KUHMO

TIETOSUOJA- JA TIETOTURVAPOLITIIKKA

Kuhmon kaupunki

Kuhmon kaupunginhallitus hyväksynyt 17.12.2025

Sisällysluettelo

KUHMON KAUPUNGIN TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

1. Johdanto

Tieto on keskeisessä roolissa Kuhmon kaupungin toiminnassa ja palvelutuotannossa. Jotta tieto on tehokkaasti hyödynnettävissä, tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa.

Tietoturva- ja tietosuojapolitiikassa Kainuun kunnat ovat yhteistyössä Kainuun liiton kanssa määritelleet tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet.

Politiikka toimii perustana Kuhmon kaupungin tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja auttaa niiden käytäntöön soveltamisessa. Tietoturva- ja tietosuojapolitiikka sekä sen soveltamisohjeet pidetään käyttäjien saatavilla Kuhmon kaupungin intranetissä.

Tietoturva- ja tietosuojapolitiikka koskee Kuhmon kaupungin koko organisaatiota -työntekijöitä, luottamushenkilöitä sekä Kuhmon kaupungin sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Kuhmon kaupungin omistamaa tai hallinnoimaa tietoa.

Politiikka kattaa Kuhmon kaupungin käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2. Tietoturvallisuus

Kuhmon kaupungin tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan Kuhmon kaupungin omistamaa tai hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa, että poikkeusoloissa. Tietoturvallisuus kattaa käsitteenä sekä kyberturvallisuuden että tietojen fyysisen suojaamisen.
Tietoturvallisuus on kiinteä osa Kuhmon kaupungin johtamista, palveluita ja toimintoja. Se ulottuu jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin sekä luottamushenkilöiden toimintaan Kuhmon kaupungin asioiden käsittelijöinä. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietoturvallisuuteen liittyvillä vastuutuksilla ja käytännöillä pyritään varmistamaan, että Kuhmon kaupungin omistama ja hallinnoima tieto

- on oikeaa ja eheää, eikä muuttunut teknisen tai inhimillisen toiminnan seurauksena (eheys)
- on vain siihen oikeutettujen saatavilla (luottamuksellisuus)
- on saatavilla, kun sitä tarvitaan (käytettävyys)
- on käsitelty niin, että käsittelyn osapuolet voidaan tunnistaa toimenpiteiden aikana ja jälkikäteen (kiistämättömyys)
- on mahdollista varmistaa sen todenmukaisuus, oikeellisuus, alkuperä ja/tai varmistetaan käyttäjän aitous määritellyllä luottamustasolla (todentaminen)

Tähän liittyen tulee tiedon käsittelyprosessien omistajuus ja käyttöoikeudet määritellä sekä huolehtia tiedon elinkaaren hallinnasta niin, että tietoon sen käsittelyn eri vaiheissa tehdyt muutokset voidaan tarvittaessa jäljittää ja todentaa.

Hyvän tietoturvallisuuden aikaansaaminen ja ylläpito edellyttävät tietoista johtamista ja hyvän hallintotavan noudattamista kunnan kaikissa toiminnoissa. Tietoturvallisuuden osalta tämä kokonaisuus sisältää suunnitteluun, toteutukseen, seurantaan ja ohjaukseen liittyvät prosessit, asiakirjat, kontrollit ja vastuut.

Kuhmon kaupungin tietoturvatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- Julkisia organisaatioita velvoittavat lait ja asetukset, mm. Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR)
- Kuhmon kaupungin omat voimassa olevat strategiat, hallinto- ja ohjesäännöt, riskienhallinta-, valmius- ja viestintäsuunnitelmat (tietoturvallisuutta koskevilta tai sivuavilta osiltaan) sekä näistä johdetut vaatimukset
- Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) suositukset
- Valtionhallinnon Tietoturvallisuuden johtoryhmän (VAHTI) ohjeet
- EU:n tekoälydirektiivi

Tietoturvallisuus on osa kaupungin riskienhallintaa, varautumista ja kokonaisturvallisuutta. Riskienhallintaa toteutetaan kaupungin sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti.
Kaupunki varautuu turvaamaan ensisijassa kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia valmius- ja muita suunnitelmia. Varautumiseen liittyvät roolit ja vastuut kuvataan em. suunnitelmissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

Tiedonhallintalaki velvoittaa tunnistamaan merkittävät tietojenkäsittelyyn kohdistuvat riskit ja hallitsemaan niihin liittyviä ennakoivia tietoturvatoimenpiteitä. Tietoturvan hallinnantaso on asetettu noudattamaan lainsäädännöllisiä velvoitteita. Kaupunki tunnistaa tietoturvan uhkatekijöitä proaktiivisesti. Uhkatekijöiden hallinta perustuu jatkuvaan seurantaan ja analysointiin, jotta poikkeamat voidaan havaita ja käsitellä ajoissa.

