



Kajaanin kaupunki

Kajaanin kaupungin tietoturva- ja tietosuojapolitiikka

Hyväksytty KH xx.x.2025 § xxx

Konsernipalvelut
Tietoturva

Sisällysluettelo

1 Kajaanin kaupungin tietoturva- ja tietosuojapolitiikka.....	1
1.1 Tietoturvan määritelmä	1
1.2 Tietosuojan määritelmä	2
1.3 Kajaanin kaupungin toimintaympäristö	2
2 Tietoturvatyön tavoitteet.....	3
2.1 Muuttuva toimintaympäristö ja tilannekuvan ylläpito.....	5
2.2 Palveluiden jatkuvuus ja tietojen turvaaminen	5
2.3 Organisaation osaamisen ja kyvykkyyden kehittäminen.....	6
2.4 Toimitusketjujen tietoturvan varmistaminen	6
2.5 Tietosuojan varmistaminen	7
2.6 Lokitietojen hallinta.....	8
2.7 Käyttövaltuuksien hallinta.....	9
3 Tietoturva- ja tietosuojatyön vastuut.....	11
3.1 Kaupunginhallituksen ja kaupungin johdon vastuut.....	11
3.2 Toimialojen, liikelaitosten ja tytäryhtiöiden vastuut	12
3.3 Esihenkilön tietoturvavastuut	12
3.4 Työntekijän tietoturvavastuut.....	13
3.5 Tiedonhallinnan vastuut.....	14
3.6 Palvelujen ja hankintojen tietoturvavastuut	16
3.7 Keskitetyt tukipalvelut.....	17
3.8 Kajaanin kaupungin tietoturva- ja tietosuojatyöryhmä	18
4 Normaaliolojen häiriötilanteisiin varautuminen	18
5 Tietoturvan seuranta, ylläpito ja kehittäminen	18

Versiohistoria

Päivämäärä	Tekijä / Muokkaaaja	Hyväksyjä
8.9.2025	Tietoturvapäällikkö	Kajaanin tietoturva- ja tietosuojatyöryhmä
18.11.2025	Tietoturvapäällikkö	Kajaanin laaja johtoryhmä
16.12.2025	Tietoturvapäällikkö	Kajaanin kaupunginhallitus



Konsernipalvelut
Tietoturva

1 Kajaanin kaupungin tietoturva- ja tietosuojapolitiikka

Tietoturva- ja tietosuojapolitiikka on Kajaanin kaupungin ylimmän johdon hyväksymä strateginen asiakirja tietoturvallisen toiminnan ylläpitämiseksi ja kehittämiseksi. Poliitiikan tavoitteena on varmistaa tietoturvallisuutta ja tietosuojaa koskevat yhdenmukaiset toimintaperiaatteet ja käytännöt. Poliitiikka määrittää tietoturvallisuutta ja tietosuojaa koskevat periaatteet, vastuut ja tavoitteet. Poliitiikan toteuttamisella luodaan edellytykset tietoturvallisen toiminnan pitkäjänteiseen kehittämiseen ja sitä täydennetään tarkentavilla linjauksilla ja ohjeilla.

Tietoturva- ja tietosuojapolitiikka koskee kaupungin koko organisaatiota – niin henkilöstöä kuin luottamushenkilöitäkin – sekä niitä kaupungin sidosryhmien edustajia, jotka toimeksiantojaan puitteissa käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa. Poliitiikka kattaa kaupungin käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta tai elinkaaren vaiheesta.

Tietoturva- ja tietosuojapolitiikan tavoitteet saavutetaan vain, jos kaikki noudattavat yhteisesti sovittuja periaatteita.

1.1 Tietoturvan määritelmä

Tietoturvallisuus on kiinteä osa kaupungin johtamista, palveluita ja toimintoja. Se ulottuu jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin sekä luottamushenkilöiden toimintaan kaupungin asioiden käsittelijöinä. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietoturvalla tarkoitetaan hallinnollisia, teknisiä ja muita järjestelyitä, joilla pyritään varmistamaan eri muodoissa olevan tiedon saatavuus, eheys ja luottamuksellisuus. Tietoturvan järjestämisellä ja hallinnalla pyritään varmistamaan myös, että digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla. Digitaalinen turvallisuus koostuu tietoturvallisuudesta, siihen liittyvästä riskienhallinnasta, varautumisesta ja toiminnan jatkuvuuden hallinnasta sekä tietosuojasta sekä kyberturvallisuudesta.

Tietosuoja on oleellinen osa tietoturvaa ja sillä tarkoitetaan toimenpiteitä, joilla varmistetaan henkilötietojen asianmukainen käsittely ja yksityisyyden säilyminen oikeudellisia säännöksiä noudattavin periaatein ja käytännöin.

Tietoturvallisuuteen liittyvillä vastuutuksilla ja käytännöillä pyritään varmistamaan kaupungin omistaman ja hallinnoiman tiedon;

- Saatavuus: Tiedot ovat käytettävissä oikeaan aikaan häiriöttä.
- Eheys: Tiedot ovat oikeita ja virheettömiä, eikä niitä pysty muuttamaan teknisen tai inhimillisen toiminnan seurauksena ilman tarvittavia valtuuksia.
- Luottamuksellisuus: Tiedot ovat vain niihin oikeutettujen saatavilla.
- Kiistämättömyys: Tietojen käsittely tai tarkastelu pystytään todistamaan jälkikäteen.



Konsernipalvelut
Tietoturva

- Todentaminen: Tietoa käsittelevä tai tarkasteleva taho pystytään tunnistamaan luotettavasti.

Kaupungin tietoturvatyötä ohjaavat kuntia velvoittavat lait ja asetukset (mm. laki julkisen hallinnon tiedonhallinnasta (906/2019), EU:n yleinen tietosuoja-asetus (2016/679), tietosuoja-laki (1050/2018)), Valtiovarainministeriön julkisen hallinnon tiedonhallintalautakunnan suositukset, Digi- ja väestötietoviraston ohjeet ja suositukset sekä kaupungin omat voimassa olevat strategiat, hallinto- ja ohjesäännöt, riskienhallinta-, valmius- ja viestintäsuunnitelmat (tietoturvallisuutta koskevilta tai sivuavilta osiltaan) sekä näistä johdetut vaatimukset.

1.2 Tietosuojan määritelmä

Tietosuoja on merkittävä osa tietoturvallisuutta, vaatimustenmukaisuutta ja riskienhallintaa. 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.

Kajaanin 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 on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Tietosuojaa ohjaavina periaatteina henkilötietojen käsittelyyn ovat tietosuoja-asetuksen mukaiset: lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä tietojen eheys ja luottamuksellisuus.

Toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Tietosuoja otetaan huomioon ennakoivasti ja monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa sekä toimintaprosesseissa. Henkilöstön tietosuojaosaamisesta huolehditaan säännöllisillä koulutuksilla sekä työroolin mukaisilla ohjeistuksilla. Kajaanin kaupunki mahdollistaa asiakkaille tiedonsaannin omiin henkilötietoihinsa sekä informoi henkilötietojen käsittelystä kaupungin verkkosivuilla. Kajaanin kaupungin henkilörekistereitä käsittelevät sopimuskumppanit veloitetaan noudattamaan vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

1.3 Kajaanin kaupungin toimintaympäristö

Kajaanin kaupungin tuottamien palveluiden häiriötön toiminta luo perustan arjen toimivuudelle. Yhteiskunnan digitaalinen kehitys on muuttanut organisaatioiden toimintaympäristöjä ja lisännyt niihin kohdistuvia uhkia, minkä seurauksena tietojen ja toimintojen turvaamiseen liittyy uudenlaisia haasteita. Kajaanin kaupungin tuottamat palvelut ovatkin enenevässä määrin riippuvaisia digitaalisen toimintaympäristön luotettavasta toiminnasta.



