Helsingin kaupungin tietoturvalinjaukset

1.6.2020

Johdanto

Yleisiä tavoitteita kaikelle tietojen turvaamiselle ovat:

- tietojen suojaaminen luvattomalta käytöltä (luottamuksellisuus)
- tietojen vääristymisen estäminen (eheys)
- tietojen käytön mahdollistaminen niitä tarvittaessa (saatavuus).

Helsingin kaupungin Organisaatioturvallisuuden linjausten luvun 2.7 mukaan tietoturva on osa kaupungin organisaatioturvallisuuden kokonaisuutta. Organisaatioturvallisuuden linjausten mukaisesti tietoturvallisuuden tavoitteena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon.

Helsingin kaupungin tietoturvalinjaukset sisältävät ohjeita siitä, miten tietoturvan tavoitteita toteutetaan Helsingin kaupungilla.

Helsingin kaupungin tietoturvalinjaukset koskevat kaikkia kaupungin toimialoja, virastoja ja liikelaitoksia ja kaupungin tietoverkkoon liitettyjä yhteisöjä sekä kaupungin yleisen tietoverkon lisäksi palvelutuotannoissa käytettäviä erillisverkkoja.

Kaupungin tietoturvalinjaukset, tietoturvan hallinnointi, organisointi ja toimintatavat toteutetaan julkishallinnolle annettujen tietoturvaohjeista (Vahti-ohjeistukset) muodostuvan tietoturvamallin mukaisesti. Tietoturvatoiminnassa käytetään julkishallinnolle annettuja suosituksia, vakiintuneita tietoturvastandardeja ja -kontrolleja, Vahti-ohjeita sekä muiden viranomaisten kuten esimerkiksi Kyberturvallisuuskeskuksen ohjeita.

Helsingin kaupungin tietoturvalinjausten lisäksi toimialoilla, virastoilla ja liikelaitoksilla on omia tietoturvaan liittyviä ohjeistuksia, jotka ohjaavat tietoturvalliseen toimintaan. Toimialojen omissa ohjeissa on huomioitava kunkin toimialan erityislainsäädännön vaatimukset.

Helsingin viestintäverkon ja viestintäpalveluiden käyttöä linjaa oma ohjeensa (kansliapäällikön päätös § 63 13.7.2017).

Tietoturvan teknisen tavoitearkkitehtuurin linjauksesta on kansliapäällikkö päätös § 105 30.4.2020.

Teknisissä tietoturvaratkaisuissa käytetään hyödyksi palvelutoimittajien antamia ohjeita tai julkisesti saatavia ohjeita.

Helsingin kaupungilla on tietosuojalinjaukset (kaupunginhallituksen päätös § 287 29.4.2019), jotka linjaavat osaltaan myös kaupungin tietoturvatoimintaa.

Keskeiset määritelmät

ISO/IEC 27001

ISO/IEC 27001 on standardi tietoturvallisuuden hallintajärjestelmän kehittämiselle, toteuttamiselle, käyttämiselle, valvomiselle, katselmoinnille, ylläpitämiselle ja parantamiselle.

Katakri

Kansallinen turvallisuusauditointikriteeristö, joka toimii tietoturvallisuuden auditointityökaluna ensisijaisesti viranomaisille.

Kiistämättömyys

Kiistämättömyys tarkoittaa varmistumista siitä mitä käyttäjä on tehnyt käsitellessään tietoa.

Kokonaisarkkitehtuuri

Kokonaisarkkitehtuuri on toiminnan, prosessien ja palvelujen, tietojen, tietojärjestelmien ja niiden tuottamien palvelujen muodostaman kokonaisuuden rakenne, jota sovelletaan Helsingin kaupungilla.

Kontrolli

Kontrollit (tietoturvajärjestelyt) ovat toimenpiteitä, joilla pyritään minimoimaan toteutuneen uhan aiheuttamaa vahinkoa tai estämään uhan toteutuminen.

Lokitieto

Lokitieto tarkoittaa dokumenttia (tapahtumakirjanpitoa) jonkin tapahtuman toteutumisesta tiettynä hetkenä.

Pitukri

Pilvipalveluissa käsiteltävän salassa pidettävän tiedon turvallisuuskriteeristö ensisijaisesti viranomaisille.

Riski

Riski on epävarma asia, joka tapahtuessaan vaikuttaa hankkeeseen tai toimintaan. Riskien vaikutukset voivat olla sekä negatiivisia että positiivisia. Negatiivisista riskeistä puhutaan uhkina, positiiviset riskit ovat mahdollisuuksia.

Tietosuoja

Tietosuoja tarkoittaa henkilötietojen suojaamista. Helsingin kaupungin tietosuojavastaava neuvoo ja ohjeistaa tietosuojalainsäädännön mukaisista velvollisuuksista ja seuraa, että tietosuojalainsäädöksiä noudatetaan. Toimialojen, virastojen ja liikelaitosten nimetyt tietoturvasta vastaavat henkilöt toimivat yhteistyössä tietosuojavastaavan, tietosuoja-asioiden yhteyshenkilöiden ja asiantuntijoiden kanssa.

Tietoturva

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan, että tiedot ovat vain käyttöön oikeutettujen saatavilla, muut kuin siihen oikeutetut käyttäjät eivät voi muuttaa tietoja, ja tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen saatavilla ja hyödynnettävissä.

Tietovaranto

Tietovaranto tarkoittaa määriteltyä tietojen joukkoa, josta muodostuu looginen kokonaisuus.

Todentaminen

Todentamisella henkilö todistaa tietojärjestelmälle käyttäjäidentiteettinsä.

Tuoteomistaja

Järjestelmän tuoteomistaja (liiketoimintaomistaja) vastaa järjestelmän operatiivisesta toiminnasta ja sen kehittämisestä.

