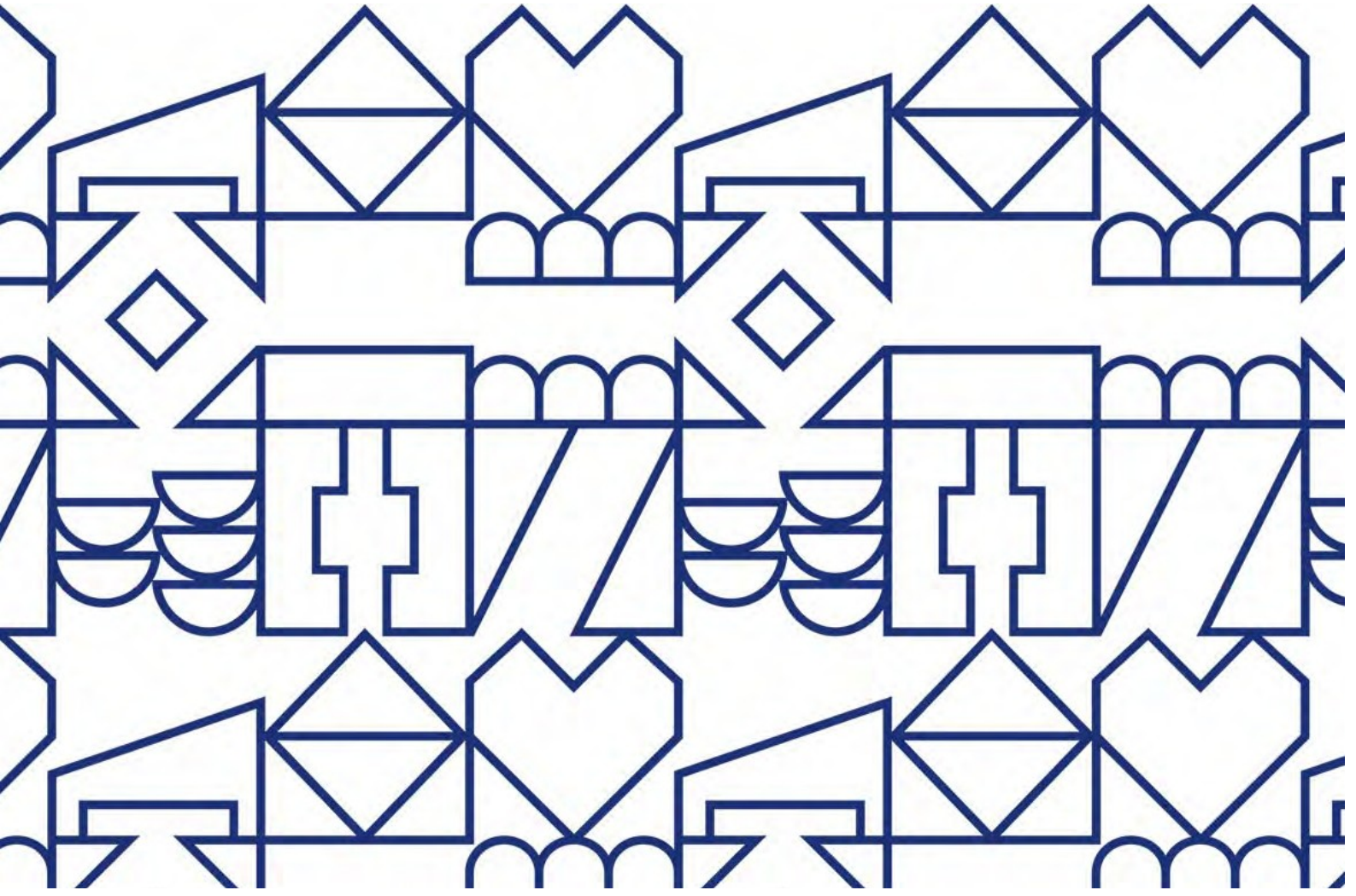
Seinäjoki

Seinäjoen kaupungin tietoturvapolitiikka

Kh 14.5.2018, § 149



Sisällys

Johdanto

Seinäjoen kaupungin vetovoimatekijä on hyvät palvelut. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn Seinäjoen kaupungin ja sen konsernin toimintaympäristöissä. Kaupungin palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta.