Konsernipalvelut
Tietoturva

Digitaalisen toimintaympäristön hallinta edellyttää suunnitelmallisuutta ja joustavaa kykyä reagoida odottamattomiin tapahtumiin ja palautua niistä varmistaen kriittisten palveluiden jatkuvuus. Riskienhallintatoimenpiteiden tulee olla ajantasaisia, oikeasuhtaisia ja riittäviä. Huomioimalla digitaalinen turvallisuus päivittäisessä toiminnassa varaudutaan erilaisiin uhkatilanteisiin ja varmistetaan tietoturvan, tietosuojan ja lainsäädännöllisten velvoitteiden toteutuminen.

2 Tietoturvatyön tavoitteet

Tietoturvatyön tavoitteena on varmistaa Kajaanin kaupungin palveluiden luotettava ja häiriötön toiminta sekä digitaalisen toimintaympäristön turvallisuus. Tietoturvatyö on osa kaupungin kokonaisturvallisuutta, ja sen toteuttamisessa noudatetaan lainsäädäntöön perustuvia periaatteita.

Tietoturvatyön tavoitteena on varmistaa kaupungin tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit huomioon ottaen. Lisäksi varmistetaan lainsäädännön, kansallisten ohjeiden ja parhaiden käytäntöjen noudattaminen arjen työssä ja palveluiden kehittämisessä.

Riskienhallinnan näkökulmasta tavoitteena on tunnistaa, arvioida ja hallita toimintaan kohdistuvat riskit sekä toteuttaa tarvittavat toimenpiteet jäännösriskit huomioiden. Tietojen asianmukainen käsittely turvataan tiedonhallintalain (Laki julkisen hallinnon tiedonhallinnasta 906/2019) mukaisilla tietoturvakäytännöillä.

Tietoturvan kehittämistoimenpiteet johdetaan tietoturvapolitiikan ja toimintaympäristön vaatimuksista ja tavoitteita tarkennetaan vuosittain Kajaanin kaupungin tietoturvan työryhmällä.

Tietoturvatyön tavoitteet:

1. Muuttuva toimintaympäristö ja tilannekuvan ylläpito
 - o toiminnan mahdollistavat ja jatkuvuuteen liittyvät kriittiset kohteet on tunnistettu
 - o vakavat uhkatekijät tunnistetaan ja niiden hallinta ja toimenpiteet on suunniteltu
 - o ajantasaisen tilannekuvan teknistä näkyvyyttä kehitetään ja ylläpidetään
2. Palveluiden jatkuvuus ja tietojen turvaaminen
 - o digitaalinen toimintaympäristö toimii luotettavasti
 - o tietoturva- ja tietosuojatoimenpiteitä hallitaan
 - o kriittisten toimintojen ja palveluiden jatkuvuus turvataan normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa
3. Organisaation osaamisen ja kyvykkyyden kehittäminen
 - o tietoturva- ja tietosuojatietoisuuden ja osaamisen lisääminen
 - o positiivisen tietoturva- ja tietosuojakulttuurin ylläpitäminen
 - o henkilöstö ja muut palveluiden käyttäjät noudattavat tietoturvapolitiikkaa ja toimivat vastuullisesti tietoturvallisilla toimintatavoilla



Konsernipalvelut
Tietoturva

4. Toimitusketjujen tietoturvan varmistaminen

- o Ulkoiset palveluntuottajat, yhteistyökumppanit ja alihankintaketjut ovat sitoutuneet noudattamaan Kajaanin kaupungin hyväksymiä tietoturvakäytänteitä.
- o Hankintojen ja palveluostojen tietoturvasta huolehditaan ennakoiden ja tiedon elinkaari huomioiden. ICT-järjestelmä- ja palveluhankinnat ovat tietohallinnon hyväksymiä.
- o Palveluiden jatkuvuuden hallinnasta huolehditaan sopimuksilla ja palvelun hallinnalla. ICT-toimittajaympäristössä on sovittu selkeät vastuunjaot.

5. Tietosuojaan varmistaminen

- o Tietosuojaan ja rekisteröityjen oikeuksien toteutumista seurataan säännöllisesti ja systemaattisesti.
- o Osoitusvelvollisuuden edellyttämä dokumentaatio pidetään ajan tasalla (rekisteröityjen informointi, seloste käsittelytoimista, vaikutustenarvioinnit, tietovirtakuvaukset, henkilöstön koulutukset ja palveluntuottajien kanssa laaditut sopimukset).
- o Henkilötietojen käsittelijöiden kanssa laaditaan kuvaukset henkilötietojen käsittelystä, sekä varmistetaan sopimuksellisesti henkilötietojen käsittelyyn liittyvät ehdot.

6. Lokitietojen hallinta

- o Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, kun tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.
- o Lokitietoja käsitellään lainsäädännön mukaisesti tietosuoja huomioiden.

7. Käyttövaltuuksien hallinta

- o Käyttövaltuudet määritellään työntekijän tehtäviin liittyvien käyttötarpeiden mukaan.
- o Käyttövaltuushallinnassa huolehditaan käyttöoikeuksien elinkaaren aikaisesta hallinnasta ja tarpeettomien käyttöoikeuksien poistosta.

ICT-arkkitehtuuria kehitetään tietoturvallisuus ja lainsäädännön velvoitteet huomioiden. Luotettavat ja palvelutoimintaa tukevat tietoturvaratkaisut mahdollistavat digitaalisten palveluiden kehittämisen sekä tehokkaat ja modernit työtavat. Uusia tietojärjestelmiä ja palveluita hankittaessa tulee suunnitteluvaiheessa huomioida lisäksi tietosuojaan vaikutustenarviointi, mikäli palvelussa käsitellään henkilötietoja.

Toimintaympäristössä tapahtuvissa merkittävässä muutoksissa muutoksesta vastaava taho laatii tiedonhallintalain mukaisen muutosvaikutusten arvioinnin (Laki julkisen hallinnon tiedonhallinnasta 906/2019). Arvioinnin tarkoituksena on varmistaa muutosten hallinnolliset, taloudelliset, toiminnalliset ja riskeihin perustuvat vaikutukset, sekä pyrkiä varmistamaan tietojärjestelmien yhteentoimivuus, tietoturvallisuus ja tietoaineistojen lainmukainen käsittely.



Konsernipalvelut
Tietoturva

2.1 Muuttuva toimintaympäristö ja tilannekuvan ylläpito

Tiedonhallintalaki velvoittaa tiedonhallintayksikköä seuraamaan tietoturvallisuuden tilaa ja varmistamaan tietoa-aineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Lisäksi tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Digitaalisen toimintaympäristön tilannekuvan muodostaminen ja ylläpito vaatii sekä Kajaanin kaupungin oman, kuin myös organisaation ulkopuolisen toimintaympäristön havainnointia. Tämän toteuttamiseen tarvitaan niin automaattista havainnointia tietojärjestelmien, palveluiden ja päätelaitteiden tapahtumista kuin myös henkilöstön tekemiä havaintoja sekä erilaisista ulkoisista lähteistä kerättyä uhka- ja tilannetietoa. Tilannekuvan ylläpidolla havaitaan mahdollisia tietoturvallisuuteen liittyviä uhkatekijöitä ja ehkäistään turvallisuuteen liittyvät poikkeamat normaalitilanteesta.

