Helsingin kaupungin tietoturvalinjaukset

Kansallinen digiturvaviikko 26.-30.10.2020

Helsinki

Helsingin kaupungin tietoturvalinjaukset

Helsingin kaupungin tietoturvalinjaukset löytyvät kaupungin verkkosivulla kansliapäällikön päätöksistä

- Helsingin kaupungin tietoturvalinjaukset (16 sivua) ja
- kansliapäällikön päätös 166/22.06.2020

Lisäksi niistä löytyvät mm. Helsinki-kanavan videotietoiskut

- Helsingin kaupungin tietoturvalinjaukset (video, 2 minuuttia)
- Tietoturvalinjaukset ja tiedonhallintalaki (video, 2 minuuttia)

sekä digitaalisen Helsingin blogista artikkelit

- tietoturvalinjaukset
- tietoturvalinjaukset ja tiedonhallintalaki

Helsinki

Nämä esityskuvat toimivat jäsennyksenä oppitunnin mittaisen esitelmän seuraamiseen.
Kuvat tukevat esityksen etenemistä, mutta varsinainen luettava aineisto on itse linjausten tekstit, jotka löytyvät verkko-osoitteiden avulla.

Katsaus sisältöön

- ❑ Rakenne
- ❑ Laatiminen
- ❑ Sisältö
- ❑ Kuinka liittyy jokaisen työhön
- ❑ Keskustelua

Johdantona
aivan ensiksi,
tietoturvatoiminnan
liittyminen
kaupunkistrategiaan.

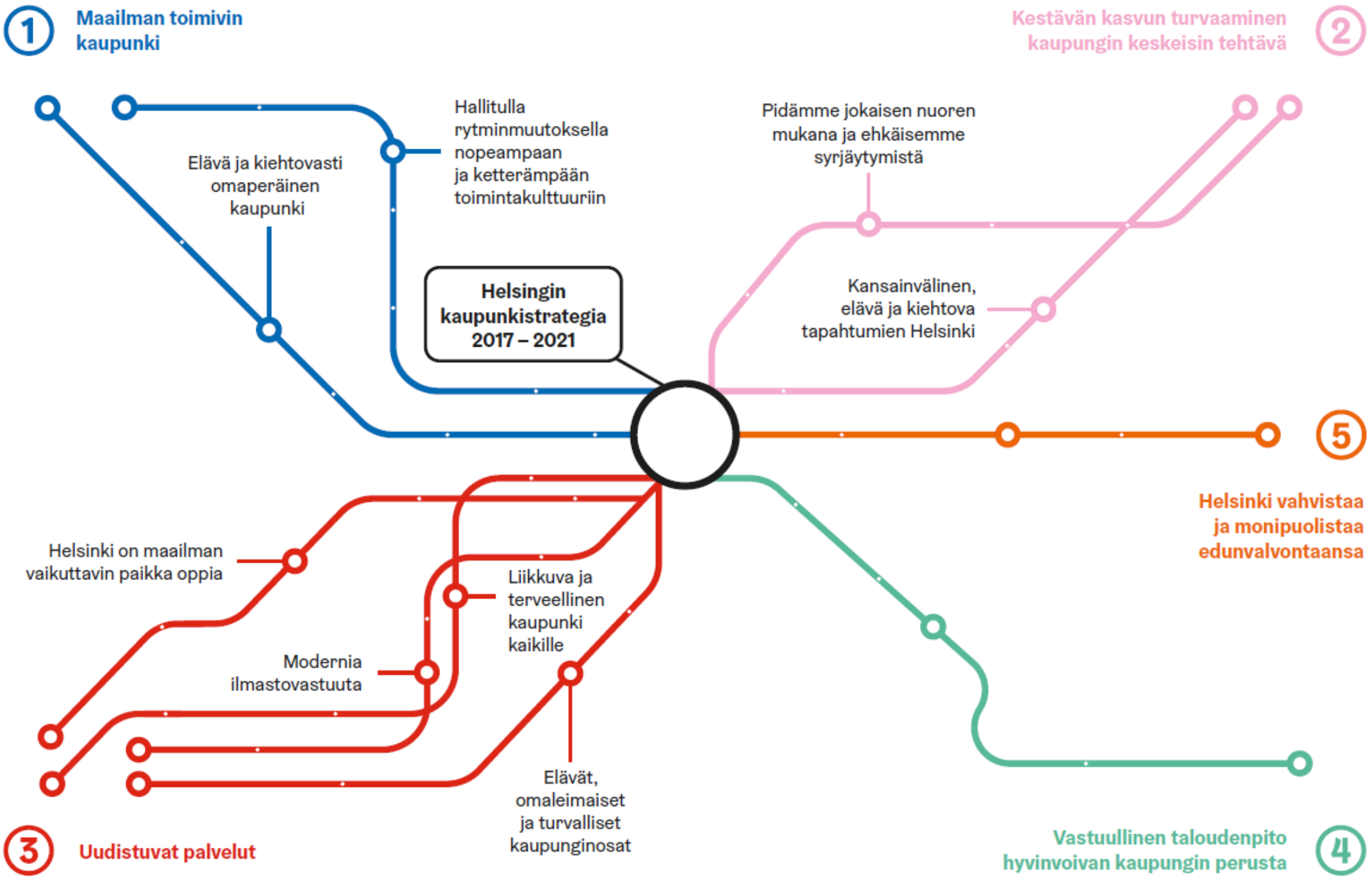
Helsingin tavoitteena on olla maailman parhaiten digitalisaatiota hyödyntävä kaupunki maailmassa.