VAHTI-ohjeistus

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) toimittaa ohjeita, joita sovelletaan Helsingin tietoturvatyössä.

Tietoturva-asioiden vastuunjako Helsingin kaupungin organisaatiossa

Linjaus 1: Tietoturvan vastuunjako

Kokonaisvastuu Helsingin kaupungin tietoturvasta määritellään hallintosäännössä ja toimintasäännöissä. Kaupunginkanslian tietohallintoyksikön toimialaan kuuluu kaupungin tietohallinnon kokonaisohjaus ja osana tätä sen toimialaan liittyvän tietoturvatoiminnan ohjaus kaupungin toiminnassa.

Kansliapäällikkö

Hallintosäännön 12 luvun 1 §:n 1 momentin 1 kohdan mukaan kansliapäällikkö antaa toimialajohtajille, liikelaitosten johtajille ja muille vastuuhenkilöille menettelytapaohjeita ja määräyksiä sekä hallintoa koskevia määräyksiä ja ohjeita. Tämä koskee myös tietoturvaan liittyvää ohjeistusta.

Kansliapäällikkö on antanut päätöksen 278/23.12.2019 koskien tiedonhallinnan ohjausvastuita ja tiedonhallintaryhmän asettamista sekä päätöksen 125/25.5.2020 kaupunginkanslian tiedonhallinnan toteutusvastuita, joissa on päätetty myös eräistä tietoturvan vastuista.

Kaupunginkanslian tietohallinto

Kaupunginkanslian toimintasäännön luvun 5.1 mukaan kaupunginkanslian tietohallinnon toimialaan kuuluvat kaupungin tietohallinnon kokonaisohjauksen ja yhteentoimivuuden

kehittäminen, tietohallinnon strateginen suunnittelu ja seuranta, tietoteknisen perusinfrastruktuurin palvelujen järjestäminen ja ylläpito, yhteisten ja strategisesti keskeisten tietojärjestelmien ja ICT-palvelujen kehittäminen, yhteisten tietojärjestelmien ja tietovarastojen sovellushallinta sekä kaupunginkanslian tietohallinto ja lähituki.

Lisäksi se vastaa tarjoamiensa kaupunkiyhteisten palveluiden tietoturvasta sekä Helnet-verkon tietoturvasta runkoverkon osalta. Kaupunginkanslia järjestää myös kaupunkiyhteistä tietoturvakoulutusta.

Kaupunginkanslian turvallisuus- ja valmiusyksikkö

Kaupunginkanslian toimintasäännön luvun 3.1 mukaan kaupunginkanslian turvallisuus- ja valmiusyksikön toimialaan kuuluvat kaupungin organisaatioturvallisuuden ja yleisten turvallisuusasioiden koordinoiminen ja edistäminen sekä varautumisen, jatkuvuudenhallinnan ja paikallisen turvallisuussuunnittelun kaupunkitasoinen ohjaaminen.

Tähän liittyen turvallisuus- ja valmiusyksikkö vastaa ICT-varautumisessa tarvittavasta ohjauksesta sekä ohjeistaa ICT-varautumisen tavoitetasoista.

Digitaalinen johtoryhmä (digijory)

Kansliapäällikön päätöksen (§ 62 27.3.2019) mukaan digitaalinen johtoryhmä johtaa kaupunkitasoista strategista digitalisaation kehittämistä ja ohjaa kaupungin digitaalisten palvelujen, yhteisen infran ja tukipalvelujen kehittämistä ja toteuttamista. Digitaalinen johtoryhmä tekee linjauksia yhteisen infrastruktuurin ja digitaalisten palvelujen kehittämisestä. Toimivaltainen viranomainen tekee tarvittavat linjausten mukaiset päätökset. Tämä koskee myös tietoturvaan liittyviä asioita.

Sisäisen valvonnan ja riskienhallinnan koordinaatioryhmä

Kaupunginhallituksen hyväksymän (§ 1125 23.11.2015~~)~~ Sisäinen valvonta ja riskienhallinta Helsingin kaupunkikonsernissa -ohjeen luvun 3.5 mukaan sisäisen valvonnan ja riskienhallinnan koordinaatioryhmä kokoaa ja laatii arvioita kaupungin merkittävistä riskeistä. Tähän sisältyvät myös tietoturvariskit.

Tiedonhallintapäällikkö

Tiedonhallintapäällikön vastuut digitaalisen aineiston osalta sisältävät tietyt vastuut tietoaineiston todistusvoimaisuuteen liittyen (laatiminen ja talteenotto, autenttisuus, luotettavuus, eheys ja käytettävyys). Nämä vastuut liittyvät tietoaineistojen tietoturvallisuuden varmistamiseen.

Tiedonhallintapäällikön vastuut analogisen aineiston (paperiaineisto, mikrofilmit) osalta sisältää asiakirjahallinnon johtamisen ja kehittämisen mukaan lukien tietoturvan ohjausvastuu asiakirjojen arkistokelpoisuudesta, arkistotiloista ja asiakirjojen suojaamisesta poikkeusoloissa.

Kaupungin tietoturvallisuuspäällikkö

Kaupungin tietoturvallisuuspäällikkö koordinoi ja ohjaa kaupungin tietoturvaa. Tietoturvaa ovat tekniset toimenpiteet tiedon ja toiminnan suojaamiseksi sekä organisatoriset toimenpiteet ja ohjeistukset. Asiakirjahallinnon tietoturvavastuista vastaa tiedonhallintapäällikkö.

Toimialat, virastot ja liikelaitokset

Kunkin toimialan, viraston ja liikelaitoksen johto vastaa tietoturvan toteutumisesta oman organisaationsa vastuualueella ja järjestää tietoturvaan tarvittavat resurssit.