Havainnointikyky mahdollistaa tiedonkäsittelyyn liittyvien päivittäisten tapahtumien ja tapahtumaketjujen osapuolten yksiselitteisen selvittämisen, kiistämättömyyden ja jäljitettävyyden. Tätä kautta varmistetaan myös tietoa käsittelevien henkilöiden oikeusturvan toteutuminen.

Kajaanin kaupunki tunnistaa toiminnan mahdollistavat ja jatkuvuuteen liittyvät kriittiset kohteet, kuten tietojärjestelmät, tilat ja muut tietoturvallisuuteen vaikuttavat kohteet, havainnoi toimintaympäristön tilaa ja reagoi uhkatekijöihin ja poikkeamiin proaktiivisesti. Tietoturvan tason tulee noudattaa lainsäädännön velvoitteita ja mukautua muuttuvan toimintaympäristön asettamiin vaatimuksiin.

Tietoturvallisuustoimet tulee suhteuttaa suojattavaan tietoon. Tietoturvatoimia tulee mitoitaa sekä järjestelmän tietosisällön, että kaupungin kriittisten prosessien näkökulmasta. Tietoa-aineistoihin, tietovarantoihin ja tietojärjestelmiin kohdistuvia riskejä tulee tarkastella osana kokonaisvaltaista riskienhallinnan prosessia. Tieto- ja ICT-riskien hallinnassa sovelletaan kaupungin riskienhallinnasta annettuja ohjeita.

2.2 Palveluiden jatkuvuus ja tietojen turvaaminen

Tietojärjestelmien, tietoverkkojen ja tietojenkäsittelyn keskeytyksetön toiminta on perusedellytys Kajaanin kaupungin tuottamien palveluiden toimivuudelle. Tietojen luvaton käyttö sekä tahaton tai tahallinen tuhoaminen tai vääristäminen tulee havaita ja estää, ja näistä mahdollisesti aiheutuvat vahingot on pyrittävä minimoimaan.

Kajaanin kaupunki varautuu turvaamaan 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. Toimialat, liikelaitokset ja keskeiset sidosryhmät kehittävät digitaalisen



Konsernipalvelut
Tietoturva

turvallisuuden hallintamallia määrittelemällä kriittisyysluokittelut ja hallinnalliset toimenpiteet tietojärjestelmille, tiedoille ja palveluille.

Tietoturvapoikkeamien hallintaa kehitetään riskilähtöisesti muuttuva toimintaympäristö huomioiden. 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 tietoturvan työryhmällä ja raportoidaan johdolle kaupunginjohtajan erikseen tarkemmin ohjeistamalla tavalla. Poikkeamista tiedotetaan henkilöstölle niiden luonteen ja laajuuden edellyttämällä tavalla.

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

2.3 Organisaation osaamisen ja kyvykkyyden kehittäminen

Tietoturva- ja tietosuojapolitiikka sekä tietoturvan ja tietosuojan ohjeet ja linjaukset ovat osa kaupungin johtamista ja käytännön toimintaa. Tämä edellyttää henkilöstöltä tietoturvakäytäntöjen tuntemista, ohjeiden noudattamista ja jatkuvaa osaamisen päivittämistä. Tietoturva- ja tietosuojakoulutukset ovat osa säännöllistä kehittämis- ja perehdyttämistoimintaa. Tavoitteena on positiivisen tietoturvakulttuurin kehittämisen ja ylläpidon kautta parantaa organisaation kyvykkyyttä vastata tietoturvan uhkakuviin. Henkilöstö noudattaa annettuja ohjeita ja toimii vastuullisesti tietoturvallisilla toimintatavoilla.

Johdon tehtävänä on varmistaa koulutuksen ja ohjeiden avulla, että henkilöstön tietoturva- ja tietosuojaosaaminen on riittävää. Myös osaamisen ylläpidosta on huolehdittava niin, että se vastaa kulloinkin vallitsevia tilanteita ja toimintaympäristön vaatimuksia. Esihenkilö huolehtii uudessa tehtävässä aloittavan työntekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään. Tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti, ja tietoturva- ja tietosuojaohjeet pidetään henkilöstön saatavilla.

Jokaisen Kajaanin kaupungin työntekijän tulee vuosittain suorittaa omatoiminen tietoturva- ja tietosuojakoulutus ja siihen liittyvä testi. Esihenkilö tarkistaa alaistensa osalta sen suorittamisen. Koulutuksia ja ohjeita päivitetään vastaamaan digitaalisen toimintaympäristön muutoksia sekä lainsäädännön uudistuksia. Luottamushenkilöiden tulee osallistua kaupungin järjestämään tietoturva- ja tietosuojakoulutukseen (osana luottamustoimen hoitamiseen perehtymistä) ja sitoutua noudattamaan luottamustoimessaan kaupungin tietoturva- ja tietosuojaohjeita.

2.4 Toimitusketjujen tietoturvan varmistaminen

Tietoturvallisen toimintaympäristön hallinta edellyttää tietoturvan huomioon ottamista hankinnoissa, palveluostoissa ja kumppanuuksissa jo niiden suunnitteluvaiheessa. Myös



Konsernipalvelut
Tietoturva

tiedonhallintalaki velvoittaa viranomaisia varmistamaan hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Tietohallinto hyväksyy kaikki tietojärjestelmähankinnat hankintaprosessin mukaisesti. Palveluntuottajat ja alihankintaketjut sitoutetaan sopimuksilla noudattamaan Kajaanin kaupungin tietoturva- ja tietosuojakäytänteitä. Hankinnoissa sopimuksen omistaja huomioi tietoturva- ja tietosuojasitoumusten laatimisen yhteistyökumppanien kanssa. Asiantuntija-apua antavat konsernipalveluiden tietoturvapääällikkö ja tietosuojavastaava.

Tietojärjestelmä- ja ICT-sopimuksissa tulee huomioida myös toiminnallinen vastuunjako tietoturvan, tietosuojan, palveluiden jatkuvuuden ja varautumisen osalta, esimerkiksi RACI-mallilla. Säännöllinen seuranta ja raportointi palvelutason toteutumisesta, häiriötilanteiden hallinnasta ja tietoturvapoikkeamista sekä rikkomuksiin liittyvistä käytänteistä ovat osa palveluiden hallinnointia.

2.5 Tietosuojan varmistaminen

Kajaanin kaupungissa henkilötietojen käsittelyssä määritellään aina rekisterinpitäjä. Kajaanin kaupungin rekisterinpitäjinä toimivat pääsääntöisesti toimielimet ja poikkeustapauksissa yksittäinen viranhaltija. Rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta, laatii tietosuojan vaikutustenarvioinnit ja tietovirtakuvaukset osoitusvelvollisuuden toteuttamiseksi (Tietosuojalaki 1050/2018 ja EU:n yleinen tietosuoja-asetus 679/2016).

Rekisterinpitäjä määrittää mihin käyttötarkoitukseen ja millä keinoin henkilötietoja käsitellään.

