (681/2010) (linkki) kuvaaman tietoturvallisuuden **perustason** vaatimukset koko kaupungin laajuisesti ja korotetun tason vaatimukset lainsäädännön tai toiminnan tarpeiden niin vaatiessa.

2.3 Tietosuojan huomioiminen

Tietosuojan lähtökohdat tulevat yksilön perusoikeuksien ja –vapauksien suojaamisesta, erityisesti henkilön ja hänen perheensä yksityisyyden suojasta. Savonlinnan kaupungilla noudatetaan asiakkaiden ja henkilöstön sekä muiden sidosryhmien henkilötietojen käsittelyssä voimassa olevaa tietosuojan lainsäädäntöä. Toukokuusta 2018 lähtien EU:n yleinen tietosuoja-asetus velvoittaa rekisterinpitäjää osoittamaan, että henkilötietojen käsittelyssä noudatetaan lakia ja rekisterinpitäjän omia erillisiä ohjeita. Tietosuojalla turvataan henkilötietojen asianmukainen käsittely koko organisaation toiminnassa, varmistetaan tietojen oikeellisuus ja ennalta ehkäistään henkilötietojen käyttöön liittyviä loukkauksia.

Tietosuojan arvioinnin lisäksi tulee toteuttaa rekisterinpitäjän edustajan, tietoturva- ja tietosuojavastaavan konsultointi aina kun toiminnassa/palveluissa tapahtuu muutoksia tai toteutetaan hankintoja, joihin liittyy henkilötiedon käsittely. Henkilötiedon käsittelyn vastuut ja velvoitteet on huomioitava palvelusopimuksissa yhteistyötahojen kanssa. Vastuu henkilötietojen käsittelystä on rekisterinpitäjällä.

Henkilötiedon käsittelyn ohjeet on hyväksytty kaupunginhallituksessa 12/2019 ja ne löytyvät Santrasta (Linkki: Henkilöstölle/Tietosuoja/Henkilötiedon käsittely).

2.4 Tietoturvallisuuden hallinta

Kaupungin tietoturvallisuuteen liittyvää toimintaa johdetaan ja kehitetään osana kaupungin hallintojärjestelmää. Tietoturvallisuuden osalta kokonaisuus sisältää suunnitteluun, toteutukseen, seurantaan ja ohjaukseen liittyvät prosessit, asiakirjat, kontrollit ja vastuut.

Kaupungin tietoturvatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- Kaupunkia velvoittavat lait ja asetukset (mm. Tiedonhallintalaki, EU:n tietosuoja-asetus)
- Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (Tiedonhallintalautakunnan suositus)
- Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositukset
- Kaupungin strategia ja siitä johdetut vaatimukset
- Valtionhallinnon Tietoturvallisuuden (VAHTI) ohjeet
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
- Katakri 2020, Tietoturvallisuuden auditointityökalu viranomaisille (Kansallinen turvallisuusviranomainen)
- PiTuKri, Pilvipalveluiden turvallisuuden arviointikriteeristö (Traficom)
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö
- ISO/IEC 27001 -standardin hyödyntäminen kehittämisessä ja valvonnassa
- Kaupungin omat ohjeet: Hallintosääntö, Tietohallintosuunnitelma, Tiedonhallinnan vastuut, Asiakirjahallinnon ja arkistotoimen toimintaohje ja Henkilötiedon käsittelyn ohjeet sekä yksittäiset tietoturvan poikkeustilanteita koskevat erillisohjeet .

2.5 Riskienhallinta sekä jatkuvuuden hallinta ja varautuminen

Kaupunginhallituksen vastuulla oleva turvallisuus- ja valmiussuunnittelu sekä riskienhallinta ja pelastussuunnitelmat ovat kaupungin turvallisuusjärjestelyiden ja varautumisen perusta. 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.

Tietoturvaa ja tietosuojaa koskevien riskien arviointi on jatkuvaa, mutta erityistä huomiointia riskien arviointin pitää kiinnittää muutostilanteissa, kuten uutta järjestelmää hankittaessa tai palvelua suunniteltaessa. Lisäksi it-järjestelmä- sekä tietosuoja- ja tietoturvariskit tulevat kartoitetuksi tulosaluekohtaisesti toteutettavassa vuosittaisessa kokonaisvaltaisessa riskikartoituksessa.

