OULUN KAUPUNGIN TIETOTURVAPOLITIIKKA

Voimaantulo 1.4.2023

KH 13.3.2023 (OUKA/2825/07.01.00/2023)

Konsernihallinto,
Digi ja ICT -vastuualue

OULU

Sisällysluettelo

Tekijä: Konsernihallinto, Digi ja ICT -vastuualue
Lisätiedot: Tietoturvapäällikkö
Taitto: Sara Kurtti, Monetra Oulu Oy, Painatuspalvelut
Paino: Monetra Oulu Oy, Painatuspalvelut

1. Oulun kaupungin tietoturvapolitiikka

Tietoturvapolitiikka on Oulun kaupungin ylimmän johdon hyväksymä strateginen asiakirja tietoturvallisen toiminnan ylläpitämiseksi ja kehittämiseksi. Tietoturvapolitiikan tavoitteena on varmistaa yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietoturvatason toteuttamiseksi. Politiikassa määritellään kaupungin tietoturvatyölle visio, tavoitteet, vastuut ja seurantatavat. Tietoturvapolitiikan toteuttamisella luodaan edellytykset tietoturvallisen toiminnan pitkäjänteiseen kehittämiseen ja sitä täydennetään erikseen hyväksyttävillä linjauksilla ja ohjeistuksilla. Tietoturvapolitiikassa määritellään myös tiedonhallinnan periaatteita ja vastuita.

1.1 Tietoturvan määritelmä

Tieto eri muodoissaan on tärkeä perusta kaupungin toiminnalle. Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen suojaamista uhkatekijöiltä siten, että palvelutoiminnan laatu, luotettavuus ja jatkuvuus varmistuvat ja että toiminnassa käsiteltäviin ja säilytettäviin tietoihin kohdentuvat riskitekijät minimoidaan. Tietoturvan järjestämiseen ja hallintaan kuuluun merkittävästi digitaalinen turvallisuus, jonka tavoitteena on toimintaympäristön turvallinen hallinta ja luotettava toiminta myös häiriötilanteissa. Digitaalinen turvallisuus koostuu tietoturvallisuudesta, tietosuojasta, kyberturvallisuudesta, riskienhallinnasta sekä toiminnan jatkuvuudenhallinnasta ja varautumisesta. Tietosuoja on merkittävä osa tietoturvaa ja se tarkoittaa ihmisten yksityisyyden kunnioittamista ja suojelemista oikeudellisia säännöksiä noudattavin periaattein ja käytännöin.

Tietoturvalla tarkoitetaan toimia, joilla varmistetaan:

- **Tietojen luottamuksellisuus:** tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeudet.
- **Tietojen eheys:** tiedon oikeellisuus ja suojaus on järjestetty niin, että tietoa ei voi tahallisesti tai tahattomasti

muuttaa vaarantaen toiminnan luotettavuutta.

- **Palveluiden ja tietojen saatavuus:** tieto on saatavissa ja käytettävissä silloin, kun sitä palvelutoiminnassa tarvitaan.
- **Kiistämättömyys:** tiedonkäsittelyyn liittyvät toimenpiteet suoritetaan niin, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa toimenpiteiden aikana ja jälkikäteen.
- **Todentaminen:** varmistetaan kohteen todenmukaisuus, oikeellisuus, alkuperä tai varmistetaan käyttäjän aitous määritellyllä luottamustasolla.

Hyvä tietoturvataso saavutetaan tietoturvapolitiikan, linjauksien ja ohjeiden mukaisilla toimintaperiaatteilla ja erilaisilla turvamekanismeilla, joita hallitaan ja katselmoidaan jatkuvan kehittämisen periaatteita noudattaen.

1.2 Oulun kaupungin toimintaympäristö

Oulun kaupunkikonserni on merkittävä toimija yhteiskunnassa, ja kaupungin tuottamat palvelut heijastuvat laajalle maantieteelliselle ja toiminnalliselle alueelle. Kaupungin tuottamien palveluiden häiriötön toiminta luo perustan arjen toimivuudelle ja uusien palveluiden kehittämiselle. Digitaalisten palveluiden kehittäminen on yksi kaupunkistrategian keskeisistä painopisteistä. Tavoitteena on edistää tiedon hyödyntämisen avulla palveluiden laatua, tehokkuutta ja vaikuttavuutta sekä alueen elinvoimaa. Oulun kaupungin tuottamat palvelut ovat kriittisesti riippuvaisia digitaalisen toimintaympäristön luotettavasta toiminnasta.

Yhteiskunnan digitaalisen kehityksen myötä organisaatioiden toimintaympäristöt ja niihin liittyvät uhkatekijät ovat muuttuneet siten, että uudenlaisia haasteita tietojen ja toimintojen turvaamiseen on tunnistettu. Digitaalisen toimintaympäristön hallinta edellyttää suunnitelmallisuutta ja joustavaa kyvykkyyttä varautua odottamattomiin tapahtumiin ja toipua niistä kriittiset toiminnot turvaten.