Kajaanin kaupungissa noudatetaan seuraavia tietosuojaperiaatteita:

- Tietosuojan varmistamiseksi kaupunki kerää ainoastaan ennalta määriteltujen, laillisten käyttötarkoitusten kannalta tarpeellisia henkilötietoja kaupungin tehtävien suorittamiseksi ja palveluiden kehittämiseksi.
- Kaupunki huolehtii suunnitelmallisesti ja läpinäkyvästi henkilötietojen suojaamisesta ja elinkaarenhallinnasta.
- Rekisteröidyille mahdollistetaan helppo tiedonsaanti omien henkilötietojen osalta ja rekisteröityjä informoidaan kattavasti henkilötietojen käsittelyn periaatteista ja tarkoituksista.
- Säännöllisillä koulutuksilla pyritään varmistamaan, että kaupungin henkilöstöllä on riittävä tietosuojaosaaminen tehtävänkuvan mukaisesti.
- Henkilötietojen käsittelystä yksilöiden vapauksille ja oikeuksille aiheutuvia riskejä arvioidaan säännöllisesti.
- Sopimuskumppaneiden osalta varmistetaan, että he noudattavat vähintään lainsäädännön edellyttämiä tietosuojaperiaatteita.



Konsernipalvelut
Tietoturva

Lisätietoja rekisterinpitäjän vastuista kappaleessa 3.5 tiedonhallinnan vastuut.

2.6 Lokitietojen hallinta

Lokitiedot ovat tietojärjestelmistä automaattisesti kirjautuvia tapahtumatietoja. Niitä ovat tietojärjestelmän, sovelluksen tai laitteen tuottamat tapahtumatiedot, jotka kuvaavat esimerkiksi tietojärjestelmään ulos- tai sisäänkirjautumista, tiedon käsittelyä (katselu, lisäys, muutos, poisto) tai palomuurin suorittamaa toimenpidettä. Lokitietojen avulla seurataan tietoturvan ja tietosuojan toteutumista sekä varmistetaan tapahtumien jäljitettävyyttä. Tämä mahdollistaa poikkeamien ja väärinkäytösten ennaltaehkäisyn tai niiden todennuksen.

Lokitietojen avulla voidaan:

- muodostaa aukoton tapahtumaketju tiedonkäsittelyn ja tapahtumien todentamiseen;
- todentaa ja varmistaa tietoaaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys;
- vahvistaa ja toteuttaa henkilön tai virkavastuussa olevan oikeusturvaa tietojen käsittelyssä varmistamalla tapahtumien kiistämättömyys;
- nopeuttaa erilaisten tapahtumien tai poikkeamien selvittämistä ja niistä toipumista sekä parantaa vaatimustenmukaisuuden todentamista.

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

Lokitietojen keruu suunnitellaan osana tietojärjestelmien ja tietoaaineistojen käsittelyä jo määrittelyvaiheessa tai järjestelmä- tai palveluhankinnan yhteydessä. Keruun tarpeellisuutta arvioidaan järjestelmän tai tiedon kriittisyyden perusteella, huomioiden riskienhallinta ja vaurautuminen. Lokitietoja voidaan hyödyntää myös käytön tilastointiin lain sallimissa rajoissa.

Lokitiedot on suojattava siten, että niiden käsittely on sallittua ainoastaan siihen erikseen valtuutetuille henkilöille. Lisäksi tulee varmistaa, ettei lokitietoja voida muuttaa jälkikäteen. Lokitietojen käsittelyssä on otettava huomioon toiminnan lainmukaisuus, tiedonhallinnan elinkaaren hallinta sekä säilyttämiseen liittyvät lakisääteiset velvoitteet. Kaikessa lokitietojen käsittelyssä on varmistettava rekisteröityjen henkilöiden, tietojärjestelmien käyttäjien ja ylläpitäjien tietoturvan, tietosuojan ja oikeusturvien toteutuminen.

Tietojärjestelmän omistaja huolehtii lokitietojen määrittelystä ja siitä, että niitä käsitellään lainsäädännön edellytysten mukaisesti. Lokien tiedonsaantioikeudet, rekisterinhallinta, tietojen luovuttamiseen liittyvät prosessit ja käytännöt huomioidaan palvelusopimuksissa ja osana hankintaprosessia.

Kun yksityinen palveluntuottaja toimii viranomaisen toimeksiannosta ja ulkoisen palveluntuottajan järjestelmissä käsitellään viranomaisen tietoaaineistoja, viranomainen on rekisterinpitäjä ja sillä on oikeus saada lokitietoja. Asianomainen toimiala tai liikelaitos määrittelee yksityiselle palveluntuottajalle tietojen luovuttamisen toimintaprosessit ja käytänteet.



Konsernipalvelut
Tietoturva

2.7 Käyttövaltuuksien hallinta

Tiedonhallintalain mukaan tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina. (Laki julkisen hallinnon tiedonhallinnasta 906/2019, 16§)

Tietojärjestelmän omistajan tehtävä on määrittää tietojärjestelmän käyttövaltuustasot ja missä työtehtävissä niitä tarvitaan. Käyttövaltuuksien myöntämisessä on huomioitava tietojenkäsittelyn oikeuksiin liittyvät lakisääteiset velvoitteet ja ajantasaisuus. Esihenkilöt ja pääkäyttäjät määrittävät käyttövaltuudet työtehtävien mukaisesti ja pitävät ne ajan tasalla. Pääsyn- ja käyttäjähallinnan avulla varmistetaan tietojen luvallinen käyttö ja estetään luvaton käyttö. Hallinnan tulee perustua vähimpien oikeuksien periaatteeseen ja kattaa koko järjestelmän tai palvelun elinkaari.

Vähimpien oikeuksien periaate tarkoittaa, että käyttäjälle myönnetään toimintaympäristöön, tietojärjestelmiin, palveluihin ja tietoon vain sellaiset käyttövaltuudet, jotka ovat välttämättömiä tehtävän suorittamiseksi.

Käyttövaltuuksien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi. Kajaanin kaupungin toimialueen (Active Directory ja Microsoft Entra ID) käyttövaltuuksien hallinnasta ja perustason pääsyoikeuksien myöntämisestä vastaa yhteistyökumppani.

Käyttäjätilin luominen, käyttövaltuuksien hallinta ja ylläpito tapahtuu määritellyllä käyttöoikeuksien hakuprosessilla. Työsuhteen muodostuessa tai uuden työtehtävän alkaessa esihenkilö hakee työntekijälle perustason pääsyoikeudet ja työtehtävien mukaiset tietojärjestelmäkohtaiset käyttöoikeudet. Pääsyoikeuksien myöntäminen perustuu työsopimukseen ja sen liitteisiin. Henkilöstö sitoutuu noudattamaan työnantajan sääntöjä ja ohjeita, eikä käytä hyväkseen eikä ilmaise sivullisille, mitä asioita on saanut luottamuksellisesti tietoon työssään taikka muutoin paljasta liike- tai ammattisalaisuuksia.

Käyttöoikeudet ovat henkilökohtaiset ja niitä ei saa luovuttaa kenellekään.

Esihenkilön tulee käyttöoikeuksia tilatessaan varmistaa, että:

- henkilö on oikeutettu tunnuksen saantiin;
- henkilöllä on riittävä perehdytys käyttämänsä tiedon ja tietojärjestelmien käyttöön;
- käyttäjän oikeudet on rajattu työtehtäviin ja että;
- palvelussuhteessa tapahtuvissa muutoksissa henkilön pääsyoikeudet tarkastetaan työtehtävien mukaisiksi.