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

3 ORGANISOINTI JA VASTUUT

Tietoturvallisuuteen liittyvillä vastuilla ja käytännöillä pyritään varmistamaan, että kaupungin omistama ja hallinnoima tieto on

- oikeaa ja eheää, eikä se ole muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena
- vain siihen oikeutettujen saatavilla
- saatavilla aina sitä tarvittaessa

Lisäksi tietoon tehdyt muutokset sen käsittelyn eri vaiheissa on tarvittaessa todennettavissa.

Tietoturvallisuuden vastuujako määrittelee vastuut käyttäjäyksikköjen ja tietohallinnon välillä. Tietohallinnon tehtävänä on teknisin ratkaisuin mahdollistaa tietoturvallinen työskentelytapa ja ympäristö.

Savonlinnan kaupunki on nimittänyt tietohallintopäällikön tietoturvavastaavaksi (hallintojohtaja-kaupunginlakimiehen henkilöstöpäätös §7/2021). Tietoturvavastaavan tehtävät ovat:

- toimii tietoturvallisuuden asiantuntijana ja tietoturvan kehittäjänä
- koordinoi ja valvoo tietoturvan toteutumista sekä raportoi johdolle tietoturvan tilasta ja kehittämistarpeista
- ylläpitää käyttöoikeusrekisteriä omistamiensa järjestelmien osalta
- valvoo ja toteuttaa teknistä tietoturvaa ja ryhtyy toimenpiteisiin tietoturvan ongelmatilanteissa
- toimii tietosuojavastaavan tukena tietosuojan vaikutusten arvioinneissa ja käyttölokivalvonnan teknisessä toteutuksessa
- valmistelee toimielimien hyväksyttäväksi kaupungin tietoturvapolitiikan sekä tietohallintosuunnitelman (ent. tieto- ja viestintätekniikkasuunnitelman) ja valvoo kaupungin tietoturvapolitiikan sekä tietohallintosuunnitelman (ent. tieto- ja viestintätekniikkasuunnitelman) toteutumista
- määrittää tietoturvakäytännöt ja -toimintatavat ja valvoo, että niitä noudatetaan
- laatii tietoturva- ja tietosuojakysymyksiin liittyvän ohjeistuksen yhdessä tietosuojavastaavan kanssa

Rekisterinpitäjällä on vastuu tietojenkäsittelyn turvaamisesta ja tietosuojan toteutumisesta omalla toiminta-alueellaan. Tietohallintopäällikkö/tietoturvavastaava, tietohallinto ja tietosuojavastaava toimivat tukena ja opastajana tietoturvallisuuteen liittyvissä asioissa.

Kullakin tietojärjestelmällä tulee olla omistaja. Tietojärjestelmän omistaja määrittelee henkilöt/tahot, jotka ensisijaisesti käyttää tietojärjestelmää tai sovellusta palveluissaan tai jota sovellus ensisijaisesti palvelee. Omistaja tai omistajan valtuuttamat pääkäyttäjät vastaa järjestelmän sisällöllisestä toimintavarmuudesta (mm. käyttöoikeudet) sekä oman toiminnan että tietojärjestelmästä riippuvien muiden toimintojen varmistamiseksi. Järjestelmän omistaja asettaa vaatimukset järjestelmän toiminnalle, tietoturvallisuudelle ja kehittämiselle sekä laatii järjestelmällä ylläpidettävistä rekistereistä lakien ja asetusten vaatimat selosteet. Järjestelmän omistaja määrittelee järjestelmän kriittisyyden tason kaupungin toiminnalle, joka toimii vaatimusmäärittelynä tietoturvalle ja tekniselle suunnittelulle.

Tiedonhallintalain mukaiset vastuut on määritelty hallintosäännössä ja Savonlinnan kaupungin tiedonhallinnan vastuut -dokumentissa (linkki).

4 TIEDON JA TIETOJÄRJESTELMIEN KÄYTTÖ

Kaupungin ict-kokonaisarkkitehtuurin periaatteet on kuvattu tarkemmin vuosittain päivitettävässä Tietohallinnon tietohallintosuunnitelmassa ja käytännön toteutuksesta vastaa tietohallinto.

Tietohallinto määrittelee kaupungin strategian perusteella yleiset tietotekniset linjaukset ja kokonaisarkkitehtuurin periaatteet, joiden mukaan kaupungin tietotekninen kokonaisuus ja ympäristö toteutetaan. Tietohallinnon tehtävänä on vastata kaupungin tietohallinnosta, kokonaisarkkitehtuurista, ict-palveluista, tietoturvasta, tieto- ja viestintätekniikkajärjestelmien valvonnasta, ylläpidosta ja kehittämisestä sekä toimia konsulttina kaupungin tietotekniikkahankkeissa.