Tietoturvauhkien ja tietojen käsittelyyn liittyvien heikkouksien tunnistaminen sekä uhkien seuranta on tiedot omistavan organisaation vastuulla.

Kunkin organisaation tietohallinto vastaa teknisestä tietoturvasta teknisellä vastuullaan olevien tietojärjestelmien ja sovellusten osalta, sitä tukevien tietohallinnon ohjeiden tekemisestä ja asetettujen tietoturvavaatimusten toteuttamisesta sekä vastuulleen kuuluvien lähiverkkojen tietoturvasta. Tietohallinto seuraa vastuualueensa tietoturvan toteutumista ja informoi siitä oman organisaationsa johtoa ja tietoturvan yhteyshenkilöä.

Toimialojen, virastojen ja liikelaitosten tietohallinnot ilmoittavat henkilötietoihin kohdistuneista tietoturvaloukkauksista oman organisaationsa tietosuojan vastuuhenkilölle.

Toimialojen, virastojen ja liikelaitosten tietohallinnot ilmoittavat Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle vastuualueeseensa kuuluvista tietoturvaloukkauksista sekä informoivat niistä kaupunginkanslian tietohallintoa.

Kukin toimiala, virasto ja liikelaitos järjestää omaa toimintaansa tukevaa tietoturvakoulutusta.

Järjestelmän tekninen vastuu

Järjestelmään liittyvän teknisen alustan ja tieto- ja viestintätekniset ratkaisut toteuttava taho vastaa tietoturvajärjestelyiden riittävyydestä suhteessa tuoteomistajan asettamiin tietoturvan tavoitteisiin. Näitä ovat esim. käyttöoikeudet, salaus, tietoliikenteen analysointi, segmentointi, lokit ja kovennukset. ICT-varautuminen toteutetaan julkishallinnon digitaalisen turvallisuuden ohjeissa (VAHTI-ohjeet) esitetyillä tavoilla. Teknisiin tietoturvajärjestelyihin sisältyvät myös lokiratkaisut. Järjestelmän tekniseen vastuuseen kuuluu käyttöoikeuksien tekninen hallinta käyttöoikeuksille asetettujen vaatimusten mukaisesti.

Tuoteomistaja

Järjestelmän tuoteomistaja (liiketoimintaomistaja) vastaa järjestelmän ja sen sisältämän tiedon riskienhallinnasta ja järjestelmän heikkouksien ja siihen kohdistuvien uhkien tunnistamisesta. Lisäksi tuoteomistaja asettaa tietoturvalle tavoitteet, kuten järjestelmän tietoturvan tai varautumisen taso ja vastaa tietojärjestelmän ja sen sisältämän tiedon luokittelusta. Järjestelmän tuoteomistaja seuraa järjestelmän tietoturvan tilannetta palveluntuottajan kanssa.

Tietoturvan yhteyshenkilö

Jokaiseen toimialaan, virastoon ja liikelaitokseen tulee nimetä tietoturvan yhteyshenkilö(t). Tietoturvan tehtäviä voidaan yhdistää muihin tehtäviin sekä hoitaa oman toimen ohella.

Yhteyshenkilöt huolehtivat oman organisaationsa tietoturvan suunnittelusta, kehittämisestä ja seuraamisesta sekä osallistuvat kaupunkitasoiseen kehittämistyöhön.

Kaupunginkanslian tietoturvan yhteyshenkilö huolehtii kaupunkitasoisen tietoturvan yhteistyön järjestämisestä sekä tietoturvan hallintajärjestelmän toimivuudesta, kaupunkitasoisen tietoturvaohjauksen valmistelusta ja kehittämisestä.

Lisäksi jokaisen toimialan, viraston ja liikelaitoksen tulee huolehtia, että lähtökohtaisesti kaupungin sopimuksissa ja hankinnoissa käytettävässä Tietosuoja- ja salassapitoliitteessä on nimetty kyseistä hankintaa tai sopimusta koskeva(t) tietoturvan yhteyshenkilö(t).

Tietoturvan yhteistyöverkosto

Kaupunginkanslian tietoturvan yhteyshenkilö huolehtii kaupunkitasoisen tietoturvan yhteistyön järjestämisestä.

Kaupunkitasoisessa tietoturvan yhteistyöverkostossa käsitellään tietoturvauhkia, tietoturvapoikkeamia, tietoturvakyvykkyyksien kehittämistä sekä yhteisvalmistellaan tietoturvan ohjeistusta.

Esihenkilö

Esihenkilö vastaa tietoturvan toteutumisesta omalla vastuualueellaan. Esihenkilö neuvoo, miten tietoja käsitellään työtehtävissä ja mistä työohjeet ovat saatavilla. Esihenkilön tulee huolehtia perehdyttämisestä tietoturvaohjeisiin sekä työntekijän työtehtäviin liittyviin tietoturvavastuisiin. Esihenkilön tulee hallita lainsäädännön mukainen tietojen käsittely vastuualueensa tehtävissä sekä tiedostaa tietoihin liittyvien väärinkäytösten rikosoikeudelliset seuraamukset.

Esihenkilön tulee huolehtia henkilöstönsä tarvitsemien tietoihin ja tietojärjestelmiin liittyvien käyttöoikeuksien asianmukaisuudesta ja ajantasaisuudesta. Työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin, esihenkilö huolehtii kaupungin tiedon palauttamisesta kaupungille muun omaisuuden palauttamisen yhteydessä sekä työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta.