Tietoturvallinen toiminta mahdollistaa luotettavan digitaalisen toimintaympäristön kehittämistoimet.

Keskeinen asia on tunnistaa toimintaympäristön kriittiset rakenteet, joiden toimimattomuus vaikeuttaisi merkittävästi Oulun

kaupungin tehtävien suorittamista, aiheuttaisi merkittäviä taloudellisia tai muita vahinkoja tai heikentäisi henkilöstön turvallisuutta.

Tietoturvauhkiin varautuminen edellyttää jatkuvaa, kokonaisvaltaista ja ennaltaehkäisevää kehittämistä, minkä avulla varmistetaan palvelutoiminnan luotettavuus ja laatu sekä turvataan toiminnan jatkuvuus.

Digitaalinen turvallisuus tulee huomioida päivittäisessä toiminnassa ja palveluiden kehittämisessä, minkä avulla varmistetaan tietoturvan, tietosuojan ja lainsäädännön vaateiden toteutuminen ja varaudutaan erilaisiin uhkatilanteisiin. Riskienhallinnan näkökulmasta keskeinen tavoite on tunnistaa toimintaan kohdentuvat riskitekijät, arvioida niitä ja ryhtyä tarvittaviin toimenpiteisiin huomioiden jäännösriskit.

1.3 Kaupungin tietoturvan kehittämisvisio

Oulun kaupunki on elinvoimaltaan ja toimintakyvyltään vahva verkostokaupunki, jossa monikanavaiset palvelut tuotetaan digitaalisen turvallisuuden parhaita käytäntöjä noudattaen. Tietoturva on kiinteä osa johtamista, riskienhallintaa ja palvelutoimintaa. Oulun kaupunki on aktiivinen ja verkostoitunut digitaalisten palveluiden ja digitaalisen turvallisuuden kehittäjä. On tärkeää, että henkilökunta ymmärtää digitaalisen turvallisuuden merkityksen työtehtävissään ja on motivoitunut noudattamaan yhteisiä tietoturvallisia toimintatapoja. Tietoturvan visio julkilausuu ja vahvistaa näitä ominaisuuksia ja tavoitteita.

Visio 2026:

Oulun kaupungin digitaalisen toimintaympäristön hallinnan taso on korkea ja kuntalaispalvelut ovat tietoturvallisia ja laadukkaita.

Henkilökunta on tietoturvatietoinen ja käsittelee tietoja oikeaoppisesti ja tarkoituksenmukaisesti.

2. Tietoturvatyön tavoitteet

Tietoturvatyön tavoitteena on kehittää Oulun kaupungin toimintaympäristön digitaalisen turvallisuuden hallintaa ja siten varmistaa palvelutoiminnan luotettavuus ja jatkuvuus. Tietoturvatyö on kiinteä osa kaupungin johtamista ja riskienhallintaa ja sen avulla luodaan yhdenmukaiset tietoturvakäytänteet hallintosäännöstä johdettuja periaatteita noudattaen.

Tietoturvan kehittämisen painopisteitä ovat kokonaisvaltainen tietoturvan johtaminen, uhkatekijöiden tunnistaminen ja ennaltaehkäisy sekä tiedon ja sen arvon suojaaminen.

Tietojen oikeaoppinen ja tarkoituksenmukainen käsittely turvataan yhdenmukaisilla tietoturva- ja tietosuojakäytänteillä, jotka ovat tiedonhallintalain (Laki julkisen hallinnon tiedonhallinnasta 906/2019) edellyttämiä. Tietoturvatyössä kansallisen tason verkostoitumisella edistetään kaupungin sekä yhteiskunnan tavoitteiden ja strategioiden toteuttamista ja tuetaan kaupungin digitaalisten toimintamallien kehittämistä. Tietoturvallisilla palveluilla ja tietosuoja huomioiden varmistetaan kuntalaisten luottamus kaupungin palvelutuotantoon.

2.1 Tietoturvan uhkatekijöiden tunnistaminen ja hallinta

Tiedonhallintalaki velvoittaa tiedonhallintayksikköä tunnistamaan merkittävät tietojenkäsittelyyn kohdentuvat riskitekijät ja hallitsemaan niiden tietoturvatoimenpiteitä riskilähtöisesti. Digitaalisen toimintaympäristön hallinnassa varmistetaan kyvykkyys tunnistaa tietoturvaan kohdentuvia uhkatekijöitä herätteiden, havainnoinnin ja heikkojen signaalien tulkinnalla ja pyritään reagoimaan poikkeamiin proaktiivisesti. Tietoturvan hallinnan tason tulee noudattaa lainsäädännön velvoitteita ja mukautua tukemaan kaupungin toimintaympäristön ja palvelutoiminnan asettamia vaatimuksia.