Esihenkilön ja pääkäyttäjän tulee huolehtia tarpeettomien käyttöoikeuksien poistosta. Käyttövaltuuksien hallinnalla huolehditaan käyttäjätunnuksen ja pääsyoikeuksien elinkaarenhallinnasta työsuhteen aikana.



Konsernipalvelut
Tietoturva

Käyttövaltuuksien käyttöä valvotaan poikkeamien havaitsemiseksi ja käsittelemiseksi määriteltujen periaatteiden mukaisesti. Yhteiskäyttötunnuksia voidaan käyttää vain erikseen hyväksytyissä poikkeustapauksissa. Päätöksen yhteiskäyttötunnuksista tekee dokumentusti tietojärjestelmän omistaja. Käyttövaltuuksien ylläpidosta, käytöstä ja muutoksista voidaan kerätä lokitiedot, joiden säilytysajat määräytyvät lakisääteisten velvoitteiden mukaisesti.

Kajaanin kaupungin hallintatason eli administrator-tason pääsyoikeudet ja muut erityiset käyttäjätunnukset haetaan erillisen prosessin mukaisesti. Näiden tunnusten käyttäjiltä edellytetään salassapitositoumuksen hyväksyminen ja allekirjoittaminen tunnuksen myöntämisen yhteydessä.

Hallintatason pääsyoikeudet myönnetään etuoikeutettujen käyttöoikeuksien hallinnan vaatimusten periaatteita noudattaen (Privileged Identity Management). Tämä tarkoittaa valvotun käyttöoikeuden myöntämistä vain tarvittaessa ja oikea-aikaisesti rajatulla aikavälillä.

Administrator-tunnuksen käytön aktivointiin tarvitaan aina perusteltu syy, mikä kirjataan käyttötarkoituksen mukaisesti ylös. Tunnusten käytöstä kerätään lokitietoa, jonka avulla voidaan todentaa hallintatason tunnuksella tehdyt toimenpiteet.

Erityistä käyttöä varten perustettavat pääsyoikeudet, kuten palvelutilit esim. ohjelmistorobotiikalle arvioidaan ja määritellään tarvepohjaisesti. Myönnetylle oikeudelle täytyy määritellä voimassaoloaika sekä omistajuus, jota edustaa luonnollinen henkilö.

Vaaralliset käyttövaltuusyhdistelmät on tunnistettava, dokumentoitava ja eriytettävä mahdollisuuksien mukaan prosessin omistajan toimesta. Mikäli tehtäviä ei voida eriyttää, tulee niistä syntyviä riskejä hallita.

Käyttövaltuuksien hallinnassa ja valvonnassa kiinnitetään erityistä huomiota työrooleihin, joihin liittyy korotettu riski. Tällaisia ovat esimerkiksi pääkäyttäjien, ylläpitäjien ja muiden erityistä luottamusta vaativien tehtävien käyttöoikeudet.



Konsernipalvelut
Tietoturva

3 Tietoturva- ja tietosuojatyön vastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kaupungin sääntöjen mukaisesti. Kaupunginhallituksen hyväksymässä tietoturva- ja tietosuojapolitiikassa määritellään tietoturvan ja tietosuojan vastuut ja velvollisuudet.



Kuva 1. Tietoturvan ohjaus ja vastuut

3.1 Kaupunginhallituksen ja kaupungin johdon vastuut

Kajaanin kaupungin kokonaisvaltaisen riskienhallinnan ja sitä kautta tietoturvan ja tietosuojan toteuttamisen kokonaisvastuu on kaupunginhallituksella ja kaupunginjohtajalla. Kaupungin johto sitoutuu tietoturvan ja tietosuojan jatkuvaan kehittämiseen ja huolehtii työn riittävästä resursoinnista ja jatkuvuudesta.

Kaupunginhallitus päättää tietoturva- ja tietosuojapolitiikasta sekä siihen ehdotetuista muutoksista, seuraa tietoturvallisuuden sekä tietosuojan toteutumista kaupungissa lainsäädännön mukaisesti ja sillä on vastuu kaupungin sisäisen valvonnan ja riskienhallinnan järjestämisestä. Kaupunginhallitus toimii rekisterinpitäjänä silloin, kun tieto on käytettävissä useammalla kuin yhdellä kaupungin toimialalla. Rekisterinpitäjä määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään.



Konsernipalvelut
Tietoturva

Lauta- ja johtokunnat vastaavat toimialan/liikelaitoksen tietoturvallisesta toiminnasta ja tietosuojan järjestämisestä ja ovat toimialansa henkilötietojen käsittelyssä tietosuoja-asetuksen tarkoittamia rekisterinpitäjiä. Konsernipalvelut-toimialan osalta tehtävistä vastaa kaupunginhallitus.

3.2 Toimialojen, liikelaitosten ja tytäryhtiöiden vastuut

Lautakunta tai liikelaitoksen johtokunta vastaa alueensa tietoturvallisesta toiminnasta ja tietosuojan järjestämisestä ja on henkilötietojen käsittelyssä tietosuoja-asetuksen tarkoittama rekisterinpitäjä.

Toimialojen, liikelaitosten ja tytäryhtiöiden johtajat vastaavat riskienhallinnasta, varautumisesta ja tietoturvan ja tietosuojan toteutumisesta sekä linjausten noudattamisesta toiminnassa. Johtajien tulee tuntee toimialansa erityispiirteet ja lainsäädäntö sekä huolehtia tietoturva- ja tietosuojavastuista ja omistamiensa järjestelmien varautumisesta osana kokonaisvaltaista johtamista. Tytäryhtiöiden hallitukset ja toimitusjohtajat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta omissa organisaatioissaan.

Toimialan tai liikelaitoksen johtaja vastaa tiedonhallintamallin mukaisista tietovarannoistaan sekä näihin liittyvistä tietojärjestelmistä. Toimialojen johtajat huolehtivat vastuullaan olevien tietojärjestelmien ja sovellusten lainsäädännön mukaisten tietoturva- ja tietosuojavaatimusten toteuttamisesta. Tässä tukea antavat konsernipalveluiden asiantuntijat. Kajaanin kaupunkia velvoittavan lainsäädännön edellyttämä tietoturvan taso vaaditaan myös tietojärjestelmien toimittajilta ja palveluiden tuottajilta läpi koko toimitusketjun.

Tietojärjestelmän suojaus 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.

Uusia palveluita suunniteltaessa tai merkittävässä toimintaympäristössä tapahtuvissa muutoksissa tulee huomioida lakisääteinen velvoite tehdä muutosvaikutusten arviointi (Laki julkisen hallinnon tiedonhallinnasta 906/2019) ja huolehtia rekisterinpitäjän informoinnista.

Tiedonhallintaan kuuluvia toimialan tai liikelaitoksen vastuita käsitellään kappaleessa 3.5 Tiedonhallinnan vastuut.

3.3 Esihenkilön tietoturvavastuut

Esihenkilö vastaa tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan. Esihenkilön vastuulla on varmistaa, että toimialan lakisääteisiä tietoturva- ja tietosuojakäytänteitä noudatetaan, sekä huolehtia työntekijöiden riittävästä perehdyttämisestä ja säännöllisestä koulutuksesta kaupungin tietoturva- ja tietosuojakäytänteisiin. Esihenkilön tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojusta annettuja ohjeita.