Tietojärjestelmähankinnoissa tulee noudattaa kaupungin kokonaisarkkitehtuuriperiaatteita. Savonlinnan kaupungin toimialat ja liikelaitokset vastaavat omistajana järjestelmähankkeistaan ja niihin liittyvistä ict-sidonnaisuuksien kilpailutuksista ja toimittajasopimuksista, mutta esiselvitysten, kilpailutuksien, hankintojen ja sopimuksien tietotekninen ja tietoturva sisältö pitää aina konsultoida ja hyväksyttää

Tietohallinnossa ennen sopimista. Tällä varmistetaan yhteensopivuus Savonlinnan kaupungin tietoteknisiin linjauksiin, kokonaisarkkitehtuuriperiaatteisiin sekä tietoturvan ja tietosuojan vaatimuksiin ja ict-kustannuksien kokonaistaloudellisuus tulee huomioitua riippuvuuksineen.

Henkilöstön käytössä oleva tieto sekä tietojärjestelmät, laitteet ja ohjelmistot on tarkoitettu ensisijaisesti työtehtävien hoitamista varten. Työtehtävien ulkopuolisten internet-selailun ja asioiden hoitaminen on sallittu ja suositeltu vain yleisesti luotettavilla sivustoilla (esim. pankkiasiat, Kanta.fi-sivustot, yle.fi ja muut yleisesti luotetuksi tunnetut mediatalot ja web-sivustot). Tietohallinnon ylläpitämissä tietoturvapalveluissa on käytössä mm. URL-filteröinti, joilla estetään yleisesti epäluotettaville sivuille pääsy kaupungin IT-ympäristöstä.

Kaupungin tietojärjestelmäympäristössä saa käyttää ainoastaan tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja. Asennustyön saa suorittaa vain kaupungin tietohallinto tai sen valtuuttama taho.

Käyttöoikeudet kaupungin tietoon ja tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeuspyynnöt toteutetaan Helpdesk-järjestelmässä Tiedonhallintalain (906/2019, §17) lokitusvaatimuksen täyttämiseksi (linkki). Järjestelmän omistaja päättää käyttöoikeuksista ja teknisen luvituksen tekee pääkäyttäjä tai keskitetysti tietohallinto. (kts. politiikan liite 6). Peruskäyttöoikeudet muodostuvat henkilöstöjärjestelmän rooli- ja organisaatiotietojen perusteella automaattisesti.

Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi kaupungin normaalein kurinpidollisin keinoin (linkki Santran lomakkeisiin) tai lainsäädännön edellyttämällä tavalla, esim. tietosuojaloukkaukset (linkki Tietosuojavaltuutetun sivulle) ja tietomurrot (Linkki poliisin sivulle) ilmoitetaan aina lain vaatimalla tavalla viranomaisille.

5 TIETOTURVAOSAAMISEN JA -TIETOISUUDEN YLLÄPITO

Jokainen uudessa tehtävässä aloittava työtekijä perehdytetään kaupungin perehdytyskäytäntöjen mukaisesti tietoturvan perusteisiin ja tietoturvan toteuttamiseen hänen omissa työtehtävissään. Uuden työntekijän/viranhaltijan tulee suorittaa kaupungin Navisec -tietoturvan itseopiskelun verkkokoulutus kahden kuukauden kuluessa tehtävässä aloittamisesta. Jatkossa koulutus toteutetaan kerran vuodessa (kalenterivuosittain).

Ajantasaiset tietoturvaa ja tietosuojaa koskevat ohjeet löytyvät Santrasta.