Helsinki kehittää digitaalisia ratkaisuja, jotka tekevät helpoksi seurata ja osallistua itseä kiinnostaviin ja koskeviin asioihin riippumatta siitä, ovatko ne kaupungin vai muiden tekemiä. Helsingin toimintamalli perustuu mahdollisimman suureen avoimuuteen ja läpinäkyvyyteen.

Helsinki on maailman johtava kaupunki julkisen tiedon avaamisessa ja sen hyödyntämisessä.

Helsinki kehittää yhteensovitettuja, vaikuttavia ja ihmiskasvoisia palveluja yhdessä kaupunkilaisten kanssa. Kaupunki panostaa esteettömiin sähköisiin palveluihin sekä digitalisaation, tekoälyn ja robotisaation hyödyntämiseen. Sähköiset palvelut ovat ensisijaisia, ja ne ovat käytettävissä viikonpäivästä tai kellonajasta riippumatta.

Helsingissä otetaan käyttöön sähköinen asiointi mahdollisimman laajasti ja kerätään systemaattisesti palautetta sähköisesti.


1
Maailman toimivin kaupunki
Elävä ja kiehtovasti omaperäinen kaupunki
Hallitulla rytminmuutoksella nopeampaan ja ketterämpään toimintakulttuuriin
Helsingin kaupunkistrategia 2017 – 2021
2
Kestävän kasvun turvaaminen kaupungin keskeisin tehtävä
Pidämme jokaisen nuoren mukana ja ehkäisemme syrjäytymistä
Kansainvälinen, elävä ja kiehtova tapahtumien Helsinki
5
Helsinki vahvistaa ja monipuolistaa edunvalvontaansa
Helsinki on maailman vaikuttavin paikka oppia
Liikkuva ja terveellinen kaupunki kaikille
Modernia ilmastovastuuta
Elävät, omaleimaiset ja turvalliset kaupunginosat
3
Uudistuvat palvelut
4
Vastuullinen taloudenpito hyvinvoivan kaupungin perusta

Helsinki

Onnistuvaa tietoturvaa

Vastuullisuus

Osaaminen

Teknikka

Helsinki

Rakenne

Helsinki

Laatiminen

Helsinki

Helsingin kaupungin tietoturvalinjaukset

Sisältö

1.6.2020

Helsinki

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.

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.

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.

Kontrolli

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

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.

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.

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.

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.

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.

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.

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.

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.

Linjaus 7: Käyttöoikeuksien hallinta

Käyttöoikeudet toteutetaan Helsingin kaupungilla roolipohjaisesti käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan.

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.

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.

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.

Linjaus 11: Toimintakyvyn varmistaminen

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

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.

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.

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.

- 906/2019 laki julkisen hallinnon tiedonhallinnasta
- 306/2019 laki digitaalisten palvelujen tarjoamisesta
- 917/2014 laki sähköisen viestinnän palveluista
- 621/1999 laki viranomaisten toiminnan julkisuudesta
- Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta
- 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
- Katakri: Tietoturvallisuuden auditointityökalu viranomaisille
- Pitukri: Pilvipalveluiden turvallisuuden arviointikriteeristö
- ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä ja siihen liittyvät standardit
- ISO/IEC 27018 Henkilötietojen suojaaminen pilvipalveluissa
- Payment Card Industry Data Security Standard (PCI DSS)
- Turvallisen sovelluskehityksen käsikirja, Väestörekisterikeskus
- Turvallinen tuotekehitys -opas, Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom

- Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (Vahti) ohjesivusto
- Katakri: Tietoturvallisuuden auditointityökalu viranomaisille
- Pitukri: Pilvipalveluiden turvallisuuden arviointikriteeristö
- Tiedonhallintalautakunnan ohjeet ja suositukset

Tietoturvalinjaukset koskevat tietojen käsittelyä sekä digitaalisissa ympäristöissä että niiden ulkopuolella.

Miten uudet tietoturvalinjaukset liittyvät jokaisen työhön?

Jokainen kaupungilla palvelussuhteessa oleva työntekijä vastaa omalta osaltaan tietoturvan toteuttamisesta ja ohjeiden noudattamisesta. Jokaisella on vastuu omaan tehtäväänsä liittyvien tietojen ja tietojärjestelmien asianmukaisesta käytöstä tietoturva huomioon ottaen.

Ainakin alkusivujen johdanto ja keskeiset määritelmät sopivat kaikkiin tehtäviin johdatukseksi tietoturvaan. Samoin kannattaa tietoturva-asioiden vastuunjako kappaleesta tunnistaa omaan tehtäväänsä liittyvät vastuut.

Keskustelua

- Digitaalisen Helsingin blogi
  digi.hel.fi/blogi
- Helsinki-kanavan tietoturva työpisteellä -sarja
  helsinkikanava.fi

Koulutuskalenterista kurssit hakusanalla ”tietoturva”

Tietoturva-asiantuntija Aaro Hallikainen, Kaupunginkanslia

Vastuullisuus

Osaaminen

Tekniikka