Konsernipalvelut
Tietoturva

Esihenkilön tehtävänä on varmistaa, että jokainen työntekijä:

- on perehtynyt tehtäviinsä liittyviin tietoturva- ja tietosuojaohjeisiin,
- on suorittanut kaupungin tietoturva- ja tietosuojakoulutukset,
- ymmärtää oman vastuunsa tietoturvasta ja tietosuojasta toiminnassaan,
- käsittelee tietoja oikein ja tarkoituksenmukaisesti,
- tiedostaa, että väärinkäytöksillä voi olla rikosoikeudellinen luonne

Kehityskeskusteluissa esihenkilö voi tarkistaa, onko työntekijä suorittanut tarvittavat tietoturva- ja tietosuojakoulutukset ja perehtynyt riittävästi työtehtäviinsä liittyviin tietoturva- ja tietosuojakäytänteisiin. Esihenkilöä koskevat samat velvoitteet, kuin työntekijää.

Esihenkilön ja tietojärjestelmien pääkäyttäjien vastuulla on huolehtia työntekijöiden käyttöoikeuksista ja siitä, että oikeudet annetaan työtehtävien edellyttämässä laajuudessa. Käyttövaltuus- ja pääsynhallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään luvaton käyttö. Käyttöoikeudet toteutetaan Kajaanin kaupungilla roolipohjaisesti työtehtävien hoitoon tarvittavassa laajuudessa. Hallinnan tulee noudattaa vähimpien oikeuksien periaatteita ja sen on toteuduttava järjestelmän tai palvelun koko elinkaaren ajan.

Käyttöoikeudet ovat henkilökohtaiset ja niitä ei saa luovuttaa kenellekään.

Esihenkilö vastaa oman vastuualueen toiminnassa syntyvien asiakirjojen oikeaoppisesta säilytyksestä ja arkistoinnista. Esihenkilön vastuulla on myös huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa ja työsuhteen päättyessä työntekijät palauttavat kaikki työnantajalle kuuluvat laitteet sekä tiedot ja käyttöoikeudet tietojärjestelmistä poistetaan.

Esihenkilön tulee varmistaa, että työntekijä tai harjoittelija on tietoinen vaitiolovelvollisuuden jatkumisesta myös palvelussuhteen sekä harjoitteluajan päättymisen jälkeen. Esihenkilöiltä odotetaan esimerkillistä ja vastuullista tietoturvakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvapoikkeamista omalle esihenkilölle ja tietoturva- ja tietosuojatyöryhmälle.

3.4 Työntekijän tietoturvavastuut

Työntekijällä tarkoitetaan tässä sekä työsopimus- että virkasuhteista henkilöstöä.

Työsuhteen perustamisen yhteydessä työntekijä sitoutuu noudattamaan työnantajan sääntöjä ja ohjeita. Työntekijä sitoutuu IT-palveluiden käyttösääntöihin sekä suorittaa säännöllisesti ajantasaiset tietoturva- ja tietosuojakoulutukset. Koulutuksia voidaan järjestää myös toimialakohtaisesti tarpeen mukaan. Työntekijään rinnastettavat tietoturva- ja tietosuojavelvoitteet koskevat myös luottamushenkilöitä sekä muita tahoja, joille on myönnetty Kajaanin tietoverkon käyttäjätunnukset.

Jokainen työntekijä on vastuussa siitä, että noudattaa kaupungin tietoturva- ja tietosuojaohjeita ja käsittelee tietoja oikein ja tarkoituksenmukaisesti työssään. Tavoitteena on, että työntekijä ymmärtää oman oikeusturvansa ja sen, että väärinkäytöksistä voi seurata



Konsernipalvelut
Tietoturva

rikosoikeudellisia seuraamuksia. Jokainen vastaa myös itse niistä tietoturvariskeistä, jotka liittyvät hänen päätöksiinsä tai päätöksentekovaltaansa.

Käyttöoikeudet ovat henkilökohtaiset eikä niitä saa luovuttaa kenellekään.

Työntekijä vastaa käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokittelusta (julkisuuden ja salassapidon määrittely) sekä siitä, että tietoja käsitellään organisaation tietoturva- ja tietosuojakäytäntöjen mukaisesti. Kun tietojen säilytysaika päättyy, viranomaisen asiakirjat on hävitettävä hyväksytyn tiedonohjaussuunnitelman mukaisesti. Työsuhteen muuttuessa tai päättyessä työntekijän on luovutettava kaikki työnantajalle kuuluva tieto ja laitteet. Muiden tietojen siirrosta tai hävittämisestä on sovittava esihenkilön kanssa ennen työsuhteen päättymistä. Työntekijän on ilmoitettava viipymättä esihenkilölleen ja tietoturva- ja tietosuojatyöryhmälle kaikista tietoturvaan ja tietosuojaan liittyvistä poikkeamista, puutteista, uhkista ja riskeistä. Tietoturvatavoitteet saavutetaan vain, jos kaikki noudattavat yhteisesti sovittuja periaatteita.

3.5 Tiedonhallinnan vastuut

Kajaanin kaupunki toimii yhtenä tiedonhallintayksikkönä ja kaupunginhallituksen vastuulla on varmistaa, että tiedonhallinnan vastuut, käytännöt ja valvonta on selkeästi määriteltä viranomaisen tai vastuuhenkilön tehtävissä. Tiedonhallintaan liittyvät vastuut on määritetty tässä tietoturvapoliitikassa, sisäisen valvonnan ja riskienhallinnan ohjeella sekä kaupungin hallintosäännössä.

Kajaanin kaupunki ylläpitää ja kehittää digitaalisen turvallisuuden ja tiedonhallinnan hallintamallia. Malli sisältää vastuunjaot toimintaprosesseista, tietovarannoista ja tietojärjestelmistä. Tiedonhallintamallia ylläpidetään ja päivitetään digitaalisen turvallisuuden ja tiedonhallinnan hallintajärjestelmässä.

Hallintajärjestelmään tallennetaan tiedot, joiden avulla muodostetaan tiedonhallintalain mukaiset kuvaukset: tiedonhallintamalli ja asiakirjajulkisuuskuvaus. Kuvausten sisältö on tiedon omistajien vastuulla ja niiden ylläpito edellyttää moniammatillista asiantuntemusta ja yhteistyötä.

Kajaanin kaupungin jokaisen prosessin, tietojärjestelmän ja tietovarannon omistaja on toimialan, liikelaitoksen tai tulosalueen johtaja, jonka toimintaan tietojärjestelmä lähinnä liittyy tai jonka toimintaa se tukee, ja joka käyttää siihen kuuluvaa määräysvaltaa. Omistaja vastaa tietojärjestelmän dokumentoinnista, toimintavarmuudesta ja riskienhallinnasta. Nämä tulee huomioida myös palvelu- ja alihankintasopimuksissa.

Omistaja nimeää tietojärjestelmälle vastuuhenkilön, jonka vastuulle asianomainen tietojärjestelmä kuuluu, ja joka käyttää siihen kuuluvaa määräysvaltaa. Tietojärjestelmän vastuuhenkilö varmistaa, että tietojärjestelmä on asianmukaisesti luokiteltu, hallittu ja suojattu tiedon luokittelun ja kaupungin ohjeiden mukaisesti ja resurssien rajoissa.