Seinäjoen kaupungin strategiassa vuosille 2018–2025 on todettu, että digitalisaatiota hyödynnetään ajasta ja paikasta riippumattomien palveluiden kehittämiseksi. Digitalisaatiota edistetään kaupungin kaikissa toiminnoissa vuorovaikutteisesti asukkaiden kanssa. Kaupunki vaikuttaa omilla toimillaan siihen, että kaupunkilaisilla on tasa-arvoiset mahdollisuudet digitalisaation hyödyntämiseen. Digitalisointi edellyttää tietoturvallisuuden kaikkien osa-alueiden, kokonaisarkkitehtuurin ja yhteen toimivuuden laajaa huomioimista jo suunnitteluvaiheessa.

Seinäjoen kaupungin konserniohjeessa todetaan tavoitteena olevan, että Seinäjoki-konsernissa käytetään samoja järjestelmiä sekä noudatetaan yhteisiä tietohallinnon strategioita ja toimintaohjeita. Konserniyhteisön tietojärjestelmät suunnitellaan ja toteutetaan yhteistyössä kaupungin tietohallinnon kanssa silloin, kun siihen on mahdollisuus.

Tietoturvallisuuden näkökulmasta konserniohjetta tulee soveltaa niin, että yhteistyön mahdollisuudet tulee aina selvittää ennen tietojärjestelmien toteuttamista.

Tässä tietoturvapolitiikassa määritellään Seinäjoen kaupungin johtamista, palveluita ja toimintoja koskevat tietoturvallisuuden periaatteet, tavoitteet, vastuut ja toteuttamistavat. Tietoturvapolitiikka toimii perustana tietoturvallisuutta koskeville muille ohjeistuksille, joiden tehtävänä on tarkentaa tietoturvapolitiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietoturvapolitiikka koskee kaikkia kaupungin palveluksessa olevia ja luottamushenkilöitä. Tietoturvapolitiikka koskee myös kaupunkikonserniin kuuluvia yhteisöjä ja säätiöitä sekä niitä Seinäjoen kaupungin sidosryhmien edustajia, jotka työnsä tai toimeksiantojensa puitteissa käsittelevät Seinäjoen kaupungin omistamaa tai hallinnoimaa tietoa. Tietoturvapolitiikka kattaa kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä tietoturvapolitiikka on saatavissa asianhallintajärjestelmässä (LAARI), intranetin sivuilla (AALTONETTI) ja se julkaistaan kaupungin internetsivulla. Tietoturvapolitiikka liitetään tarvittaessa Seinäjoen kaupungin toimeksiantosopimuksiin ja hankintasopimuksiin.

Tietoturvallisuuden merkitys kaupunkikonsernille

Uudet lainsäädäntömuutokset, erityisesti 25.5.2018 sovellettavaksi tuleva EU:n yleinen tietosuoja-asetus (GDPR), vahvistavat luonnollisten henkilöiden oikeutta henkilötietojen suojaan. Tietosuojalaki ja EU:n saavutettavuusdirektiivi tähtäävät tietoturvan, tietosuojan, riskienarvioinnin, kokonaisarkkitehtuurin ja yhteen toimivuuden huomioimiseen suunnittelussa ja sen kautta saatavaan kustannustehokkuuteen ja tietojen käytettävyyteen.

Tietoturvallisuuden toteutumiseksi kaupunkikonsernissa tulee tunnistaa sen toiminnan kannalta elintärkeät palvelutehtävät ja määritellä niiden turvaamiseksi riittävät tietoturvaperiaatteet. Tietoturvallisuuden toteutumista tukevat käytännöt ja ohjeistukset, joita ovat muun muassa; hanke ja projektisuunnittelun tietoturvan ja tietosuojan tarkastuslistat, puite-, palvelu- ja toimitussopimukset sekä niihin liittyvät turvallisuus- tai tietoturvasopimukset, ohjeistukset riskienhallinnasta sekä toimialakohtaisesta tietojenkäsittelystä. Suunniteltujen kuvattujen käytäntöjen toteutumista valvotaan säännöllisesti.