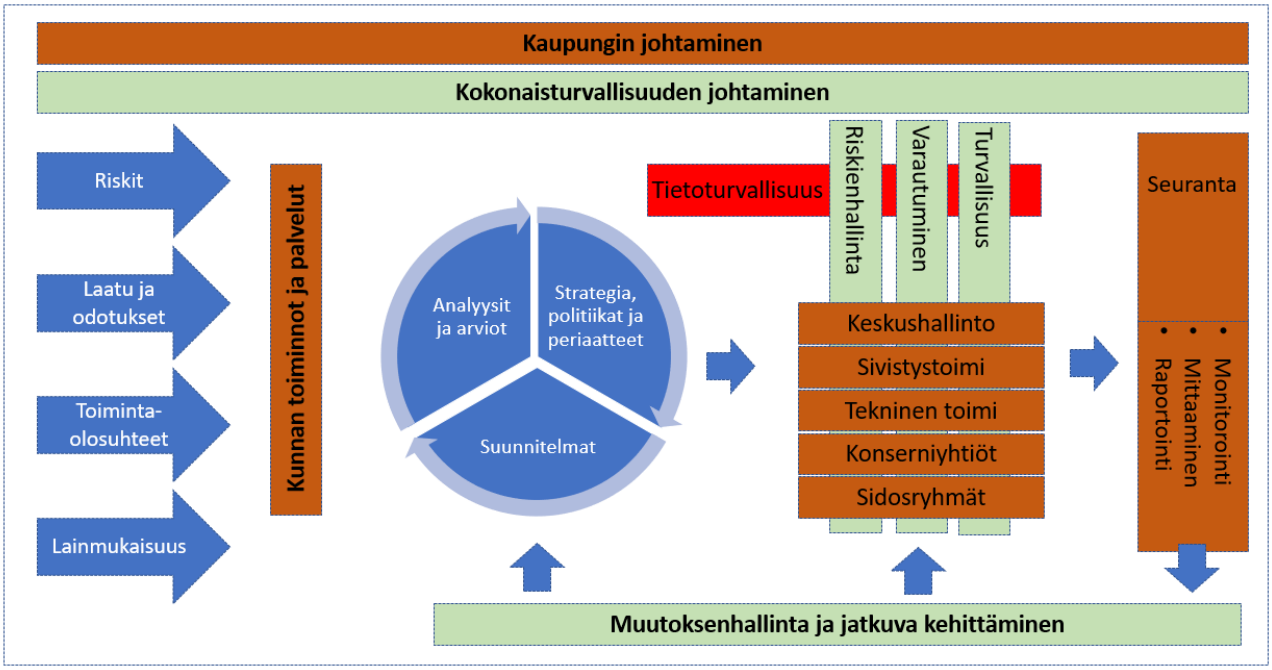
6 TIETOTURVALLISUUDEN SEURANTA, YLLÄPITO JA KEHITTÄMINEN

Jokaisen kaupungin IT-ympäristöä käyttävän velvollisuutena on tuntea sekä yleiset että omaa tehtäväänsä koskevat ohjeet tietoturvasta sekä tietosuojasta ja noudattaa niitä. Työntekijöiden/viranhaltijoiden tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista esimiehelle, tietohallintopäällikölle/tietoturvavastaavalle ja/tai Helpdeskiin ja/tai tietosuojavastaavalle.

Rekisterinpitäjän (tai tietosuojavastaavan) on ilmoitettava ilmenneestä henkilötietoihin kohdistuneesta tietoturvaloukkauksesta erillisen arvioinnin perusteella tietosuojaviranomaiselle 72 tunnin kuluessa siitä, kun loukkaus on tullut rekisterinpitäjän tietoon. Ilmoitus tulee tehdä myös rekisteröidylle, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille.

Kaupungin tietoturvallisuustyö perustuu toiminnan, teknologian ja osaamisen jatkuvaan kehittämiseen seuraavassa prosessissa kuvattujen vaiheiden mukaisesti:

- **SUUNNITTELU**-vaiheessa tuotetaan analyysien ja arvioiden perusteella politiikkoja, periaatteita ja suunnitelmia.
- **TOTEUTUS**-vaiheessa edellisen vaiheen tuotokset otetaan käyttöön kaupungin toiminnassa.
- **SEURANTA**-vaiheessa suoritetaan teknistä valvontaa ja hallinnollista seurantaa.
- **MUUTOSHALLINTA**-vaiheessa seurantavaiheen tuloksista opitun perusteella toteutetaan muutoshallintaa kaupungin normaalin muutoshallintaprosessin mukaisesti.



Kuva 2. Kaupungin kokonaisturvallisuusprosessi

Tämä tietoturvapolitiikka katselmoidaan vuosittain ja päivitetään tarvittaessa.

Liitteet:

Liite 1: Tietosuojan ja tietoturvan perusohjeet ja määräykset
Liite 2: Henkilöstön tietoturvaohje
Liite 3: Etätyöohje
Liite 4: Tietojen käsittely pilvipalveluissa
Liite 5: Sosiaalisen median ohje
Liite 6: Ohje esihenkilöille henkilöstön käyttäjätunnuksista
Liite 7: Deltagon turvaposti
Liite 8: Tietosuojapolitiikka
Liite 9: Valtakirja henkilökohtaisen levyaseman tietoihin