3. Tietosuoja

Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten ihmisten yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi.
Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä.
Kuhmon kaupunki käsittelee henkilötietoja vain perustellun käyttötarkoituksen vuoksi ja vain siinä määrin ja niin kauan, kun se on käyttötarkoituksen kannalta tarpeellista.
Käytettävien tietojen oikeellisuus pyritään varmistamaan ja tietoja päivitetään.
Henkilötietoja säilytetään ainoastaan niin kauan kuin se on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Tietosuojaa ohjaavina periaatteina ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä tietojen eheys ja luottamuksellisuus.

Toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa.

Henkilöstön tietosuojaosaamisesta huolehditaan koulutuksilla sekä työroolin mukaisilla ohjeistuksilla. Kuhmon kaupunki mahdollistaa asiakkaille tiedonsaannin omiin henkilötietoihinsa sekä informoi henkilötietojen käsittelystä kaupungin verkkosivuilla. Kaupungin henkilörekistereitä käsittelevät sopimuskumppanit velvoitetaan noudattamaan vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

4. Tietoturvallisuustavoitteet

Kaupungin tavoitteena on saavuttaa Tiedonhallintalain (906/2019) asettamat tietoturvallisuutta koskevat vaatimukset. Tässä yhteydessä otetaan huomioon, että tiedonhallintaa koskeva lainsäädäntö ja siihen liittyvät kansalliset suositukset ovat muutoksessa ja sisältävät useita siirtymäaikoja.

Kaupunki päivittää tietoturvaa koskevia tavoitteita ja tähän liittyviä toimintaprosessejaan suhteessa muuttuvaan lainsäädäntöön osana tietoturvan kokonaissuunnittelua. Toiminnan suunnittelussa ja kehittämisessä otetaan huomioon Valtiovarainministeriön Tiedonhallintalautakunnan, valtionhallinnon tietoturvallisuuden johtoryhmän (Vahti) ja Suomen Kuntaliiton päivittyvät suositukset sekä muu kansallinen julkishallinnon tietoturvaa koskeva lainsäädäntö ja ohjeistus.

5. Organisointi ja tietoturvavastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kaupungin sääntöjen mukaisesti.

Kaupunginhallitus seuraa tietoturvallisuuden toteutumista kunnassa. Se hyväksyy tietoturva- ja tietosuojapolitiikan ja siihen ehdotetut muutokset. Kaupunginhallituksella on vastuu kaupungin sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Vastuuhenkilö tietoturvallisuuden toteutumisesta ja sen raportoinnista kaupunginhallitukselle määrätään hallintosäännössä.
Hallintosääntö myös määrittelee, että kuka omistaa tietoturvapolitiikan, esittelee muutokset kaupunginhallitukselle ja hyväksyy organisaatiotasoiset ohjeet sekä linjaukset.
Tietoturvallisuusasioissa vastuuhenkilön tukena toimivat palvelualueiden johtajat ja tietosuojavastaava.

Palvelualueiden johtajat vastaavat toimialansa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Esihenkilö vastaa tietoturvallisuuden toteutumisesta omalla vastuualueellaan. Esihenkilön keskeisimpinä tehtävinä on huolehtia:

- oman organisaationsa perehdyttämisestä kaupungin tietoturvaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturvavastuisiin
- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
    - kaupungin tiedon ja muun omaisuuden palauttamisesta
    - työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta

Henkilöstö vastaa tietoturvan ja -suojan toteuttamisesta omalta osaltaan. Jokaisen on edesautettava omalla tekemisellään turvallisuuden tavoitteiden toteutumista mm. noudattamalla tietosuojaa ja tietoturvaa koskevia ohjeita.
Jokaisen velvollisuus on tuoda esille mahdolliset turvallisuuspoikkeamat, epäkohdat sekä havaitsemansa uhkat ja riskit ja raportoida niistä välittömästi palveluntarjoajan asiakastukeen ja omalle esihenkilölleen.
Henkilöstö on velvollinen pyytämään apua tietoturvaa ja -suojaa koskevissa kysymyksissä sitä tarvitessaan. Tietoturvatavoitteet saavutetaan vain, jos kaikki noudattavat yhteisesti sovittuja periaatteita.