Tietoturvallisuuden määritelmä ja tavoitteet

Tietoturvallisuus koostuu tietoturvaan ja tietosuojaan liittyvistä vastuista ja käytännöistä, joilla pyritään varmistamaan tietojen, tietojärjestelmien ja palvelujen suojaaminen ja turvaaminen siten, että niiden luottamuksellisuus, eheys ja saatavuus voidaan taata ja osoittaa toteutuneen.

- Luottamuksellisuus: Tiedot, tietojärjestelmät ja palvelut ovat vain niihin oikeutettujen saatavilla eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon.
- Eheys: Tiedot, tietojärjestelmät ja palvelut ovat oikeita ja eheitä, eivätkä muuttuneet tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- Saatavuus: Tiedot, tietojärjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä hyödynnettävissä.

Tietosuojaa käsitellään tarkemmin Seinäjoen kaupungin tietosuojapolitiikassa.

Kuva 1. Tietoturvallisuus integroituu kuvan mukaisesti kaikkiin kokonaisuuden osa-alueisiin: turvallisuus, riskienhallinta sekä jatkuvuudenhallinta ja varautuminen. Kaupungin johdon vastuulla on huolehtia tietoturvallisuuden integroimisesta kaupungin operatiiviseen toimintaan.

Tietoturvatoimintaa ohjaavat tekijät

Seinäjoen kaupungin tietoturvallisuutta velvoittavat ja ohjaavat yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lisäksi muut tietoturvallisuutta ohjaavat velvoitteet, määräykset ja ohjeet kuten esimerkiksi toimittajien kanssa tehdyt turvallisuussopimukset. Lisäksi noudatetaan soveltuvin osin muuta tietoturvaan liittyvää ohjeistusta (mm. JUHTA/VAHTI).

Seinäjoen kaupungin johdon tehtävänä on ohjata tietoturvallisuuden kehittämistä strategisella tasolla yhdessä tietoturvasta vastaavien kanssa.

Seinäjoen kaupungin tietoturvallisuutta ohjaavasta lainsäädännöistä pidetään ajantasaista luetteloa, joka on nähtävissä asian hallintajärjestelmässä (LAARI) ja kaupungin intranetissä (AALTONETTI).

Tietoturvallisuuden organisointi ja vastuut

Seinäjoen kaupungin tietoturvavastuut on kuvattu liitteessä 1.

Tietoturvavastuut Seinäjoen kaupungin ja keskeisten sidosryhmien ja yhteistyökumppaneiden osalta tulee kuvata ja sopia kirjallisesti. Tietoturvavastuista sopimisesta vastaavat kyseisistä palveluista vastaavat henkilöt yhteistyössä tietosuojatyöryhmän ja tietohallinnon kanssa.

Seinäjoen kaupunkikonsernin tietoturvaa koskevan tietoturvapolitiikan ja sen muutokset hyväksyy kaupunginhallitus. Yksittäisten tietoturvaa koskevan ohjeistuksesta poikkeavan menettelyn hyväksyy tietosuojatyöryhmä. Tietoturvastandardit sekä tietoturvaohjeet ja niiden muutokset hyväksyy tietosuojatyöryhmä.

Tiedon ja tietojärjestelmien käyttö

Seinäjoen kaupungin henkilöstönsä käyttöön luovuttamat laitteet, ohjelmistot, tietojärjestelmät sekä tieto on tarkoitettu työtehtävien hoitamiseen. Seinäjoen kaupungin tietojärjestelmä-ympäristössä saa käyttää ainoastaan tietohallinnon ja tietohallinnon ohjausryhmän hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja. Asennustyöt suorittaa tietohallinto tai Seinäjoen kaupungin kanssa sopimussuhteessa olevat toimijat, esimerkiksi ICT-palveluntuottajat, järjestelmä- ja laitetoimittajat. Kaupungin ja näiden toimijoiden välisissä sopimuksissa tulee huomioida tietoturvaan ja tietosuojaan liittyvät vastuut ja velvoitteet.

Jokainen Seinäjoen kaupungin henkilöstöön kuuluva sitoutuu tietojen ja tietojärjestelmien tietoturvalliseen ja ohjeiden mukaiseen käyttöön allekirjoittamalla tätä koskevan sitoumuksen. Vastaavasti sitoumus edellytetään niiltä Seinäjoen kaupungin luottamushenkilöiltä, joille sallitaan oikeus käyttää Seinäjoen kaupungin omistamia tietojärjestelmiä.