2.2 Palveluiden jatkuvuuden ja tietojen turvaaminen

Tietojärjestelmien, tietoverkkojen ja tietojenkäsittelyn keskeytymätön toiminta täytyy turvata. Tietojen luvaton käyttö sekä tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen täytyy havaita ja estää, ja näistä mahdollisesti aiheutuvat vahingot tulee minimoida. Kriittisten toimintojen saatavuus varmistetaan sekä normaalioloissa että poikkeusolojen häiriötilanteissa mahdollisimman lyhyellä toipumisajalla. Palveluiden omistajat ja keskeiset sidosryhmät kehittävät digitaalisen turvallisuuden hallintamallia määrittelemällä kriittisyysluokittelut ja hallinnalliset toimenpiteet tietojärjestelmille, tiedoille ja palveluille.

2.3 Henkilöstön tietoturvatietoisuuden, tietosuojan ja osaamisen kehittäminen

Tietoturvapolitiikka ja -ohjeistukset sekä tietosuojakäytänteet sisällytetään luonnolliseksi osaksi kaupungin johtamista ja käytännön toimintaa. Toiminta vaatii henkilökunnalta tietoturvakäytänteiden tuntemista ja ohjeiden noudattamista. Tietoturva- ja tietosuojakoulutukset ovat osa säännöllistä kehittämis- ja perehdyttämistoimintaa. Jokainen työntekijä on velvollinen suorittamaan kaupungin edellyttämät koulutukset.

Koulutusten lisäksi henkilöstöä motivoidaan positiivisen tietoturvakulttuurin ylläpitämiseen. Tavoitteena on parantaa organisaation kyvykkyyttä vastata tietoturvan uhkakuviin ja ylläpitää yksittäisten ihmisten ja eri sidosryhmien luottamusta kaupungin tarjoamiin palveluihin sekä niiden tietoturvan, tietosuojan ja yksityisyydensuojan toteutumiseen.

2.4 Tietoturvan varmistaminen läpi toimintaketjujen

Tietoturvallisen toimintaympäristön hallinta tarkoittaa palvelutuottajien, yhteistyökumppanien ja alihankintaketjujen sitouttamista ja velvoittamista sopimusteknisesti noudattamaan Oulun kaupungin tietoturvakäytänteitä. Hankinnoissa sopimuksen omistaja huomioi tietoturva- ja tietosuojasitoumusten laatimisen yhteistyökumppanien kanssa.

Tietojärjestelmä- ja ICT-sopimuksissa täytyy huomioida myös toiminnallinen vastuunjako tietoturvan, tietosuojan, palveluiden jatkuvuuden ja varautumisen osalta, esimerkiksi RACI-mallilla.

Säännöllinen raportointi palvelutason toteutumisesta, häiriötilanteiden hallinnasta ja tietoturvapoikkeamista sekä rikkomuksiin liittyvistä käytänteistä ja sanktioista on tarpeen.

2.5 Tietoturva toiminnan kehittämisen mahdollistajana

Tietoturva- ja tietosuojatyön tavoitteena on osaltaan varmistaa, että noudatamme kulloinkin voimassa olevia lainsäädännön vaateita, kansallisia tietoturvaohjeistuksia ja kansainvälisten tietoturvastandardien mukaisia parhaita käytänteitä jokapäiväisessä työssä ja digitaalisten palveluiden kehittämisessä.

Tietoturvallinen toimintaympäristö ja luotettavat ratkaisut mahdollistavat digitaalisten palveluiden kehittämisen, tehokkaan työskentelyn ja modernit työtavat ajasta, paikasta tai työvälineistä riippumatta.

Uusia palveluita hankittaessa tulee jo suunnitteluvaiheessa huomioida tietosuojan vaikutusten arvioinnin perusteet, mikäli palvelussa käsitellään henkilötietoja. Toimintaympäristössä tapahtuvissa merkittävissä muutoksissa muutoksesta vastaava taho laatii tiedonhallinnan muutosvaikutusten arvioinnin (Laki julkisen hallinnon tiedonhallinnasta 906/2019). Arvioinnilla varmistetaan muutosten hallinnolliset, taloudelliset, toiminnalliset ja riskeihin perustuvat vaikutukset, millä pyritään varmistamaan järjestelmien yhteentoimivuus, tietoturvallisuus ja tietoaineistojen lainmukainen käsittely.

2.6 Tietosuojan varmistaminen

Tietosuoja on merkittävä osa toiminnan vaatimustenmukaisuutta, tietoturvallisuutta ja riskienhallintaa. Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata kuntalaisten, asiakkaiden, henkilöstön ja sidosryhmien henkilötietoja sekä varmistaa toiminnan läpinäkyvyys rekisteröidylle. Kaupunki käsittelee henkilötietoja sisäänrakennetun ja oletusarvoisen tietosuojan toimintaperiaatteiden mukaisesti, kulloinkin voimassa olevaa lainsäädäntöä noudattaen. Oulun kaupungin tietosuojatyön toimintaperiaatteet ovat:

Keräämme ainoastaan ennalta määriteltyjen käyttötarkoitusten kannalta tarpeellisia henkilötietoja kaupungin tehtävien suorittamiseksi ja palveluiden kehittämiseksi.