Jokainen työntekijä

Jokainen kaupungilla palvelussuhteessa oleva henkilö vastaa omalta osaltaan tietoturvan toteuttamisesta ja ohjeiden noudattamisesta. Jokaisella on vastuu omaan tehtäväänsä liittyvien tietojen ja tietojärjestelmien asianmukaisesta käytöstä tietoturva huomioon ottaen. Jokaisen vastuulla on tietoturvaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi omalle esihenkilölleen ja/tai tietoturvan yhteyshenkilölle tai muulle organisaation nimeämälle taholle.

Tietovarannot

Linjaus 2: Tietovarantojen hallinta

Helsingin kaupungin tiedot, tietojenkäsittely-ympäristö ja niihin liittyvät muutokset tulee hallita. Myös tietojen versiointi ja tietojenkäsittely-ympäristöjen kokoonpanojen rakenne tulee hallita (konfiguraation hallinta). Helsingin kaupungin käyttöön luovutettujen tietojen käsittelyohjeita tulee noudattaa.

Tiedoilla on aina omistaja. Se on tyypillisesti tietojen alkuperäinen kirjaaja tai toimintayksikkö, jolle tietojen hallinnointi on asetettu ja jonka toimintaa varten tietoja tarvitaan. Tietojen omistaja vastaa tietojen luokittelusta ja oikeasta käsittelystä ja voi valtuuttaa tietovarantojen teknisen hoitamisen jollekin muulle organisaatiolle. Kaupunki soveltaa toiminnassaan kokonaisarkkitehtuuria ja siihen kuuluu yhtenä osa-alueena tietoarkkitehtuuri.

Tietojärjestelmien luokittelu

Järjestelmien luokittelu tehdään osana Helsingin kaupungin kokonaisarkkitehtuurityöhön liittyvää tietojärjestelmien dokumentaatiota. Merkinnät järjestelmien sisältämien tietojen julkisuuden asteesta tehdään kaupungin tietojärjestelmäluetteloon. Kukin toimiala, virasto ja liikelaitos ylläpitää omaa tietojärjestelmäluetteloaan, ja kaupunginkanslian tietohallinto vastaa kaupunkiyhteisen järjestelmäsalkun ylläpidosta.

Linjaus 3: Riskiperusteinen lähestymistapa

Tietoturvallisuustoimet tulee aina suhteuttaa suojattavaan tietoon; julkisen tiedon suojaamiseksi ei tarvita samanlaisia toimenpiteitä kuin salassa pidettävien tietojen suojaamiseksi. Tietoturvauhkien kartoittamisen kautta muodostetaan käsitys suojattavaan tietoon kohdistuvista riskeistä, jotka arvioidaan ja joiden perusteella tietoturvallisuustoimenpiteet toteutetaan.

Tieto- ja ICT-riskien hallinnassa sovelletaan kaupungin riskienhallinnasta annettuja ohjeita ja määräyksiä.

Riskiarvioon perustuvat tietoturvajärjestelyt toteutetaan monitasoisen suojaamisen periaatetta noudattaen. Tietoturvajärjestelyiden riittävyyttä arvioidaan julkishallinnon yleisiä vaatimustasoja ja alan vakiintuneita standardeja vasten. Tällaisia ovat esimerkiksi kansallinen (tieto)turvallisuuden arviointikriteeristö (Katakri) ja pilvipalveluiden turvallisuuden arviointikriteeristö (Pitukri).

Helsingin ICT-kehittämismenetelmiä (Kehmet) voidaan soveltaa tieto- ja ICT-riskien sekä tietosuojariskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi.

Toimialat, virastot ja liikelaitokset arvioivat tietojensa ja tietojärjestelmiensä vaatimien turvatoimien tarpeen ja määrittelevät tietoturvajärjestelyt.

Jos tietojärjestelmälle on tietosisällöstä johtuvia toteutusvaatimuksia, ne toteutetaan hyödyntäen jo käytössä olevia ratkaisuja. Toteutusvaatimukset voivat johtua esimerkiksi maksukorttitietojen käsittelystä (PCI DSS –standardi, Payment Card Industry Data Security Standard), viranomaisen turvaluokitteleman tiedon käsittelyvaatimuksista tai julkishallinnolle annetuista ICT-varautumisen vaatimuksista.

Tieto- ja ICT-riskienhallinnan tukena voidaan käyttää tietoturvan asiantuntijapalveluita. Kaupunginkanslia kilpailuttaa ja tarjoaa kaikille toimialoille, virastoille ja liikelaitoksille puitesopimuksen kautta tietoturvan asiantuntijapalveluita. Tällaisia palveluita ovat esimerkiksi vaatimustenmukaisuuden, jatkuvuuden sekä tietoturvan testaus- ja arviointipalvelut.

Tietoturvan taso

Tietojärjestelmän suojaustaso määräytyy siinä käsiteltyjen tietojen eniten suojausta vaativan tiedon mukaan. Tietoaineiston suojaamistarpeista on huolehdittava tarvittavien teknisten ratkaisujen ja hallinnollisten prosessien avulla siten, että ne mitoitetaan aina suojattavan kohteen merkityksen mukaan. Tietoaineiston saatavuudesta tulee huolehtia, vaikka sen luottamuksellisuuteen liittyisikin tiukkoja vaatimuksia.

Linjaus 4: Tietoturvan perustaso

Toimintaan liittyvät tietoturvallisuusriskit tulee olla kartoitettu ja tietoturvallisuuden hoitamista ja asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritelty. Tietojen saanti ja käytettävyys tulee turvata eri tilanteissa, myös poikkeustilanteissa.

Asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy tietoihin vain sellaisille henkilöille, joiden työtehtävät tätä edellyttävät. Asiakirjojen tietojenkäsittely- ja säilytystilojen tulee olla valvottuja ja suojattuja riittävällä tasolla. Tietojen luvaton muuttaminen tai asiaton käsittely estetään käyttöoikeushallinnalla, käytön valvonnalla sekä tietoverkkojen, tietojärjestelmien ja tietopalvelun asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä.