Seinäjoen kaupungin omistamat tietojärjestelmät tunnistetaan ja niille nimetään omistajaksi organisaatioyksikkö, jonka vastuulla on tietojärjestelmän käyttövaltuushallinta.

Tietoturvallinen toimintatapa on kuvattu tietoturvaohjeissa. Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi.

Tietojen luokittelu

Seinäjoen kaupungin omistamat tiedot luokitellaan tiedon omistajan toimesta. Tietojen luokittelu perustuu lakiin viranomaisten toiminnan julkisuudesta ja konsernipalveluiden antamiin ohjeisiin lain soveltamisesta.

Tietoturvaosaamisen ja -tietoisuuden ylläpito

Jokainen Seinäjoen kaupungin työntekijä, jonka tehtävät edellyttävät tietoturvaohjeistuksen osaamista, saa opastuksen tietoturvaohjeiden sijainnista sekä tietoturvan organisoinnista Seinäjoen kaupungissa sekä suorittaa perehdytyskäytäntöjen mukaisen tietoturvan perusteet sisältävän verkkokoulutuksen.

Tietoturvaohjeet ovat jokaisen henkilöstöön kuuluvan saatavissa asianhallintajärjestelmässä (LAARI) ja kaupungin intranetissä (AALTONETTI).

Tietoturvallisuuden ylläpidosta, kehittämisestä ja johtamisesta vastaaville tarjotaan mahdollisuus riittävän perus- ja jatkokoulutuksen hankkimiseen.

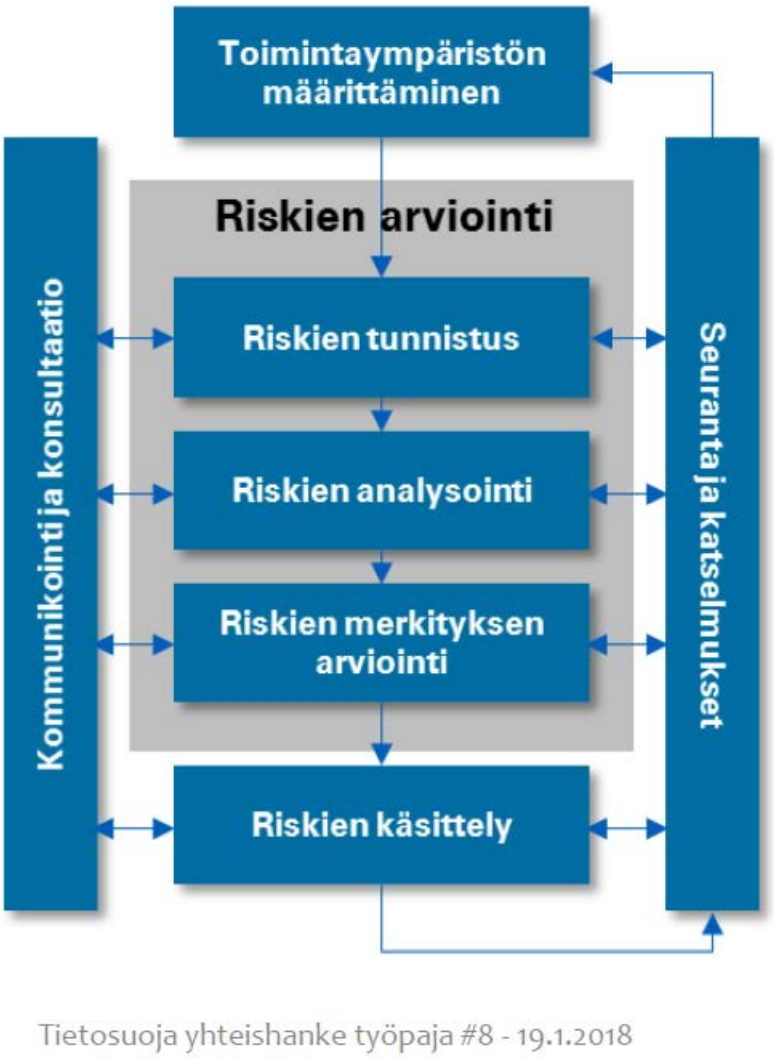
Tietoturvallisuudesta tiedottaminen

Tietoturvallisuuteen liittyvä henkilöstön tiedottaminen ajankohtaisasioista, ohjeista ja poikkeamatilanteista tehdään pääsääntöisesti intranetissä (AALTONETTI). Jokainen esimies on velvollinen seuraamaan ja varmistamaan, että henkilöstö seuraa tiedotteita.