Huolehdimme suunnitelmallisesti ja läpinäkyvästi henkilötietojen suojaamisesta ja elinkaarenhallinnasta.

Varmistamme säännöllisen koulutuksen avulla, että työntekijöillä on riittävä tietosuojaosaaminen tehtävänkuvan mukaan.

Mahdollistamme asiakkaillemme tiedonsaannin omiin henkilötietoihin ja informoimme kattavasti henkilötietojen käsittelyn periaatteita.

Arvioimme säännöllisesti henkilötietojen käsittelyyn liittyviä riskejä yksilöiden oikeuksille ja vapauksille.

Varmistamme, että sopimuskumppanimme noudattavat vähintään lainsäädännön edellyttämiä tietosuojaperiaatteita.

Tietosuoja on ihmisen perusoikeus, joka turvaa rekisteröidyn henkilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Tietosuoja-asetuksen mukaiset henkilötietojen käsittelyn periaatteet ovat:

Lainmukaisuus, kohtuullisuus ja avoimuus

Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn (asiakkaan) kannalta läpinäkyvästi, miten ja missä määrin häntä koskevia henkilötietoja käsitellään.

Täsmällisyys

Käsiteltävien henkilötietojen laatu tulee varmistaa, jotta tiedot ovat täsmällisiä ja virheettömiä. Kaikki virheelliset tiedot tulee korjata.

Eheys ja luottamuksellisuus

Henkilötietojen luottamuksellisuus ja turvallisuus tulee varmistaa. Tiedot tulee suojata luvattomalta pääsyltä, vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta.

Tietojen minimointi

Käsiteltävien henkilötietojen tulee olla olennaisia, asianmukaisia ja samalla riittäviä palvelun tarjoamiseksi. Tietoja ei kerätä mitään muuta käyttötarkoitusta varten tai esimerkiksi mahdollista tulevaa käyttöä varten.

Säilytyksen rajoittaminen

Henkilötietoja tulee säilyttää vain niin kauan, kuin se on tarpeellista kyseistä käyttötarkoitusta varten. Tietojen säilytysajan tulee olla mahdollisimman lyhyt. Tietojen säilyttämisessä huomioidaan kunkin palvelun arkistointisäännöt.

Käyttötarkoitussidonnaisuus

Henkilötietoja saa käsitellä vain siinä tarkoituksessa, mitä varten ne on kerätty tai sen kanssa yhteensopivalla tavalla (esim. arkistointi). Kaupungin palveluissa käyttötarkoitus on usein lakisääteisen palvelun järjestäminen. Henkilötietoja ei voi käsitellä muihin tarkoituksiin, esim. jakaa muille asiakkaille.

Henkilötietojen käsittelyssä määritellään aina rekisterinpitäjä. Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä, oikeushenkilöä tai viranomaista, jonka käyttöä varten henkilörekisteri perustetaan tai jonka tehtäväksi rekisterinpito on lailla säädetty. Rekisterinpitäjällä on vastuu henkilötietojen käsittelyn lainmukaisuudesta ja velvollisuus tehdä tietosuojan vaikutustenarviointi ja laatia tietovirtakuvaukset osoitusvelvollisuuden toteuttamiseksi (Tietosuojalaki 1050/2018 ja EU:n yleinen tietosuoja-asetus 679/2016). Rekisterinpitäjä määrittää mihin käyttötarkoitukseen ja millä keinoin henkilötietoja käsitellään. Oulun kaupunki on määritellyt rekisterinpitäjät hallintosäännössä, ellei lainsäädännössä tai viranomaismääräyksissä määrätä toisin rekisterinpitovastuista. Tämän avulla saadaan selkeä kokonaiskuva toimintaan liittyvästä henkilötietojen käsittelystä ja siihen kohdentuvista riskeistä.

2.7. Lokitietojen hallinta

Lokitiedoilla tarkoitetaan suojattavan tiedon tai tietojärjestelmän käsittelystä tai luovuttamisesta kerättäviä käyttäjäkohtaisia merkintöjä. Myös tietoliikenneverkon käytöstä kerätään lokitietoja häiriö- tai väärinkäyttötilanteiden selvittämiseen. Lokimerkinnöistä käy ilmi jonkin tapahtuman toteutuminen ja ajankohta.

Lokitiedoilla valvotaan tietoturvan ja tietosuojan toteutumista ja jäljitettävyyttä, ennaltaehkäisten tai todentaen poikkeavia tapahtumia tai väärinkäytöksiä. Lokitiedot kerätään aina, kun tietojärjestelmän tai palvelun käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen avulla voidaan muodostaa aukoton tapahtumaketju tiedonkäsittelyn ja tapahtumien todentamiseen. Tiedoilla pystytään todentamaan ja varmistamaan tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys.