Mikäli järjestelmässä on julkisuuslaissa (JulkL 24.1 1-32) tai erillislaeissa säädettyä salassa pidettävää tietoa, sen tietoturva tulee toteuttaa vähintään VAHTI-ohjeistuksissa kuvatun perustason mukaan (ohjeissa käytetty tason vaatimuksista nimikettä turvallisuusluokka IV, suojaustaso IV tai käyttö rajoitettu).

Viranomaisen turvaluokittelemaa tietoa tulee käsitellä kyseiselle turvaluokalle annettujen vaatimusten mukaisesti. Turvaluokitellun tiedon käsittelyä voi tapahtua sekä sähköisesti että muutoin (esimerkiksi paperilla).

Linjaus 5: Tietoturvan korotettu taso

Osassa kaupungin toimintoja tavoitetason tulee olla perustasoa korkeampi.

Tietoturvan perustasoa vaativammat tietoturvajärjestelyt toteutetaan tietoja käyttävän organisaation ja kaupunginkanslian kanssa yhteistyössä.

Yleistä tietoturvan perustasoa korkeampaa kyvykkyyttä tietoturvaosaamisessa saatetaan tarvita raha- ja maksuliikenteessä, salassa pidettävien ja erityisiin henkilötietoryhmiin kuuluvien henkilötietojen (esim. terveystietojen) käsittelyssä, turvallisuuteen, tietoturvallisuuteen ja varautumiseen liittyvässä toiminnassa sekä silloin, kun käsitellään valtionhallinnon salassa pidettäväksi merkitsemiä asiakirjoja tai muuta salassa pidettävää aineistoa.

Tällaisia erityisjärjestelyitä ovat käytännössä esimerkiksi korotetun tietoturvatason viestintäjärjestelmät (suojattu sähköposti, suojattu matkapuhelin), ryhmätyöympäristöt (suojattu ryhmätyöympäristö), tallennusalustat tai korotetun turvatason työasemat.

Linjaus 6: Poikkeaminen linjausten mukaisesta tietoturvan tasosta

Jos toimiala, virasto tai liikelaitos ei pysty toteuttamaan tavoiteltua tietoturvan tasoa toiminnassaan tai vastuullaan olevassa tieto- tai viestintäjärjestelmässä, tulee toiminnasta vastuussa olevan linjajohdon päättää poikkeamaan liittyvän riskin hyväksymisestä.

Tietoturvasta tinkiminen vaarantaa kaupungin toiminnan jatkuvuuden ja palveluiden saatavuuden. Tietoturvapoikkeama aiheuttaa korjauskuluja, palvelukatkoja, huonoa mainetta ja voi johtaa oikeudellisiin seuraamuksiin.

Todentaminen ja kiistämättömyys

Linjaus 7: Käyttöoikeuksien hallinta

Käyttöoikeudet toteutetaan Helsingin kaupungilla roolipohjaisesti käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan.

Vastuu käyttöoikeuksista on aina sillä toimialalla, virastolla tai liikelaitoksella, joka ne myöntää. Toimialat, virastot ja liikelaitokset voivat käyttää käyttöoikeuksien hallinnassa sähköisiä työnkulkuja, paperilomakkeita tai muita menettelytapoja. Tärkeintä on varmistaa, että käyttäjätunnusten elinkaari on hallittavissa siten, että kaikki käyttäjätunnuksiin ja käyttövaltuuksiin tehdyt muutokset ovat asianmukaisesti esihenkilön valtuuttamia, dokumentoituja ja valvottuja.

Esihenkilön tulee huolehtia käyttöoikeuksien asianmukaisuudesta ja ajantasaisuudesta. Työntekijän palvelussuhteen päättyessä tai tehtävien muuttuessa esihenkilö huolehtii työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta.

Linjaus 8: Käyttäjien tunnistaminen

Tietojen käytön luottamuksellisuuden varmistaminen edellyttää tietoa käyttävien henkilöiden tai ohjelmien todentamista (tunnistamista). Luotettavampia käyttäjien tunnistaminen menetelmiä ovat esimerkiksi käyttötunnuksen ja salasanan lisäksi henkilökohtaiseen puhelimeen lähetettävä kertakäyttökoodi tai Suomi.fi-tunnistus.

Käyttäjältä voidaan vaatia digitaalisessa palvelussa sähköistä tunnistamista, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi.

Jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi, on palvelun käyttäjä tunnistettava luonnollisen henkilön tunnistuspalvelua, vahvaa sähköistä tunnistamista tai painavasta perustellusta syystä muuta vastaavaa tietoturvallista tunnistuspalvelua käyttämällä.

Pääkäyttäjätunnusta käyttävän henkilön tunnistaminen tulee pystyä todentamaan luotettavasti.

Linjaus 9: Lokitietojen kerääminen

Silloin kun tieto- ja viestintäjärjestelmän toiminta tai todennetun käyttäjän toimet pitää osoittaa kiistämättömästi, tulee tarvittava tapahtumakirjanpito toteuttaa tietojen eheyden säilyttävillä teknisillä ratkaisuilla (lokijärjestelmät). Lokitietojen kerääminen edellyttää, että käyttöoikeudet ovat henkilökohtaisia.

Lokien keräämiselle tulee olla peruste ja käsittelytavat sekä vastuut määritelty. Lokeihin tallentuvien tietojen tyypit ja suojaustarpeet tulee tunnistaa ja määritellä. Pääsyä lokitietoihin tulee kontrolloida pääsyoikeushallinnalla ja lähtökohtaisesti käyttäjien pääsy tulee olla evätty, silloin kun henkilön työtehtävät eivät pääsyä edellytä. Luottamuksen säilyttämiseksi lokeja ei tule oikeudettomasti muuttaa tai tuhota.