Teknistä tietoturvaa tuottavien ulkopuolisten ICT- palveluntuottajien kanssa sovitaan kirjallisesti poikkeamatilanteiden tiedotusmenettelyistä ja yhteyshenkilöistä palvelusopimuksia tehtäessä materiaali- ja tietohallinnon toimesta.

Tietoriskien hallinta

Tietoriskien hallinnan perusta on niiden tunnistaminen ja vaikutusanalyysin muodostaminen sekä tarvittavista toimenpiteistä päättäminen riskien hallitsemiseksi. Seinäjoen kaupungin tietojen turvaamistoimet mitoitetaan riskien mukaisesti yhteistyössä tiedon omistajan ja tietohallinnon toimesta.



Kuva 2. Esimerkki tietoriskien hallintaprosessista.

Toiminta häiriötilanteissa ja poikkeusoloissa

Kaupungin varautuminen häiriötilanteisiin ja poikkeusoloihin perustuu lakisääteiseen valmiussuunnitteluun. Kaupungin palveluista vastaavat toimialat, konsernipalvelut sekä liikelaitokset, laativat kukin omat valmiussuunnitelmansa Seinäjoen kaupunginhallituksen hyväksymän valmiusohjeen mukaisesti. Suunnitelmat muodostavat yhdessä Seinäjoen kaupungin valmiussuunnitelman. Kaupungin varautumista johtaa kaupunginjohtaja yhdessä kaupunginhallituksen kanssa.

Seinäjoen kaupunginvaltuusto hyväksyy kaupunkikonsernia koskevat Sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa.

Seinäjoen kaupungissa on määritetty toimintaprosessi ja ohje liittyen toimintaan tietoturva-loukkausten ja tietosuojapoikkeamien tapahtuessa. Tämän prosessin mukaista toimintatapaa noudatetaan ko. tilanteissa.

Seinäjoen kaupungin on rekisterinpitäjänä ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle, jos siitä voi aiheutua riski luonnollisen henkilön oikeuksille tai vapauksille.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava valvontaviranomaiselle ilman aiheetonta viivästystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun Seinäjoen kaupunki rekisterinpitäjänä on tullut tietoiseksi tietoturvaloukkauksesta.

Henkilötietojen tietoturvalaukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Asiasta on ilmoitettava rekisteröidylle ilman aiheetonta viivästystä, jotta hänellä on mahdollisuus suojata itseään. Ilmoitus rekisteröidylle henkilötietojen tietoturvaloukkauksesta voidaan jättää tekemättä vain tietosuoja-asetuksessa määritellyissä tilanteissa.

Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Seinäjoen kaupungin tietoturvallisuustyö perustuu toiminnan, teknologian ja osaamisen jatkuvaan kehittämiseen tietoturvan hallinnan prosessin kuvauksen mukaisesti noudattaen jatkuvan kehittämisen periaatteita:

SUUNNITTELU - vaiheessa tuotetaan johdon ja tietoturvasta vastaavien toimesta analyysien ja arvioiden perusteella politiikkoja, periaatteita ja suunnitelmia. Tälle vaiheelle vaatimuksia asettavat mm. lainsäädäntö, riskienhallinnan tulokset, vaatimukset (sopimukset, asiakkaat ja sidosryhmät) sekä toimintaolosuhteet.

TOTEUTUS - vaiheessa edellisen vaiheen päätökset ja suunnitelmat otetaan käyttöön, tiedotetaan ja jalkautetaan niin henkilökunnalle kuin yhteistyökumppaneille ja asiakkaille.

SEURANTA - vaiheessa suoritetaan tietoturvallisuuden teknistä valvontaa ja raportointia sekä arvioidaan ratkaisevatko toteutetut toimenpiteet tunnistettuja tietoturvariskejä ja vähenivätkö ne suunnitellulle tasolle.

