Kouvolan kaupungin digitaalisen turvallisuuden politiikka

Versiotiedot

Versio	Kuvaus	Päivämäärä ja muutoksen tekijän	Muutoksen hyväksyjä
0.9	Ehdotus tietosuoja- ja tietoturvaryhmälle, konsernipalveluiden johtoryhmälle ja YT-ryhmälle	12.2.2019, Tietohallinto, 18.2.2019, Tietotuoja- ja tietoturvaryhmä, 26.2.2019, Konsernipalveluiden johtoryhmä 5.3.2019, YT-ryhmä	Tietosuoja- ja tietoturvaryhmä, konsernipalveluiden johtoryhmä, YT-ryhmä
0.91	Muokattu versio, lisätty versiotiedot-taulukko ja 7 luvun kohdan ”Henkilöstöturvallisuus” 2. kappaleessa muutettu kohta ”henkilöt allekirjoittavat turvallisuussopimuksen” muotoon ”henkilöt hyväksyvät turvallisuussopimuksen”	7.3.2019, Teppo Saarela	
0.95	Konsernijaoston käsittely	11.6.2019, Sirpa	Konsernijaosto
0.95	Tytäryhtiöiden lausuntokierros	12.6.-1.7.2019	
0.98	Muokattu versio:luku 4 ”Sidosryhmät ja vaatimukset” *valmisteilla oleva laki julkisen hallinnon tiedonhallinnasta (HE 284/2018)* muutettu muotoon Tiedonhallintalaki (HE 284/2018) ja 0.91 muokatun version mukainen sanamuoto tekstiosaan (*allekirjoittavat ->hyväksyvät).* Korjattu version 0.9 YT-ryhmän kokouspv. 6.3.2019 -> 5.3.2019	7.8.2019 Sirpa Mäntynen	
0.98	Kaupungin johtoryhmän käsittely	12.8.2019	kaupungin johtoryhmä
0.99	Kaupunginhallituksen käsittely	26.8.2019	kaupungin hallitus
1.0	Hyväksytty politiikka	kh:n esityksestä lisätty lukuun 6 kaupunginjohtajan vastuu / Sirpa Mäntynen 17.8.2019	hyväksytty kaupunginhallituksessa 26.8.2019

Sisältö

1 Johdanto

Kouvolan kaupungin palveluiden tuottaminen perustuu enenevässä määrin tietoon ja sen käsittelyyn sekä käsittelyä tukeviin digitalisoituihin palveluihin.

Kouvolan kaupungin johto määrittelee tässä politiikassa ylätasolla kaupungin digitaalisen turvallisuuden vaatimukset, palveluiden tuottamisessa noudatettavat linjaukset, organisoinnin ja vastuut sekä digitaalisen turvallisuuden hallintaprosessit.

Politiikka toimii perustana Kouvolan kaupungin digitaalista turvallisuutta koskeville ohjeille ja prosessikuvauksille.

2 Digitaalisen toimintaympäristön turvallisuus

Verkostoituneessa yhteiskunnassa palveluiden taustalla toimivat yhä laajemmat digitaalisten palveluiden ekosysteemit, jotka muodostava entistä laajempia palveluketjuja ja –alustoja. Palvelukokonaisuuksien toteuttamiseen osallistuu tyypillisesti myös ulkoisia palveluntuottajia.

Julkisessa hallinnossa palveluiden toimivuuteen, palveluissa käsiteltävien tietojen luottamuksellisuuteen sekä niiden toimivuuteen myös poikkeustilanteissa kohdistuu korkeita vaatimuksia. Tietojenkäsittelyn muuttuessa verkottuneemmaksi, tietojenkäsittely-ympäristöt edellyttävät laajempaa kokonaissuunnittelua, jossa tulee pystyä varmistamaan ratkaisujen yhteensopivuus, kustannustehokkuus sekä turvallisuus koko toimintoketjussa.

Nopeassa muutoksessa oleva toimintaympäristö edellyttää aktiivista uhkien seurantaa ja riskienhallintaa, joiden avulla organisaatio pystyy varmistamaan tarkoituksenmukaisen turvallisuuden kehittämisen osana sen jokapäiväistä toimintaa. Tässä mallissa entistä tärkeämmäksi nousevat verkostossa toimivien tahojen välinen yhteistyö ja vastuunjaosta sopiminen.

Kouvolan kaupungin palvelujen ja hallinnon digitaalisen turvallisuuden tavoitteena on tietoturvallinen digitaalinen ympäristö, jossa noudatetaan voimassaolevaa lainsäädäntöä ja asetusten määräämiä normeja sekä tehtyjen sopimusten edellyttämiä vaatimuksia kattavasti koko palveluketjussa.