Henkilötietojen käsittelyn osalta kaupungin tietosuojalinjauksissa on linjattu, että mitä keskeisemmästä tietojärjestelmästä on kyse ja mitä arkaluonteisempia sen keräämät

henkilötiedot ovat, sitä välttämättömämpää lokitietojen kerääminen on. Jos järjestelmässä käsitellään salassa pidettävää tai arkaluontoista henkilötietoa, on järjestelmän kerättävä lokitiedot myös henkilötietojen katselusta. Uusia tietojärjestelmiä hankittaessa yhtenä järjestelmävaatimuksena on, että järjestelmä kerää lokitiedot henkilötietojen käsittelystä, myös tietojen katselusta.

Kun tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista, tulee tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätä tarpeelliset lokitiedot. Lokitietoja käytetään seuraamaan tietojärjestelmissä olevien tietojen käyttöä ja luovuttamista sekä selvittämään tietojärjestelmien teknisiä virheitä.

Poikkeustilanteiden ja jatkuvuuden hallinta

Linjaus 10: Poikkeustilanteen ja jatkuvuuden hallinta

Helsingin kaupungilla tulee olla kyky toimia kaikissa arjen tilanteissa sekä vaikeutuneissa toimintaolosuhteissa myös tietojen käytön osalta. Lisäksi kaupungilla tulee olla kyky reagoida tehokkaasti tietoja uhkaavissa tilanteissa ja tietoturvan poikkeamatilanteissa.

Toimialan, viraston tai liikelaitoksen tulee järjestää itselleen oman ydintoimintansa kannalta riittävä reagointikyky tietoturvaan liittyviä häiriötapahtumia varten. Toiminnasta vastaava johto vastaa myös omien palveluidensa jatkuvuuden turvaamisesta.

Jatkuvuuden turvaamiseen sisältyy luotettavien tietojärjestelmien käyttämisen varmistaminen myös poikkeustilanteissa. ICT-varautumiseen liittyvien järjestelyiden tarve tunnistetaan julkishallinnon digitaalisen turvallisuuden ohjeissa esitetyillä tavoilla niille keskeisille tietojärjestelmille, jotka vaativat parhaimman palvelukyvyn myös vaikeutuneessa yhteiskunnallisessa turvallisuustilanteessa.

Oikean tasoinen reagointikyky tietoturvaan liittyviä häiriötapahtumia varten määritellään tieto- ja ICT-riskien arvioinnin kautta.

Kriittisyydeltään elintärkeiden järjestelmien toimivuuden takaamiseksi tulee olla laadittuna ajantasainen toipumissuunnitelma.

Toiminta poikkeustilanteissa

Jokaisen työntekijän velvollisuutena on ilmoittaa välittömästi omalle esihenkilölleen sekä oman organisaationsa sovitulle taholle havaitsemistaan tietoturvapoikkeamista, mukaan lukien tietoturvaan liittyvät uhkat, vahingot, tietojen väärinkäyttö tai muut poikkeamat. Organisaation vastuulla on varmistaa, että poikkeustilanneprosessi on henkilöstön tiedossa ja kuvaus saatavilla.

Toimialan, viraston tai liikelaitoksen, jossa poikkeustilanne on havaittu, johto vastaa toimintansa vakiinnuttamiseksi tarvittavan tilanteen johtamisesta. Johtamisen lisäksi poikkeustilanteen hallinta ja vahinkojen minimointi sekä kehittämistoimenpiteiden seuranta tulee olla vastuutettu.

Toimialan, viraston tai liikelaitoksen, jossa poikkeustilanne on havaittu, tulee käynnistää tarvittavat toimenpiteet poikkeaman hallitsemiseksi ja vahinkojen minimoimiseksi sekä väärinkäytösten ja rikollisen toiminnan keskeyttämiseksi. Jos tilanne edellyttää, on asia saatettava toimivaltaisen viranomaisen selvitettäväksi sekä asianomistajarikoksissa että virallisen syytteen alaisissa rikoksissa. Kaupunginkanslian oikeuspalvelut antaa konsultaatiota asian oikeudellisessa arvioinnissa.

Ulkopuolisen toimijan omistaman tiedon katoamisesta, väärinkäytöstä, varkaudesta tai muusta toimijaan vaikuttavasta poikkeamasta pitää välittää mahdollisimman nopeasti tieto kyseiselle organisaatiolle heidän antamansa ohjeistuksensa mukaisesti.

Vakavassa poikkeamatilanteessa noudatetaan kaupunkikonsernin kriisijohtamisen mallia. Vaikutuksen alaisen palvelun poikkeaman hallinnasta vastaa se taho, joka vastaa palvelun normaalista toiminnasta.

Poikkeamatilanteen viestinnässä noudatetaan kaupungin kriisiviestintäohjeita.

Henkilötietoihin kohdistuneiden tietoturvaloukkausten osalta työntekijän tulee ilmoittaa havaitsemastaan loukkauksesta välittömästi esihenkilölleen ja oman organisaationsa tietosuojan vastuuhenkilölle. Henkilötietoihin kohdistuneista tietoturvaloukkauksista ilmoitetaan asianosaisille erikseen määritellyn prosessin mukaisesti.

Linjaus 11: Toimintakyvyn varmistaminen

Varmistuakseen organisaation toimintakyvystä, vastuussa olevan johdon tulee teettää tarkastuksia ja harjoituksia. Tarkastuksissa verrataan toteutuvaa kykyä toiminnalle asetettuihin tietoturvatavoitteisiin.