MUUTOSHALLINTA - vaiheessa toteutetaan muutoshallintaprosessin mukaista normaalia muutoshallintaa seurantavaiheen tuloksista opitun perusteella.

Kuva 3. Seinäjoen kaupungin tietoturvallisuustyön jatkuva kehittäminen

Liitteet

Liite 1 Tietoturvavastuut
Liite 2 Keskeiset käsitteet
Liite 3 Tietoturvallisuuden osa-alueet

Tietoturvavastuut Seinäjoen kaupungissa

Tämä dokumentti kuvaa tietoturvallisuuden vastuut ja velvollisuudet Seinäjoen kaupungissa. Tietoturvallisuuden vastuujärjestelyn tulee seurata kaupungin toiminnan mahdollisia muutoksia.

Tietoturvallisuuden valvontaan ja ylläpitämiseen osallistuu jokainen kaupungin henkilöstöön ja järjestelmien ja palveluiden käyttäjiin kuuluva osana omaa yleistä toimintavastuutaan.

Suurin osa tietoturvallisuuden toteuttamiseksi tehdystä työstä sisältyy Seinäjoen kaupungissa työskentelevien normaaleihin tehtäviin. Tietoturvallisuuden ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä turvallisuusvastuuhenkilöitä.

Tietoturvallisuuden vastuunjako

VASTUUTAHO	TEHTÄVÄ
Kaupunginhallitus	Tietoturvapolitiikan hyväksyminen Valmiusohjeen hyväksyminen
Kaupunginjohtaja	Tietosuojatyöryhmän nimeäminen
Kaupungin johtoryhmä	Tiedon ja tietojärjestelmien omistajien nimeäminen Tietoturvan toteutumisen valvonta Tietoturvan hallintaprosessien hyväksyminen Tietoturvapolitiikan ja riskienhallinnan sekä valmiussuunnittelun yhteensovittaminen Tietoturvallisuuden poikkeustilanteiden prosessien hyväksyminen
Hallintojohtaja	Tietosuojatyöryhmän johtaminen Tietoturvallisuutta koskevien asioiden raportointi ja valmistelu kaupungin johtoryhmälle ja kaupunginhallitukselle Tietoturvapoikkeustilanteiden koordinointi
Tietosuojatyöryhmä	Tietoturvapolitiikan valmistelu ja ylläpito Tietoturvan toteutumisen valvonnan suunnittelu ja seurannan järjestäminen Tietoturvaohjeiden- ja käytäntöjen kehittäminen, valmistelu ja muutosten hallinta Tietoturvallisuuden hallintaprosessien suunnittelu ja valmistelu Tietoturvallisuuden poikkeustilanteiden prosessien suunnittelu ja valmistelu
Tietohallinnon ohjausryhmä	Organisaation teknisten tietoturvaratkaisujen hyväksyminen tietohallinnon valmistelun pohjalta Tietoturvallisuuden kehittämishankkeiden hyväksyntä

Tietohallinto	Organisaation tietoturvaratkaisujen määrittäminen ja kehittäminen Keskitettyjen tietoturvallisuuden kehittämishankkeiden valmistelu ja toteutus Tietoturva-asioista viestittäminen Järjestelmien tietoteknisen tietoturvan suunnittelu, toteutus ja valvonta Tietoturvan hallinnointi ja koordinointi
Tietosuojavastaavat	Tietosuoja-asioiden neuvonta ja opastus Tietosuojasääntöjen noudattamisen seuranta Vaikutusten arviointien valvonta ja niiden tekemisen neuvonta Yhteistyö valvontaviranomaisen kanssa Tietosuojakoulutuksen suunnittelu, organisointi ja toteuttaminen Yhteyshenkilönä toimiminen rekisteröidyille Tietosuojatyöryhmän toimintaan osallistuminen
Tulosaluejohtajat / Esimiehet	Tietoturvan toteutuminen oman organisatorisen vastuu-alueensa osalta Yksikkökohtaisten erityisvaatimusten määrittäminen Tiedon omistajien määrittäminen johtamisjärjestelmän vastuiden mukaisesti Oman yksikkönsä tietoturvakoulutukseen osallistumisesta huolehtiminen Vastaa, että yksiköllä on sen oman toiminnan erityisvaatimukset huomioiden tarkennetut tietoturvatavoitteet ja periaatteet Raportoi tietoturvaa koskevista asioista annetun ohjeistuksen mukaisesti esimiehiään, tietosuojavastaavaa sekä tietohallintoa.
Tiedon omistaja	Tietoturvallisuuden varmistaminen tiedon koko elinkaaren ajan lakien, asetusten, tietoturvapolitiikan ja ohjeiden mukaisesti.
Tietojärjestelmien omistajat	Käyttövaltuushallinnan määrittely, kuvaaminen, toteutus ja ohjeistus Tietojärjestelmän käytönaikainen tietoturvallisuus. Pääkäyttäjien nimeäminen vastuullaan olevien järjestelmien osalta.
Pääkäyttäjä	Tietojärjestelmien sisäisten käyttövaltuuksien tekninen toteutus
Tiedon käsittelijä	Tiedon tietoturvallinen käsitteleminen ja ohjeiden noudattaminen
Liikelaitosten- ja konsernin tytäryhtiöiden johtajat	Oman liikelaitoksen tai yhtiönsä tietoturvatyön johtaminen ja organisointi konserniohjeistuksen mukaisesti