3 Politiikan soveltamisala

Digitaalisen turvallisuuden politiikkaa noudatetaan koko kaupungin organisaation toiminnassa ja se koskee kaikkia kaupungin palveluksessa työskenteleviä, luottamushenkilöitä ja kaupungille palveluita tuottavien organisaatioiden henkilöitä.

Politiikkaa noudatetaan kaikkien Kouvolan kaupungille palveluita tuottavien organisaatioiden toiminnassa siinä laajuudessa, kun toiminta liittyy Kouvolan kaupunkiin. Palvelutuottajien turvallisuusvelvoitteet täsmennetään palvelutuottajan kanssa laadittavassa sopimuksessa.

Politiikkaa suositellaan noudatettavaksi soveltuvin osin myös kaupungin omistamien tytäryhtiöiden toiminnassa.

Digitaalisen turvallisuuden politiikka koskee kaikkea tietojen käsittelyä sekä niihin liittyviä laitteita, järjestelmiä, toimintaprosesseja, henkilöitä sekä fyysisiä tiloja riippumatta mitä tietoja käsitellään ja missä muodossa tiedot sijaitsevat.

Erityisesti digitaalisen turvallisuuden politiikkaa hyödynnetään digitalisesti toteutettavien palveluprosessien toiminnassa koko palveluketjun laajuisesti niiden koko elinkaaren ajan.

4 Sidosryhmät ja vaatimukset

Lainsäädäntö asettaa lähtökohdat Kouvolan kaupungin digitaalisen turvallisuuden varmistamiseksi tehtävälle työlle. Keskeisimpiä ohjaavia lakeja ovat EU:n yleinen tietosuoja-asetus 2016/679, Laki viranomaisen toiminnan julkisuudesta 621/1999, Tietosuojalaki (1050/2018), valmisteilla oleva laki julkisen hallinnon tiedonhallinnasta (HE 284/2018) sekä julkisen hallinnon digitaalisen turvallisuuden johtoryhmän antamat VAHTI-ohjeet.

Kaupungin tärkein sidosryhmä ovat asukkaat. Kaupunki tehtävänä on tuottaa asukkaille luotettavia ja helppokäyttöisiä palveluita, joiden tuottamisessa digitalisaatiolla on tulevaisuudessa entistäkin suurempi rooli.

Kaupungissa toimivat yritykset ja organisaatiot ovat kaupungin tulevaisuuden ja elinvoimaisuuden kannalta hyvin tärkeä sidosryhmä, jotka asettavat korkeat vaatimukset palveluiden saatavuudelle ja toimintaympäristön luotettavuudelle.

Lisäksi digitaaliselle turvallisuudelle asettavat vaatimuksia kaupungin yhteistyökumppanit sekä useat viranomaistahot.

Sidosryhmät asettavat vaatimuksia digitaalisten palveluiden saatavuudelle sekä käsiteltävien tietojen virheettömyydelle ja luottamuksellisuudelle. Osana digitaalisen turvallisuuden hallintaa täsmennetään eri sidosryhmien asettamat yksityiskohtaisemmat turvallisuusvaatimukset, joiden perusteella suunnitellaan riskilähtöisesti hallintakeinot vaatimusten täyttämiseksi.

5 Visio ja linjaukset

Kouvolan kaupungin ylin johto on sitoutunut palveluiden tietoturvallisuuden varmistamiseen ja sen jatkuvaan kehittämiseen.

Kaupungin digitaaliset palvelut ovat luotettavia, helppokäyttöisiä ja helposti saavutettavia. Palveluiden turvallisuutta ohjataan riskilähtöisesti ja niiden tuottamisessa hyödynnetään yhteistyökumppaneita. Palveluiden turvallisuus varmistetaan koko tuotantoketjussa ja palveluien turvallisuudesta huolehditaan koko elinkaaren ajan.

Digitaalisten palveluiden tuottamisessa ja turvallisuuden varmistamisessa noudatetaan seuraavia linjauksia:

- Digitaaliseen turvallisuuteen resursoidaan riittävästi.
- Turvallisuutta johdetaan suunnitelmallisesti ja riskilähtöisesti.
- Henkilöstön turvallisuustietoisuus, turvallisuusosaaminen sekä sitoutuminen turvallisen toimintaan varmistetaan.
- Palveluiden tuottamisessa hyödynnetään uudenlaisia digitaalisia ratkaisuja ja verkostomaista toimintatapaa.
- Palveluiden turvallisuus varmistetaan hankintojen yhteydessä ja turvallisuutta ylläpidetään koko elinkaaren ajan.
- Palveluiden tuottajat velvoitetaan sopimuksellisesti noudattamaan palveluille asetettuja turvallisuusvaatimuksia.
- Digitaalisen turvallisuuden toteutumista seurataan ja digitaalisen turvallisuuden kehittymisestä muodostetaan säännöllisin väliajoin ajantasainen kokonaiskuva.