Lokitietojen avulla voidaan vahvistaa ja toteuttaa henkilön tai virkavastuussa olevan oikeusturvaa tietojen käsittelyssä varmistamalla tapahtumien kiistämättömyys.

Lokien käsittelyllä voidaan nopeuttaa erilaisten tapahtumien tai poikkeamien selvittämistä ja niistä toipumista sekä parantaa vaatimustenmukaisuuden todentamista. Kerättävät lokitiedot määritellään osana tietojärjestelmien ja tietoaineistojen käsittelyn suunnittelua määrittelyvaiheessa tai tietojärjestelmäpalvelun han-

kinnan yhteydessä. Keräämisen vaateita arvioidaan tiedon tai tietojärjestelmän kriittisyyden perusteella riskienhallinnan ja varautumisen lähtökohdista. Lokitietoja voidaan hyödyntää myös tietojen käytön tilastoinnissa lain sallimissa puitteissa.

Lokitiedot on suojattava siten, että niitä pääsee käsittelemään vain siihen oikeutettu henkilö ja että tietoja ei voi muuttaa jälkikäteen. Lokitietojen käsittelyssä on huomioitava toiminnan oikeellisuus, tiedonhallinnan elinkaari ja säilyttämisen lakisääteiset velvoitteet. Rekisteröityjen henkilöiden, tietojärjestelmien käyttäjien ja ylläpitäjien tietoturva, tietosuoja ja oikeusturva huomioidaan kaikessa lokien käsittelyssä.

Tietojärjestelmän ja tiedon omistaja huolehtii lokitietojen määrittelystä ja siitä, että niitä käsitellään lainsäädännön edellytysten mukaisesti. Lokien tiedonsaantioikeudet, rekisterinhallinta, tietojen luovuttamisen toimintaprosessit ja käytänteet huomioidaan palvelusopimuksissa.

Kun yksityinen palvelun-tuottaja toimii viranomaisen toimeksiannosta ja ulkoisen palveluntuottajan järjestelmissä käsitellään viranomaisen tietoaineistoja, viranomainen on rekisterinpitäjä ja sillä on oikeus saada lokitietoja.

Asianomainen viranomainen määrittelee yksityiselle palveluntuottajalle tietojen luovuttamisen toimintaprosessit ja käytänteet.

Lokitietojen hallinnan toteutumista tarkastellaan digitaalisen turvallisuuden hallintamallin vuosikellon mukaisesti. Tietoturvapäällikkö ja tietosuojavastaavat valvovat lokitietojen hallinnan toteutumista ja raportoivat puutteista tiedon omistajalle tai rekisterinpitäjälle.

2.8 Käyttövaltuuksien hallinta

Tietojärjestelmän, tiedon omistajan, rekisterinpitäjän tai muun vastuutahon tehtävä on määrittää tietojärjestelmän tai palvelun käyttövaltuuksien hallinnan ja käsittelyn myöntämisen periaatteet. Käyttövaltuuksien myöntämisessä on huomioitava tietojenkäsittelyn oikeuksiin liittyvät lakisääteiset velvoitteet. Pääkäyttäjät määrittelevät käyttövaltuudet työtehtävien edellyttämässä laajuudessa ja ne on pidettävä ajantasaisina. Pääsynhallinnan ja käyttäjähallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään luvatonta käyttöä. Hallinnan tulee

noudattaa vähimpien oikeuksien periaatteita ja sen on toteudutettava järjestelmän tai palvelun koko elinkaaren ajan.

Vähimpien oikeuksien periaate tarkoittaa, että käyttäjälle annetaan toimintaympäristöön, tietojärjestelmiin, palveluihin ja tietoon vain sellaiset käyttövaltuudet, jotka ovat työn suorittamisen kannalta välttämättömiä.

Käyttövaltuuksien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi. Oulun kaupungin toimialueen (Active Directory ja Azure Active Directory) käyttövaltuuksien hallinnan ja perustason pääsyoikeuksien myöntäminen on vastuutettu yhteistyökumppanille.

Käyttäjätilin luontiin, käyttövaltuuksien hallintaan ja ylläpitoon on määritelty pääsyoikeuksien anomisen palveluprosessi. Työsuhteen muodostuessa tai uuden työtehtävän alkaessa esihenkilö hakee työntekijälle perustason pääsyoikeudet ja työtehtävien mukaiset tietojärjestelmäkohtaiset käyttöoikeudet. Käyttövaltuuksien hallinnan avulla huolehditaan käyttäjätunnuksen ja pääsyoikeuksien elinkaarenhallinnasta työsuhteen aikana.

Käyttöoikeudet ovat henkilökohtaiset ja niitä ei saa luovuttaa kenellekään.