Tietoturva
Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta.

Tietosuoja
Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä.

Tietoturvapolitiikka
Johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvasuunnittelu
Suunnitteluprosessi, johon kuuluu muun muassa uhka-analyysi, perusturvallisuuden määrittely sekä toipumisvalmiuden ja poikkeusolojen valmissuunnittelu, ja jonka tuloksena on tietoturvasuunnitelmia, -linjauksia ja - ohjeistoja.

Tietoaineistoturvallisuus
Tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Eheys
Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Käytettävyys
Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Luottamuksellisuus
Henkilötietojen käsittely tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä

https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

Tietoturvallisuuden osa-alueet

- **Hallinnollinen turvallisuus**
  Hallinnollinen tietoturva koostuu johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista ja valvonnasta.
- **Ohjelmistoturvallisuus**
  Käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.
- **Tietoaineistoturvallisuus**
  Tietoaineistoturvallisuudella säilytetään asiakirjojen, tietueiden ja tiedostojen luottamuksellisuus sekä estetään tietojen tuhoutuminen tai tahaton muuttuminen. Oleellista on myös tallenteiden suojaaminen ja oikeanlainen säilyttäminen. Tietoaineistoturvallisuuteen liittyvät tiedon jatkuva varmistaminen, asianmukainen säilytys sekä hävittäminen.
- **Käyttöturvallisuus**
  Käyttöturvallisuutta ovat mm. salasanat, käytössä olevien ohjelmien osaaminen ja virustentorjunta. Annettujen käyttöoikeuksien tulee olla mukautettu työtehtäviin. Käyttöturvallisuus koostuu järjestelmien turvallisista käyttöperiaatteista, tietojenkäsittelytapahtumien valvonnasta sekä jatkuvuuden turvaamisesta. Laitteiden käyttövarmuus on myös käyttöturvallisuutta. Laaditaan ns. toipumissuunnittelu, jonka avulla varmistetaan toiminnan jatkuminen jonkun yllättävän tilanteen ilmaantuessa.
- **Laitteistoturvallisuus**
  Tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.
- **Fyysinen turvallisuus**
  Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden. Fyysinen turvallisuus koostuu monesta eri osatekijästä, turvallisuuden perusta kuitenkin luodaan jo rakennus- vaiheessa.
- **Tietoliikenneturvallisuus**
  Tietoliikenneturvallisuudella pyritään varmistamaan tietoturvan perustavoitteet eli verkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Keskeisenä tavoitteena on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus. Tieto- liikenneturvallisuudessa on kyse kaikista niistä toimenpiteistä, joilla varmistetaan tietojen turvallisuus tiedon liikkuessa järjestelmän sisällä tai organisaatioiden välillä.
- **Henkilöstöturvallisuus**
  Henkilöstöturvallisuuden tavoite on, ettei työntekijä tietämättömyyden, huonon motivaation tai pahantahtoisuuden vuoksi pääse muuttamaan tai tuhoamaan tietoa, tai mahdollista jonkun ulkopuolisen käyttämään sitä. Henkilöstöturvallisuuden pääpaino on riskien välttäminen ennakkoon ja synnyn estäminen.