Tiedonomistaja vastaa tiedon elinkaaren hallinnasta, tiedon luokittelusta (julkisuuden ja salassapidon määrittely), eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön. Tiedonomistaja on se, joka tiedon tuottaa ja joka vastaa sen oikeellisuudesta.

Tietojärjestelmän omistaja vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy työntekijän esihenkilön tai keskitetysti hallintojohtajan hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho. Tietojärjestelmän omistaja on tietojärjestelmästä vastaava palvelualueen johtaja tai toimintayksikön esihenkilö.

Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Palveluntuottajat vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta ICT-ympäristössä sekä tietojärjestelmissä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin. Milloin tietosuojalainsäädäntö edellyttää tietosuojan vaikutusten arvioinnin (dpia) tekemistä, vastaa palveluntuottaja vaikutustenarviointiprosessiin osallistumisesta omalta osaltaan. Palveluntuottajat noudattavat kaupungin tietoturvapolitiikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

Pääkäyttäjät ovat keskeisessä roolissa tietojärjestelmien hallinnassa ja käytössä. Hän varmistaa, että tietojärjestelmät toimivat asianmukaisesti olemalla ongelmatilanteissa yhteydessä käyttäjätukeen. Lisäksi hän antaa käyttäjille heidän tarvitsemaa tukea ja ohjeistusta.

Tietosuojavastaava antaa tietoa ja neuvoja tietosuojaan liittyvissä asioissa. Tietosuoja-säännösten noudattaminen on aina rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla. Tietosuojavastaava ei ole henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen rikkomisesta.

6. Tiedon ja tietojärjestelmien käyttö

Kuhmon kaupungin tietojärjestelmäympäristössä käytetään toimialan hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Uusien ratkaisujen käyttöönoton yhteydessä tulee varmistua, että ne ovat toimialan tiedossa ja hyväksymiä.

Jos järjestelmässä käsitellään henkilötietoja, on ennen uuden järjestelmän käyttöönottoa tehtävä tietosuojan vaikutusten arviointi (DPIA).
Käyttöoikeudet kaupungin omistamaan ja hallinnoimaan tietoon, sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeudet toteutetaan roolipohjaisesti käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan.
Vastuu käyttöoikeuksista on aina toimialalla tai liikelaitoksella, joka ne myöntää. Tärkeintä on varmistaa, että käyttäjätunnusten elinkaari on hallittavissa siten, että kaikki käyttäjätunnuksiin ja käyttövaltuuksiin tehdyt muutokset ovat asianmukaisesti esimiehen valtuuttamia, dokumentoituja ja valvottuja. Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi kaupungin ohjeita. Henkilötietojen käsittelyssä noudatetaan voimassa olevaa lakia ja tietosuojaa ohjaavia periaatteita.

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

Tiedolla on aina omistaja. Tiedon omistaja vastaa tiedon luokittelusta ja oikeasta käsittelystä. Kaupungin tietojen käsittelynohjeita tulee noudattaa. Kaupungin tietojen käsittelyohjeita sekä tietoturva- ja tietosuojaperiaatteita ja ohjeita sovelletaan myös hankkeisiin ja pilotteihin.

Pilvipalveluiden käytössä tulee noudattaa kaupungin tietoturvaohjeita. Tietojen suojaaminen pilvipalveluissa on varmistettava käyttämällä vahvoja salausmenetelmiä ja valitsemalla luotettavia pilvipalveluntarjoajia, jotka täyttävät tietoturvavaatimukset. Pilvipalveluiden käsittelemä data tulisi olla EU/ETA-alueella erityisesti henkilötietoja käsittelyssä.

Etätyössä tulee noudattaa organisaation etätyöohjeistuksen tietoturvakäytäntöjä.