Tietoturvaan liittyvät tarkastukset ja harjoitukset voidaan liittää esimerkiksi toimialan, viraston tai liikelaitoksen valmiusharjoituksiin tai järjestelmien katselmointeihin ja testauksiin. Kaikkiin valmius- ja johtamisharjoituksiin on hyvä sisällyttää ICT-järjestelmiin liittyvä osa-alue (kybertoimintakyvyn harjoite).

Linjaus 12: Tietoturvan tilannekuva

Tietoturvan tilannekuva tarkoittaa ajantasaista ymmärrystä tietoja koskevasta tilanteesta Helsingin kaupungilla. Yleistä tietoturvan tilannekuvaa Suomessa tuottaa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus.

Seuranta voi sisältyä esimerkiksi toimialan, viraston tai liikelaitoksen omaan laadunhallintaan, palvelusopimusten seurantaan ja siinä voi hyödyntää sisäisen valvonnan ja tarkastuksen tekemiä selvityksiä.

Kaupungin yhteisten tietoverkkojen tietoturvaa seurataan kaupunginkanslian tietohallinnossa sekä palveluoperaattoreiden valvomoissa.

Työasemien osalta tilannetta seurataan kaupunginkanslian tietohallinnon keskitetyssä työasemapalvelussa, jonka lisäksi toimialat, virastot ja liikelaitokset voivat seurata tilannetta oman tarpeensa mukaan niiden omissa tietohallinnoissa.

Tietojärjestelmien tietoturvaa seurataan palvelutuottajan omassa organisaatiossa. Tietojärjestelmän tuoteomistaja kuitenkin seuraa järjestelmän tietoturvaa palvelutuottajan kanssa.

Valvomopalvelu

Tietoturvan tilannekuvan muodostamista varten keskuksessa (service operation center, kyberturvakeskus, valvomo) valvotaan verkon, työasemien, palvelinten, verkon aktiivilaitteiden, erilaisten ohjelmistojen ajantasaista käyttötilannetta. Tieto palveluiden hetkellisestä tilanteesta voi sisältää myös tietoturvaa kuvaavia havaintoja: tunnistettuja haittaohjelmia, tukoksia tietoliikenteessä, rikkoutuneita laitteita ja muita häiriöitä.

Kaupungin yleistilanteen kannalta tarpeellisen valvomopalvelun järjestää kaupunginkanslia.

Toimiala, virasto tai liikelaitos järjestää toimintansa kannalta tarpeelliset valvomotoiminnot.

Hankinnat ja sopimukset

Linjaus 13: Hankinnat ja sopimukset

Hankinnoissa tulee noudattaa hankintalainsäädäntöä, kaupungin hankintaohjeistusta sekä julkishallinnon yleisiä suosituksia ICT-hankintojen ja hankinnan kohteiden tietoturvan huomioimisesta.

Erityistä huomiota tulee kiinnittää siihen, että tieto- ja viestintätekniset hankinnat sopivat kaupungin kokonaisarkkitehtuuriin. Tieto- ja viestintäteknisissä hankinnoissa tulee hankintalainsäädännön asettamissa puitteissa pyrkiä mahdollisimman yhdenmukaisiin, olemassa olevaa osaamista hyödyntäviin hankintoihin kokonaistaloudellisuus ja riskit huomioon ottaen.

Helsingin kaupungin tiedot tulee turvata palvelujen tuotantoketjuissa ja palvelutoimittajien huostassa. Jo hankintaa suunniteltaessa tulee määritellä, millaista tietoturvan tasoa tavoitellaan, mitkä ovat asianmukaiset tietoturvajärjestelyt ja kuinka tietoturvan toteutumista valvotaan. Helsingin ICT-kehittämismenetelmiä (Kehmet) soveltamalla tieto- ja ICT-riskit sekä tietosuojaan liittyvät riskit tulevat huomioiduiksi.

Palvelusopimuksissa määritellään, kuinka tietoturva huomioidaan palvelutuotannossa mukaan lukien se, minkä tasoinen häiriönhallintakyky palveluntuottajalta ostetaan. Joillakin palveluntuottajilla on tarjonnassaan ympärivuorokautista nopean vasteen reagointipalvelua (soc; service operation centre, security operations center). Kaupunginkanslian tietohallinto hyödyntää yhteisten ICT-palveluiden palvelusopimuksia kaupungin yhteisten ICT-palveluiden häiriönhallinnassa.

Hankintaohjeistuksesta löytyy tietosuoja- ja salassapitoliitteen malli, joka sisältää myös tietoturvaa koskevat keskeiset sopimusvelvoitteet. Kyseisten sopimusvelvoitteiden lisäksi hankinnasta tulee huomioida tietoturvavaatimukset tarkemmalla tasolla näiden tietoturvalinjausten mukaisesti. Sopimuksen tietoturvaa koskevien liitteiden laatimiseen saa tarvittaessa tukea kaupunginkanslian oikeuspalveluista. Tietoturvan tekniseen ja muuhun tarkempaan sisältöön sekä näiden liitteisiin liittyvissä kysymyksissä tukea saa kaupunginkanslian tietohallinnosta.

Tietosuojan osalta tietosuoja-asetus edellyttää, että kaupunki saa käyttää ainoastaan sellaisia palvelutuottajia tai muita henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet. Käsittelyn on täytettävä tietosuoja-asetuksen vaatimukset ja varmistettava rekisteröidyn oikeuksien suojelu. Kaupungin tietosuojalinjauksissa on linjattu, että lähtökohtaisesti kaupungin sopimuksissa ja hankinnoissa käytetään kaupungin tietosuoja- ja salassapitoliitettä. Tietosuoja- ja salassapitoliite tai muut tietosuoja-asetuksen 28 artiklan vaatimukset täyttävät ehdot sisällytetään kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja kaupungin lukuun.