Pääsyoikeuksien myöntäminen perustuu tunnuksen saajan kanssa tehtyyn sopimukseen, mikä allekirjoitetaan työsuhteen perustamisen yhteydessä. Sopimuksessa työntekijä sitoutuu noudattamaan työnantajan sääntöjä ja ohjeita, eikä käytä hyväkseen eikä ilmaise sivullisille, mitä asioita on saanut luottamuksellisesti tietoon työssään tai muutoin paljasta liike- tai ammattisalaisuuksia.

Käyttövaltuuksien käyttöä valvotaan käyttäjän normaalikäytössä eroavien poikkeamien havaitsemiseksi ja niihin reagoimiseksi määriteltyjen periaatteiden mukaisesti. Yhteiskäyttötunnuksista pyritään luopumaan ja niitä voidaan käyttää vain erikseen hyväksytyissä poikkeustapauksissa.

Esihenkilö tilaa käyttäjätunnuksen palveluportaalin kautta ja varmistaa, että henkilöllä on riittävä perehdytys käyttämänsä tiedon ja tietojärjestelmien käyttöön. Käyttövaltuuden hakemisen ja myöntämisen yhteydessä tarkistetaan, että pääsyoikeuden saaja kuuluu henkilöstöön tai on muuten sopimusperäisesti oikeutettu tunnusten saantiin. Työsuhteessa

tapahtuvissa muutoksissa pitää aina tarkastaa henkilön työtehtävien mukaiset pääsyoikeudet. Oulun kaupungin sisäiset ja ulkoiset (esim. yhteistyökumppanit) käyttäjät erotetaan käyttäjätunnuksen muodon perusteella. Tarpeettomat käyttövaltuudet poistetaan, kun niitä ei enää tarvita. Käyttövaltuuksien ylläpidosta, käytöstä ja muutoksista kerätään lokitiedot, joiden säilytysajat määräytyvät lakisääteisten velvoitteiden mukaisesti.

Oulun kaupungin toimialueen hallintatason eli administrator-tason pääsyoikeudet ja muut erityiset käyttäjätunnukset haetaan erillisen prosessin mukaisesti. Näiden tunnusten käyttäjiltä edellytetään salassapitositoumuksen hyväksyminen ja allekirjoittaminen tunnuksen myöntämisen yhteydessä. Pääsyoikeuksien ja tunnuksen hakemisen perusteet käsitellään ja arvioidaan konsernihallinnon Digi ja ICT -vastuualueen muutoshallinnan prosessissa, jossa määritellään hallintatason tunnusten käyttötarkoitus ja pääsyoikeudet sekä hyväksytään tai hylätään hakemukset.

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

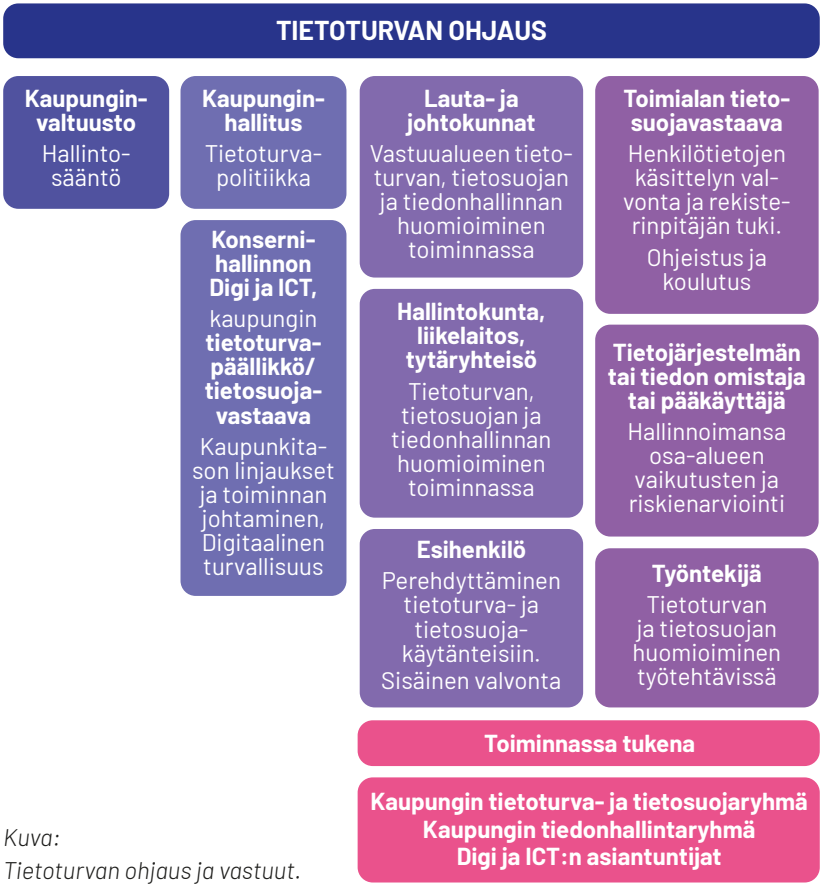
Administrator-tunnuksen käytön aktivointiin tarvitaan aina perusteltu syy, mikä kirjataan käyttötarkoituksen mukaisesti ylös. Tunnusten käytöstä kerätään lokitietoa, jonka avulla voidaan todentaa hallintatason tunnuksella tehdyt toimenpiteet.