7. Riskiperusteinen lähestymistapa

Tietoturvallisuustoimet tulee perustaa vaatimuksiin, joita toiminta ja palvelut asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle. Tietoturvallisuustoimet tulee suhteuttaa suojattavaan tietoon; julkisen tiedon suojaamiseksi ei tarvita samanlaisia toimenpiteitä kuin salassa pidettävien tietojen suojaamiseksi. Tietoturvatoimia tulee mitoittaa sekä järjestelmän tietosisällön, että kaupungin kriittisten prosessien näkökulmasta.
Tietoaineistoihin, tietovarantoihin ja tietojärjestelmiin kohdistuvia riskejä tulee tarkastella osana kokonaisturvallisuuteen liittyvää riskianalyysiä ja suunnittelua.

8. Tietoturvaosaamisen varmistaminen

Johdon tehtävänä on varmistaa koulutuksen ja ohjeiden avulla, että henkilöstön tietoturvaosaaminen on riittävää. Myös osaamisen ylläpidosta on huolehdittava niin, että se vastaa kulloinkin vallitsevia tilanteita ja toimintaympäristön vaatimuksia.

Esihenkilö huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään. Tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti, ja tietoturva- ja tietosuojaohjeet pidetään kaikkien työntekijöiden saatavilla. Koulutukset kattavat tietoturvan perusperiaatteet, ajankohtaiset uhkat ja parhaat käytännöt.

Kuhmon kaupungin työntekijät suorittavat omatoimisen tietoturva- ja tietosuojakoulutuksen kaupungin laatiman suosituksen mukaisesti.

9. Tietoturva- ja tietosuoja hankinnoissa ja sopimuksissa

Hankinnoissa tulee noudattaa hankintalainsäädäntöä, Kuhmon 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 tiedonhallintamallissa määriteltyyn kokonaisarkkitehtuuriin.

Tieto- ja viestintäteknisissä hankinnoissa tulee hankintalainsäädännön asettamissa puitteissa pyrkiä mahdollisimman yhdenmukaisiin, olemassa olevaa osaamista hyödyntäviin hankintoihin kokonaistaloudellisuus ja riskit huomioon ottaen. Hankintoja suunniteltaessa tulee määritellä tarvittavat asianmukaiset tietoturvajärjestelyt ja tietoturvan toteutumisen valvonta sekä varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Vaadittavien tietoturvajärjestelyiden tulee perustua käsiteltävien tietojen laatuun ja kriittisyyteen kaupungin palveluiden jatkuvuuden hallinnan sekä tietosuojan näkökulmista. Huomioon tulee ottaa tiedon elinkaari, normaaliolojen häiriötilanteisiin ja poikkeusoloihin varautumiseen liittyvät vaatimukset sekä muu asiaa sääntelevä lainsäädäntö.

Hankintasopimuksissa määritellään, kuinka tietoturva huomioidaan palvelutuotannossa mukaan lukien se, minkä tasoinen häiriönhallintakyky palveluntuottajalta ostetaan. Hankintasopimukseen tulee lisäksi liittää kaupungin tietoturva- ja tietosuojaliitteet. Kyseisten sopimusvelvoitteiden lisäksi hankinnassa tulee huomioida tietoturvavaatimukset tarkemmalla tasolla tämän tietoturva- ja tietosuojapolitiikan mukaisesti.

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. Lähtökohtaisesti kaupungin sopimuksissa ja hankinnoissa käytetään kaupungin tietosuojaliitettä. Tietosuojaliite tai muut tietosuoja-asetuksen 28 artiklan vaatimukset täyttävät ehdot sisällytetään kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja kaupungin lukuun.

Tietosuojalainsäädännön asettamia ehtoja ja niiden toteutumista tulee valvoa.

10.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.
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. Lokitietojen käsittelyssä tulee huomioida tiedonhallintalainsäädännön mukainen tarpeellisuusarviointi sekä tietosuojalainsäädäntö.

11.Tietoturvapoikkeamien käsittely ja niistä tiedottaminen

Tietoturva- ja tietosuojaohjeiden noudattamista valvotaan sekä säännöllisin rutiinein tai automaattisesti että pistokokein. Väärinkäytöksiin puututaan.

Sekä odottamattomista että ennalta tiedetyistä palvelukatkoksista ja muista tietojärjestelmien käytön häiriöistä tiedotetaan kaupungin tavanomaisia tiedotuskanavia hyödyntäen. Järjestelmän omistaja tiedottaa käyttöhäiriöistä niiden edellyttämässä laajuudessa.