Tietoturvan asiantuntijapalvelut

Helsingin kaupungilla on tietoturvan asiantuntijapalveluiden puitesopimus vaatimustenmukaisuuden, jatkuvuuden sekä tietoturvan ja tietoriskien hallinnan palveluille sekä tietoturvallisuuden testaus- ja arviointipalveluille.

Puitesopimuksen mukaisia palveluita tilataan kaupunginkanslian järjestämän osaamiskeskuspalvelun kautta.

Raportointi

Linjaus 14: Säännöllinen raportointi

Vastuu tietoturvan seurannasta kuuluu toimialojen, virastojen ja liikelaitosten johdolle. Kunkin toimialan, kaupunginkanslian, viraston ja liikelaitoksen tietoturvan yhteyshenkilö raportoi oman organisaationsa johdolle säännöllisesti ja pyydettäessä oman vastuualueensa tietoturvaan liittyvät asiat.

Kaupunginkanslian tietohallintojohtaja raportoi kansliapäällikölle säännöllisesti seurantatiedot koko kaupungin osalta.

Johdon tulee käynnistää raportoinnin perusteella vastuualueensa mukaiset tarvittavat korjaustoimenpiteet.

Toimialojen, virastojen ja liikelaitosten tietoturvan yhteyshenkilöt tai muu organisaation nimeämä taho raportoivat tarvittaessa kaupunginkanslian tietoturvan yhteyshenkilölle.

Kaupunginkanslian tietohallinto vastaa vuosittain julkishallinnon digiturvallisuuskyselyyn (Vahti-raportointi).

Tietoturvan tilaa voidaan tarvittaessa seurata henkilöstölle suunnatuilla kyselyillä.

Tietosuojaan liittyvistä asioista raportoidaan erikseen annettujen ohjeiden mukaisesti.
Säännöllisen raportin sisältö

Säännöllisesti raportoitavat asiat ovat raportoivan tahon itsensä havaitsemia tai sille raportoidut:

- merkittävät poikkeamat tietoturvassa
- menossa olevat tietoturvan kehitystoimet
- uudet tai seurannassa olevat merkittävät tietoturvaan liittyvät riskit, joiden seurantatieto kirjataan kyseisen organisaation riskikarttaan
- tunnistetut uudet, tietoturvan kannalta merkitykselliset kehitystarpeet
- tietoturvan osaamisen kehittämisen tilanne.

Raportoinnin tukijärjestelyt

Tietoturvan raportoinnin tukena käytetään riskienhallinnan järjestelmää. Tilannekuvajärjestelmä voi olla osa valvomopalvelua.

Raportoitavia havaintoja ja tilastotietoja voi syntyä valvomojärjestelmistä (SIEM, security information and event management), tietoliikenteen valvonnasta (IDS/IPS, intrusion detection / protection system), muista tietoturvajärjestelmistä (haittaohjelmatorjunta), ohjelmistojen tai työasemien päivitystilanteesta. Nämä tiedot tuottaa kunkin toimialan, kaupunginkanslian,

viraston ja liikelaitoksen tietohallinto ja raportoi omissa raportointikanavissa sekä saattaa ne tietoturvan yhteyshenkilöille saataville.

Normit ja ohjeet

Keskeisiä lakeja tietoturvan kannalta ovat seuraavat.

- 906/2019 laki julkisen hallinnon tiedonhallinnasta
- 306/2019 laki digitaalisten palvelujen tarjoamisesta
- 917/2014 laki sähköisen viestinnän palveluista
- 621/1999 laki viranomaisten toiminnan julkisuudesta

Tiedonhallintalautakunnan ohjeet ja suositukset, esimerkiksi seuraava.

- Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta

Keskeisiä julkishallinnolle annettuja yleisiä tietoturvaohjeita (Vahti-ohjeet) ovat tuoreimmat ohjeet, esimerkiksi seuraavat.

- Vahti 22/2017 Ohje riskienhallintaan
- Vahti 8/2017 Tietoturvapoikkeamatilanteiden hallinta
- Vahti 2/2016 Toiminnan jatkuvuuden hallinta
- Vahti 2/2014 Tietoturvallisuuden arviointiohje
- Vahti 2/2012 ICT-varautumisen vaatimukset
- Vahti 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, jonka liitteissä kuvattu käsittelyvaatimuksia

Julkishallinnon tietoturvan arviointiin keskeisiä ovat seuraavat.

- Katakri: Tietoturvallisuuden auditointityökalu viranomaisille
- Pitukri: Pilvipalveluiden turvallisuuden arviointikriteeristö

ISO/IEC-standardit, joita voi käyttää tietoturvan liittyvien toimintojen kehittämiseen, esimerkiksi seuraavat.

- ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä ja siihen liittyvät standardit
- ISO/IEC 27018 Henkilötietojen suojaaminen pilvipalveluissa

Muut tietoturvan liittyvien toimintojen kehittämisenstandardit, esimerkiksi seuraavat.

- Payment Card Industry Data Security Standard (PCI DSS)

Eräitä muita julkishallinnon ohjeita ovat seuraavat.

- Turvallisen sovelluskehityksen käsikirja, Väestörekisterikeskus
- Turvallinen tuotekehitys -opas, Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom

Lisätietoja

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (Vahti) ohjesivusto:
https://www.vahtiohje.fi/

Katakri: Tietoturvallisuuden auditointityökalu viranomaisille:
https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Pitukri: Pilvipalveluiden turvallisuuden arviointikriteeristö:
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_Pitukri.pdf

Tiedonhallintalautakunnan ohjeet ja suositukset
https://vm.fi/tiedonhallintalautakunta