Erityistä käyttöä varten perustettavat pääsyoikeudet, kuten palvelutilit esim. ohjelmistorobotiikalle arvioidaan ja määritellään tarvepohjaisesti. Myönnetylle oikeudelle täytyy määritellä 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 huomioita korkeamman riskiprofiilin työrooleihin ja niihin liitettyihin käyttövaltuuksiin. Tällaisia rooleja ovat mm. pääkäyttäjät, ylläpitäjät ja muut erityistä luotettavuutta edellyttävät työtehtävät.

3. Tietoturva- ja tietosuojatyön vastuut

Oulun kaupungin tietoturvan omistajuus ja ylätason vastuut määritellään hallintosäännössä. Kaupunginhallituksen hyväksymässä tietoturvapolitiikassa määritellään tietoturvan käytännön vastuut ja velvollisuudet.



Kuva:
Tietoturvan ohjaus ja vastuut.

3.1 Kaupunginhallituksen ja kaupunginjohdon vastuut

Oulun 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 tietoturvapolitiikasta. Kaupunginhallitus seuraa tietoturvallisuuden sekä tietosuojan toteutumista kaupungissa ja sillä on vastuu kaupungin sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kaupunginhallitus toimii rekisterinpitäjänä tilanteissa, joissa tieto on käytettävissä useammalla kuin yhdellä kaupungin toimialalla. Rekisterinpitäjä määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään.

Lauta- ja johtokunnat vastaavat toimialueensa tietoturvallisesta toiminnasta ja tietosuojan järjestämisestä ja ovat hallintokunnan henkilötietojen käsittelyssä tietosuoja-asetuksen tarkoittamia rekisterinpitäjiä. Kaupunginhallitus toimii konsernihallinnosta vastaavana toimielimenä ja siihen sovelletaan lautakuntaa koskevia hallintosäännön määräyksiä.

3.2 Konsernihallinnon Digi ja ICT -vastuualueen tehtävät

Tietoturvan ja tietosuojan ohjaaminen sekä tietoturvapolitiikan valmistelu kaupunginhallituksen päätettäväksi kuuluvat Digi ja ICT -vastuualueen tehtäviin. Digitaalisen turvallisuuden tehtäväalue sisältää lisäksi vastuun kyberturvallisuudesta, riskienhallinnasta sekä toiminnan jatkuvuudenhallinnasta ja varautumisesta. Tehtävistä vastaa kaupungin tietoturvapäällikkö, joka toimii myös kaupungin tietosuojavastaavana viranomaisyhteistyössä.

Tietoturvapäällikkö johtaa kaupungin tietoturva- ja tietosuojatoimintaa, tekee kaupunkitasoisia linjauksia ja ohjeistaa henkilöstöä.

Tietoturvapäällikkö toimii mukana kaupungin tiedonhallintatyössä sekä riskienhallinnan ja varautumisen kehittämisessä. Tietoturvapäällikkö toimii objektiivisesti ja riippumattomasti sekä raportoi tietoturvan ja tietosuojan merkittävimmistä riskeistä ja epävarmuustekijöistä kaupungin johto-

ryhmälle kaksi kertaa vuodessa tai tarpeiden mukaisesti. Tehtävään kuuluu lisäksi digitaalisen turvallisuuden tilannekuvan tuottaminen kaupungin johdolle, kaupunginhallitukselle, lautakunnille ja toimialojen johtoryhmille kerran vuodessa tai tarpeiden mukaisesti.

Tietosuojavastaavana tietoturvapäällikkö ohjaa kaupungin tietosuojatyötä ja toimialojen tietosuojavastaavia. Tietosuojavastaava seuraa ja valvoo kaupungin tietojenkäsittelyyn liittyvien toimintatapojen lainsäädännön vastaavuutta. Tietosuojavastaava ei vastaa henkilötietojen käsittelystä, vaan siitä vastaavat aina rekisterinpitäjä ja sen edustaja. Kaupungin tietosuojavastaava toimii yhteyshenkilönä sekä valvontaviranomaisiin että rekisteröityihin.

Digi ja ICT -vastuualue järjestää kaupungin ICT-palvelut ja siten huolehtii kaupungin toimintaympäristön teknisen ja operatiivisen tietoturvallisuuden järjestämisestä. Digi ja ICT -vastuualue vastaa myös toimintaa tukevien tietoturvalinjausten toteuttamisesta.