Tietoturvapoikkeamat käsitellään ja niistä raportoidaan johdolle erikseen ohjeistetulla tavalla. Muulle organisaatiolle havaituista poikkeamista tiedotetaan niiden luonteen ja laajuuden edellyttämällä tavalla.

Tietoturvaloukkauksissa noudatetaan EU:n yleisen tietosuoja-asetuksen määräyksiä henkilötietojen tietoturvaloukkauksen ilmoittamisesta valvontaviranomaiselle ja rekisteröidylle artiklojen 33 ja 34 mukaisesti.

12. Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Tietoturvallisuustyön tulee olla suunnitelmallista. Käytännön toteutusten tulee vastata toiminnan tarpeisiin, lainsäädännön vaatimuksiin sekä kaupungin riskienhallintatyössä asetettuihin muihin tavoitteisiin, ulkoiset toimintaolosuhteet huomioiden.

Seurannan ja muutoshallinnan keinoin varmistetaan, että tietoturvallisuuteen liittyvät kokemukset, palaute ja muutokset vaatimuksissa tai olosuhteissa tulevat oikea-aikaisesti huomioon otetuiksi.

Tarvittaessa tehdään tietoturva-auditointeja, joiden avulla varmistetaan tietoturvakäytäntöjen noudattaminen ja tunnistetaan mahdolliset kehityskohteet.

Tietoturva- ja tietosuojapolitiikka katselmoidaan vuosittain ja päivitetään tarvittaessa.

13. Tekoäly

Tekoälyteknologioiden käyttö organisaation toiminnassa edellyttää erityistä huomiota tietoturvaan ja tietosuojaan. Tekoälyjärjestelmien kehittämisessä ja käytössä tulee noudattaa seuraavia periaatteita:

- Läpinäkyvyys: Tekoälyjärjestelmien toiminnan tulee olla läpinäkyvää ja selitettävää. Käyttäjille tulee tarjota riittävästi tietoa tekoälyn toiminnasta ja sen päätöksenteon perusteista.
- Tietojen anonymisointi: Tekoälyjärjestelmissä käytettävät henkilötiedot tulee anonymisoida aina kun mahdollista, jotta yksityisyyden suoja voidaan varmistaa.
- Eettisyys: Tekoälyn käyttöön liittyvät eettiset kysymykset tulee huomioida ja varmistaa, että tekoälyjärjestelmät toimivat oikeudenmukaisesti ja syrjimättömästi.
- Riskienhallinta: Tekoälyjärjestelmien käyttöön liittyvät riskit tulee arvioida ja hallita huolellisesti. Tämä sisältää mahdollisten tietoturvauhkien tunnistamisen ja niihin varautumisen.
- Jatkuva seuranta ja arviointi: Tekoälyjärjestelmien toimintaa tulee seurata ja arvioida jatkuvasti, jotta voidaan varmistaa niiden tietoturvallisuus ja tietosuoja.

Kaupungin tietoturvapolitiikassa on huomioitava tekoälyjärjestelmien riskienhallinta ja varmistettava, että tekoälyjärjestelmät ovat turvallisia ja luotettavia. Tekoälysäädös korostaa henkilötietojen suojaa ja edellyttää, että tekoälyjärjestelmät noudattavat GDPR:n vaatimuksia. On varmistettava, että tekoälyjärjestelmät käsittelevät henkilötietoja asianmukaisesti ja että tietosuoja on otettu huomioon kaikissa tekoälyjärjestelmissä. Tekoälysäädös vaatii, että tekoälyjärjestelmät ovat läpinäkyviä ja selitettäviä.

On varmistettava, että käyttäjät ymmärtävät, miten tekoälyjärjestelmät toimivat ja mitä riskejä sen käyttöön liittyy.
Kaupunki laatii henkilöstölleen erillisen tekoälynkäyttöpolitiikan ja tekoälyohjeistuksen.
Vaikutusten arviointi eli DPIA tulee tehdä ennen tekoälyohjelman käyttöönottoa.

14. Lisätietoja

Oppaita ja ohjeita löytyy tietosuojaan sekä tietoturvaan liittyen löytyy mm. seuraavista linkeistä:
https://tietosuoja.fi
https://finlex.fi/fi/lainsaadanto/2018/1050
https://tietosuojakeskus.fi
https://www.kyberturvallisuuskeskus.fi/fi/ohjeet
https://tietosuoja.fi/vaikutustenarviointi
https://dvv.fi/digiturvallinen-elama