Konsernipalvelut
Tietoturva

Omistajan tehtävät:

- Yhteentoimivuus ja tietoturva: Varmistaa, että tietojärjestelmät toimivat yhdessä ja että tietoturva, tietosuoja, varautuminen ja jatkuvuudenhallinta ovat kunnossa.
- Lainmukaisuus ja tiedonhallinta: Varmistaa, että tietovarantojen ja tietoaineistojen käsittely on lainmukaista, käyttövaltuudet ovat hallinnassa, ja tiedot ovat muuttumattomia, alkuperäisiä, ajantasaisia, virheettömiä ja arkistoitavissa yhteistyössä konsernipalveluiden asianhallintayksikön kanssa.

Tietojärjestelmät ja tietovarannot luokitellaan käsiteltävien tietojen kriittisyyden ja tunnistettujen tietoturvariskien mukaisesti. Luokittelussa tukea antavat konsernipalveluiden asiantuntijat. Riskit ja häiriötilanteiden toimintamallit selvitetään yhteistyössä konsernihallinnon riskienhallinnan, tietohallinnon, asianhallinnan, tietosuojavastaavan, tietoturvapäällikön sekä palvelu- ja järjestelmätoimittajan kanssa. Käyttäjille annetaan tietoturva- ja tietosuojaohjeet ja varmistetaan, että henkilöstö saa asianmukaisen koulutuksen niiden noudattamiseen.

Tiedonhallintaan liittyvät roolit vastuineen:

Rekisterinpitäjä

Vastaa henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä vastaa sisäänrakennetun ja oletusarvoisen tietoturvan ja tietosuojan toteutumisesta ja tämän toteuttamiseksi tarvittavista teknisistä ja organisatorisista toimenpiteistä sekä rekisterinpitäjälle kuuluvan osi-
tusvelvoitteen mukaisen dokumentaation ylläpidosta. Mikäli kyseessä on useamman rekisterinpitäjän yhteisrekisteri, on henkilötietojen käsittelyyn liittyvät lakisääteiset velvollisuudet ja vastuunjako sovittava ennakoon kirjallisesti.

Rekisterinpitäjä vastaa tiedon käsittelystä, luovuttamisesta, säilyttämisestä ja hävittämisestä voimassa olevaa lainsäädäntöä noudattaen.

Rekisterinpitäjä huolehtii käsittelytoimien kuvauksista, rekisteröityjen informoinnista ja oikeuksista.

Rekisterinpitäjällä on velvollisuus tehdä tietosuojan vaikutustenarviointi tietosuoja-asetuksessa yksilöidyissä käsittelytilanteissa sekä silloin, kun käsittelytoimenpide on lisätty tietosuojavaltuutetun ylläpitämään luetteloon tai kun vaikutustenarvioinnin tekemisestä on säädetty kansallisessa lainsäädännössä.

Tiedon, palvelun tai prosessin omistaja

Tiedon omistaja on se, joka tiedon tuottaa ja joka vastaa sen oikeellisuudesta. Tiedon, palvelun tai prosessin omistaja vastaa tiedon elinkaaren hallinnasta, luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön. Palvelun tai prosessin omistaja vastaa niihin liittyvästä riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.



Konsernipalvelut
Tietoturva

Pääkäyttäjä

Tietojärjestelmän omistajan nimeämä henkilö, jonka vastuulla on huolehtia järjestelmän käyttövaltuuksista. Pääkäyttäjä toimii yhteyshenkilönä järjestelmätoimittajaan ja osallistuu poikkeamien hallintaan sekä järjestelmän kriittisyys- ja riskiarviointeihin. Pääkäyttäjä seuraa tietoturvan ja tietosuojan toteutumista tietojärjestelmässä ja raportoi havaitsemistaan puutteista tietojärjestelmän omistajalle sekä tietosuojavastaavalle tai tietoturvapäällikölle.

Rekisterin yhteyshenkilö

Rekisteröityjen informointi vastuualueen rekisterin osalta. Rekisteröity voi kääntyä yhteyshenkilön puoleen saadakseen tarkempia tietoja henkilörekisteristä tai omista oikeuksistaan.

3.6 Palvelujen ja hankintojen tietoturvavastuut

Kaupungin tietojärjestelmäympäristössä käytetään tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Suunniteltaessa uusien ratkaisujen hankintaa, on noudatettava kaupungin tietojärjestelmien hankintaohjetta. Järjestelmän omistajan on varmistettava, että ratkaisut ovat tietohallinnon tiedossa ja hyväksymiä.

Uusia tietojärjestelmiä tai palveluita hankittaessa omistaja huolehtii, että hankinta täyttää tiedonhallintalain, tietosuojalainsäädännön sekä toiminnan vaatimukset tietoturvan, tietosuojan, varautumisen ja jatkuvuuden, lokitietojen keräämisen ja mahdollisten tiedon siirtämiseen liittyvien rajapintojen osalta. Omistajan tulee huolehtia, että tarjouspyyntöihin ja palvelusopimukseen sisällytetään Kajaanin kaupungin tietoturvan ja tietosuojan sopimusliitteet ja lainsäädännön asettamat vaatimukset. Sopimusliitteet löytyvät kaupungin intranetistä.

Tietojärjestelmän hankinnan yhteydessä on omistajan kartoitettava järjestelmässä syntyvät asiakirjat, niiden säilytysajat sekä säilytys ja arkistointi niin järjestelmän käytön aikana kuin järjestelmästä luovuttaessa. Samoin palvelua hankittaessa on kartoitettava palvelussa käsiteltävät tiedot, määriteltävä osapuolten vastuut sekä sovittava tietojen toimittamisesta kaupungille palvelusopimuksen päättyessä tietosuojalainsäädäntö huomioden.

Tietojärjestelmähankinnoissa tai hallinnollisissa muutoksissa omistajan tulee tarvittaessa toteuttaa tiedonhallinnan muutosvaikutusten arviointi (Laki julkisen hallinnon tiedonhallinnasta 906/2019) Arvioinnissa tunnistetaan prosessin riippuvuudet ja arvioidaan muutoksen kriittisyys riskienhallinnan näkökulmasta.

Palveluostona hankitun ICT-palvelun operatiivisesta ja teknisestä tietoturvasta ja sen ohjeistamisesta vastaa kyseisen palvelun tuottaja. Selkeät ja konkreettiset vastuunjaot tulee sopia esimerkiksi RACI-mallilla. Palvelun tuottajan tulee nimetä tietoturvan ja tietosuojan yhteyshenkilöt, jotka varmistavat sovittujen vaatimusten toteutumisen ja ilmoittavat viipymättä tietoturvapoikkeamista tai henkilötietojen tietoturvaloukkauksista palvelusopimuksessa määritellyille Kajaanin kaupungin yhteyshenkilöille.



Konsernipalvelut
Tietoturva

Kun tietosuojalainsäädäntö edellyttää tietosuojan vaikutustenarvioinnin (dpia) tekemistä, vastaa palveluntuottaja vaikutustenarviointiprosessiin osallistumisesta omalta osaltaan. Palveluntuottajat noudattavat Kajaanin kaupungin tietoturvapolitiikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

3.7 Keskitetyt tukipalvelut

Tietoturvan ja tietosuojan ohjaaminen sekä tietoturvapolitiikan valmistelu kaupunginhallituksen päätettäväksi kuuluvat konsernihallinnon alaisuudessa toimivan tietoturvapäällikön sekä tietosuojavastaavan tehtäviin.