- Häiriötilanteisiin reagoidaan nopeasti ja niiden taustalla olevat syyt pyritään selvittämään ja poistamaan.
- Palveluiden jatkuvuus ja toiminta poikkeustilanteissa varmistetaan.
- Turvallisuutta kehitetään jatkuvan parantamisen periaatteen mukaisesti.

6 Organisointi ja vastuut

Kokonaisavastuu tietoturvasta on kaupunginhallituksella.

Kaupunginjohtaja vastaa tietoturvallisuuden kehittämisestä, valvonnasta ja asioiden valmistelusta kaupunginhallituksen käsiteltäväksi.

Tietoturvaan liittyvää käytännön kehittämistyötä ohjaa ja koordinoi konsernipalveluihin kuuluva tietohallinto, jota johtaa tietohallintojohtaja, joka toimii myös kaupungin tietoturvavastaavana.

Kaupungin tietoturvavastaava vastaa tietoturvaan liittyvien prosessien ja menettelytapojen toteuttamisesta, kehittämisestä ja ylläpitämisestä sekä dokumentointiin ja ohjaamiseen liittyvistä tehtävistä.

Tietoturvallisuuden ohjausryhmä toimii kaupungin tietoturvavastaavan apuna kaupungin tietoturvan kehittämiseen ja ylläpitoon liittyvissä tehtävissä.

Jokaisen yksikön esimies vastaa yksikkönsä vastuulla olevien tehtävien osalta tietoturvasta. Jokainen kaupungin työntekijä ja kaupungille palveluita tuottava henkilö vastaa tietoturvasta omassa toiminnassaan.

Kukin palveluntuottaja vastaa toimintansa tietoturvasta Kouvolan kaupungille tuotettavien palveluiden osalta. Kouvolan kaupungilla on vastuu palveluntuottajan palveluiden ja toiminnan tietoturvallisuuden seurannasta.

7 Digitaalisen turvallisuuden hallinta

Toiminnan suunnittelu ja vuosikello

Digitaalista turvallisuutta johdetaan ja ohjataan suunnitelmallisesti. Turvallisuuden kehittämiseksi tehtävät toimenpiteet suunnitellaan, resursoidaan ja aikataulutetaan osaksi turvallisuuden hallinnan vuosikelloa. Lisäksi varaudutaan kykyyn reagoida ja suunnata turvallisuustoimenpiteitä tarpeiden ja riskien perusteella kulloinkin tärkeimpiin kohteisiin.

Suojattavien kohteiden ja vaatimusten hallinta

Digitaalisen turvallisuuden hallinnan kannalta merkitykselliset tiedot, järjestelmät, tekniset ympäristöt ja käsittelyprosessit tunnistetaan ja luokitellaan. Jokaiselle suojattavalle kohteelle määritetään omistaja. Suojattaviin kohteisiin liittyvät vaatimukset tunnistetaan ja riskit arvioidaan hallintakeinojen mitoittamiseksi oikealle tasolle.

Henkilöstöturvallisuus

Henkilöstön turvallinen toiminta varmistetaan turvallisuusohjeilla, perehdytyksillä, säännöllisillä lisäkoulutuksilla sekä hyvällä esimiestyöllä. Henkilöstön turvallisuusosaaminen ja toiminnan turvallisuus varmistetaan seurannan avulla.

Kaupungille työskentelevät henkilöt hyväksyvät turvallisuussitoumuksen. Lisäksi turvallisuuden kannalta kriittisemmissä tehtävissä työskenteleville henkilöille voidaan tehdä turvallisuusselvitys.

Tahallisten tietoturvarikkomusten ja laiminlyöntien kohdalla voidaan käynnistää sanktiomenettely. Vakavien tietoturvarikkomusten kohdalla tehdään aina sisäinen tutkinta ja tarvittaessa voidaan käynnistää rikosoikeudellinen menettely.

Järjestelmien ja teknisen ympäristön turvallisuus

Digitaaliset toimintaympäristöt ja niissä toimivat tietojärjestelmät ovat jatkuvasti kasvavassa roolissa kaupungin toiminnassa. Niiden turvallisuus varmistetaan määrittelemällä järjestelmien turvallisuusvaatimukset, varmistamalla asetettujen vaatimusten täyttyminen katselmoinneilla ja testauksilla, huolehtimalla käyttöönoton turvallisuudesta sekä ylläpitämällä turvallisuusominaisuuksia järjestelmän koko elinkaaren ajan.

Tärkeänä osana järjestelmien turvallisuuden varmistamista on integroitujen järjestelmäkokonaisuuksien sekä niihin liittyvien käsittelyprosessien turvallisuuden suunnittelu ja varmistaminen kokonaisuutena. Turvallisuusvaatimukset otetaan huomioon heti suunnitteluprosessin alussa.

Palveluiden ja hankintojen turvallisuus

Ulkoisissa palveluhankinnoissa turvallisuusvaatimukset otetaan huomioon sopimuksissa. Vaatimusten toteutuminen varmistetaan riittävällä seurannalla. Kriittisemmissä palveluissa sekä käsiteltäessä henkilötietoja varmistetaan palvelutuottajan turvallisuuden taso sekä kysy osoittaa turvallisuusvaatimusten täyttyminen jo ennakkoon.

Riskienhallinta

Digitaalisen turvallisuuteen kohdistuvat uhat voivat johtaa huomattaviin taloudellisiin menetyksiin. Samoin digitaalisten ratkaisujen täydellinen suojaaminen voi olla hyvin kallista. Näistä seikoista johtuen riskienhallinnan merkitys osana digitaalisen turvallisuuden varmistamista korostuu.

Kouvolan kaupungissa pyritään arvioimaan systemaattisesti kaikkien kriittisten kohteiden digitaaliseen turvallisuuteen kohdistuvat riskit ja käsittelemään riskit siten, että jäännösriskit asettuvat hyväksyttävälle tasolle. Riskienhallinnalla pyritään varmistamaan, että kaikki tarpeelliset toimenpiteet riskien pienentämiseksi tehdään ja välttämään samalla ylimitoitettuja turvallisuusinvestointeja.

Riskienhallinnan menettelyitä käytetään lisäksi päätöksenteon tukena tilanteissa, joissa tunnistetaan uusia riskejä tai havaitaan puutteita tai heikkouksia nykyisissä turvallisuusratkaisuissa.

Tietoturvahäiriöiden ja -poikkeamien hallinta

Tietoturvahäiriöiden ja -poikkeamien hallinta on tärkeä prosessi, jonka avulla varmistetaan häiriötilanteiden nopea ja asianmukainen käsittely niissä tilanteissa, joissa häiriötä ei ole kyetty torjumaan ennakoivilla toimenpiteillä.

Tietoturvahäiriöiden ja -poikkeamien hallinta käsittää häiriön arvioinnin, korjaavat toimenpiteet, joiden avulla tilanne palautetaan normaaliin tilaan, juurisyyn analysoinnin ja vastaavien tilanteiden syntymisen estämisen tulevaisuudessa sekä tarvittaessa ilmoitukset eri sidosryhmille. Kaikki häiriötilanteet dokumentoidaan ja tarvittaessa suoritetaan riskianalyysi osana toimenpiteitä.

Laajojen tietoturvapoikkeamien yhteydessä kootaan erillinen selvitystyöryhmä (IRT), joka koordinoi poikkeaman selvitystyötä.

Jatkuvuuden hallinta

Tietoturvallisuuden hallintajärjestelmän ylläpitämiseen sisältyy myös kaupungin toimintojen jatkuvuuden ylläpitäminen. Jatkuvuuden varmistamiseksi ylläpidetään suunnitelmia, joiden mukaisesti toimitaan poikkeustilanteissa. Suunnitelmien toimivuus varmistetaan riittävällä testaamisella ja poikkeustilanteiden harjoittelulla.

Osoitusvelvollisuus ja dokumentointi

Digitaalisen turvallisuuden hallinnan yhtenä lähtökohtana on kyky osoittaa turvallisuus ja sitä kautta saavuttaa luottamus Kouvolan kaupungin toiminnan turvallisuuteen.

Keskeisimmät keinot turvallisuuden osoittamiseksi ovat määritellyt digitaalisen turvallisuuden prosessit, niiden systemaattinen toteuttaminen sekä digitaalisen turvallisuuden hallinnan ja saavutetun turvallisuustason osoittava dokumentaatio.

Seuranta ja auditointi

Digitaalisen turvallisuuden toteutuminen varmistetaan säännöllisellä turvallisuuden hallintatoimenpiteiden sekä saavutettujen turvallisuustulosten seurannalla.

Toiminnan turvallisuuden arvioimiseksi valitaan riittävä määrä seurattavia kohteita ja niille mittarit. Seurannan tulokset kerätään ja analysoidaan säännöllisesti siten, että koko ajan on riittävä tietoisuus turvallisuustilanteesta ja sen kehittymisestä.

Liitteet

Liite 1, Terminologia – kuvaukset tietoturvaan liittyvistä käsitteistä