Tietoturvapäällikkö suunnittelee, ohjaa ja koordinoi kaupungin hallinnollisen tietoturvan kehittämistoimenpiteitä sekä tähän liittyviä käytäntöjä ja prosesseja. Tietoturvapäällikkö ohjaa kaupungin tietoturvyötä, laatii esitykset kaupunkitasoisista linjauksista tietoturva- ja tietosuojatyöryhmälle ja kaupungin johtoryhmälle sekä ohjeistaa henkilöstöä. Tietoturvapäällikkö vastaa tietoturvaa koskevasta viestinnästä yhdessä Kajaanin kaupungin viestinnän kanssa. Lisäksi tietoturvapäällikkö ohjaa tietoturvaprosessien integroitumista muihin turvallisuuden osa-alueisiin ja kehittää tietoturvapoikkeamien hallinnan koordinoitua yhdessä tietohallinnon kanssa. Tietoturvapäällikkö toimii tietoturva- ja tietosuojatyöryhmän puheenjohtajana.

Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuoja säännösten noudattamisessa. Tietosuojavastaava antaa tietoa ja neuvoja tietosuojaan liittyvissä asioissa, seuraa tietosuoja-asetuksen ja kansallisten tietosuoja koskevien lakien noudattamista, tekee yhteistyötä valvontaviranomaisen kanssa ja toimii valvontaviranomaisen ja rekisteröityjen yhteispisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaava vastaa tietosuojaan liittyvästä viestinnästä ja osallistuu tietosuojan vaikutustenarviointeihin (dpia). Tietosuojavastaava ei päätä eikä vastaa kaupungin henkilötietojen käsittelystä eikä sen lainmukaisuudesta, vaan siitä vastaavat aina rekisterinpitäjä ja sen edustaja.

Kajaanin kaupungin tietohallinto järjestää kaupungin ICT-palvelut ja huolehtii kaupungin toimintaympäristön teknisen ja operatiivisen tietoturvallisuuden järjestämisestä ja tietoturvallisuuden huomioimisesta osana kokonaisarkkitehtuuria. Tietohallinto vastaa myös toimintaa tukevien tietoturvalinjausten toteuttamisesta. Tietohallinto järjestää kaupungin käyttämät päätelaitteet ja niiden keskitetyn hallinnan. Käytettävät tietojärjestelmät ja sovellukset ovat konsernihallinnon tietohallinnon tai toimialan arvioimia ja hyväksymiä. Kajaanin kaupungin tietoturva- ja tietosuojatyöryhmä voi sallia perusteltuja poikkeuksia linjauksiin.

Tietohallintojohtaja vastaa tietohallinnon riskienhallinnasta ja sisäisestä valvonnan järjestämisestä ja osallistuu tietoturvan kokonaissuunnitteluun ja kehittämiseen. Lisäksi tietohallintojohtaja vastaa resurssien varaamisesta ja kohdentamisesta tietoturvan kehittämiseksi.

Riskienhallintakoordinaattori vastaa kaupunkikonsernin riskienhallinnan kehittamisestä ja koordinoinnista. Riskienhallintakoordinaattori vastaa kaupunkikonsernin varautumisen, valmiussuunnittelun ja jatkuvuudenhallinnan kehittamisestä ja koordinoinnista. Riskienhallintakoordinaattori toimii organisaation tietoriskien hallinnan tukena ja tietosuojavastaavan sijaisena.



Konsernipalvelut
Tietoturva

Asianhallintapäällikkö johtaa asiakirjahallintoa ja vastaa kaupungin pysyvästi säilytettävistä asiakirjatiedoista ja keskusarkistosta. Hän ohjaa ja kehittää kaupungin asiakirjahallintoa osana kaupungin tiedonhallintaa, laatii asiakirjahallinnon ohjeet ja valvoo niiden noudattamista sekä huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta. Asianhallintapäällikkö hyväksyy kaupungin tiedonohjaussuunnitelman sekä vastaa salassa pidettävän tiedon luokittelusta sekä tietoturvallisuuden ja tietosuojan määrittelystä asiakirjahallinnossa.

3.8 Kajaanin kaupungin tietoturva- ja tietosuojatyöryhmä

Tietoturva- ja tietosuojatyöryhmä koordinoi tietoturvan kehittämistä, katselmoi ja ylläpitää tietoturva- ja tietosuojapolitiikkaa ja valmistelee kaupunkitasoiset linjaukset. Lisäksi tehtävinä on mm. suunnitella toimenpiteet ja toimintamallit tietoturvan kehittämiseksi sekä johdon hyväksyttäväksi, laatia esitykset tietoturvan parantamiseen tähtäävien investointien varalle sekä suunnitella ja kehittää poikkeamien hallintaa tietoturvan ja tietosuojan osalta.

Työryhmä analysoi toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietoturva- ja tietosuojariskejä. Työryhmä toimii kaupunkiorganisaation ja rekisterinpitäjien tukena tietoturva- ja tietosuoja-asioissa.

4 Normaaliolojen häiriötilanteisiin varautuminen

Kajaanin kaupunki varautuu turvaamaan ensisijaisesti kriittisten palveluiden jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä valmiussuunnitelmia, harjoittelemalla poikkeamatilanteita ja kehittämällä näihin liittyviä prosesseja.

Kajaanin kaupungin toimintaympäristöön kohdentuvissa tietoturvaloukkauksissa tai muissa tietoturvaa kohdentuvissa uhkatilanteissa vastatoimenpiteet on aloitettava välittömästi ja niistä on raportoitava ensi tilassa Kajaanin tietoturva- ja tietosuojatyöryhmälle.

Kaupungin toimintaympäristöön kohdentuvissa akuuteissa uhkatilanteissa tai merkittävässä häiriötilanteissa (Major Incident Management) kaupunginjohtajalla, hallintojohtajalla, tietohallintojohtajalla, tietoturvapäälliköllä ja riskienhallintakoordinaattorilla on oikeus sulkea tietoliikenneyhteys, järjestelmä, käyttäjätunnus tai laite vahinkojen minimoimiseksi.

5 Tietoturvan seuranta, ylläpito ja kehittäminen

Digitaalisen turvallisuuden hallintaa kehitetään ja arvioidaan säännöllisesti Kajaanin tietoturva- ja tietosuojatyöryhmällä. Tietoturvan kehittämisen tavoitteet tarkennetaan vuosittain johtamalla kehittämistoimenpiteet tietoturvapoliittikan tavoitteista ja toimintaympäristön vaatimuksista.

Tilannekuvan muodostamisessa hyödynnetään kansallisten ja kansainvälisten viranomaistahojen antamaa tietoa, tietoturva- ja tiesuojaverkostoja, digitaalisen toimintaympäristön



Konsernipalvelut
Tietoturva

tuottamaa dataa sekä henkilöstöltä ja palveluntuottajilta tulevaa tietoa. Saatujen tietojen perusteella toteutetaan riskiperusteisesti kehittämistoimenpiteitä.

Tietoturvan ja tietosuojan auditointeja suoritetaan sisäisenä tarkastuksena, ostopalveluna tai sisäisenä arviointina. Arvioinnin perusteella saatavaa tietoa hyödynnetään tietoturvariskien tunnistamisessa sekä tietoturvan kehittämisessä. Arviointeja voidaan kohdentaa myös ICT-palveluntuottajiin, mikä huomioidaan kaupungin ja palveluntuottajan välisissä sopimuksissa.

Kaupungin tietoturva- ja tietosuojapolitiikka katselmoidaan vuosittain ja päivitetään tarvittaessa.