Digi ja ICT -vastuualue järjestää Oulun kaupungin käyttämät päätelaitteet ja niiden keskitetyn hallinnan. Käytettävät tietojärjestelmät ja sovellukset ovat Digi ja ICT -vastuualueen tai toimialan arvioimia ja hyväksymiä. Tietoturvapäällikkö voi sallia perusteltuja poikkeuksia linjauksiin.

Oulun kaupungin toimintaan kohdentuvissa akuuteissa uhkatilanteissa tai merkittävissä häiriötilanteissa on ryhdyttävä välittömiin turvaamistoimenpiteisiin. Kaupungin toimintaympäristöön kohdentuvissa akuuteissa uhkatilanteissa tai merkittävissä häiriötilanteissa tietohallintojohtajalla, tietoturvapäälliköllä ja ICT-palvelupäälliköllä on oikeus sulkea tietoliikenneyhteys, järjestelmä, käyttäjätunnus tai laite vahinkojen minimoimiseksi.

3.3 Oulun kaupungin tietoturva- ja tietosuojatyöryhmä

Tietoturvapäällikkö toimii tietoturva- ja tietosuojatyöryhmän puheenjohtajana. Työryhmässä seurataan tietoturvan ja tietosuojan yleistä kehittymistä, uhkia ja riskejä sekä arvioidaan henkilötietojen käsittelyn periaatteita ja tietosuojalain velvoitteiden toteutumista. Työryhmä valmistelee kaupunkitasoisia ja toimialakohtaisia linjauksia, ohjeistuksia ja toimintamalleja. Työryhmä suunnittelee koulutuksia,

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

3.4 Toimialojen, liikelaitosten ja tytäryhteisöjen vastuut

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

Toimialojen, liikelaitosten ja tytäryhteisöjen johtajat vastaavat riskienhallinnasta, varautumisesta ja tietoturvan ja tietosuojan toteutumisesta sekä linjausten noudattamisesta toiminnassaan.

Johtajien ja nimettyjen vastuuhenkilöiden tulee tuntea toimialansa erityispiirteet ja lainsäädäntö sekä selventää tietoturva- ja tietosuojavastuut ja ICT-varautuminen osana kokonaisvaltaista johtamista.

Toimialojen edustajat huolehtivat vastuullaan olevien tietojärjestelmien ja sovellusten tietoturvallisuudesta ja asetettujen tietoturva- ja tietosuojavaatimusten toteuttamisesta. Määritelty tietoturvataso vaaditaan myös ICT-palveluiden toimittajilta ja palveluiden tuottajilta läpi koko toimintaketjun. Uusia palveluita suunniteltaessa tai merkittävissä toimintaympäristössä tapahtuvissa muutoksissa tulee huomioida lakisääteinen velvoite tehdä muutosvaikutusten arviointi (Laki julkisen hallinnon tiedonhallinnasta 906/2019) ja huolehtia rekisterinpitäjän informoinnista. Tietoturvapäällikkö ja toimialojen tietosuojavastaavat ohjeistavat rekisterinpitäjää toimimaan lainsäädännön ja kaupungin linjausten mukaisesti.

3.5 Hallintokuntien tietoturva- ja tietosuojavastaavat

Hallintokunnat nimeävät yhden tai useamman tietoturva- tai tietosuojavastaavan, joka toimii yhteyshenkilönä kaupungin tietoturvapäällikköön/tietosuojavastaavaan. Vastuuhenkilön tehtävä on kehittää oman toimialueen henkilöstön osaamista tietoturva- ja tietosuoja-asioissa sekä parhaiden käytäntöjen omaksumista päivittäisissä työtehtävissä. Lisäksi tehtävänä on valvoa tietoturvan ja tietosuojan toteuttamista ja ohjeiden noudattamista.

Tietosuojavastaavat toimivat rekisterinpitäjän tukena ja auttavat lakisääteisten velvoitteiden toteuttamisessa.

Tietoturvavastaavat huolehtivat toimialojensa tietoturvan toteutumisesta tietoturvapäällikön ohjauksessa. Vastuuhenkilöt suorittavat käytönvalvontaa, tarkastavat toimintatapoja ja suorittavat auditointeja. He valvovat tietoturvapolitiikan ja tietoturvaohjeiden noudattamista sekä osallistuvat väärinkäytösepäilyiden selvittämiseen. Vastuuhenkilöt raportoivat tietoturva- ja tietosuojapoikkeamista johdolle, rekisterinpitäjälle, esimiehelle ja tietoturvapäällikölle ohjeiden mukaisesti.

Tietosuojavastaava on henkilötietojen käsittelyä koskevan lainsäädännön erityisasiantuntija, joka toimii johdon, rekisterinpitäjän ja henkilöstön tukena henkilötietojen käsittelyn hallinnassa ja suunnittelussa. Tietosuojavastaavat toimivat objektiivisesti ja riippumattomasti. Tietosuojavastaavat seuraavat vastuualueen henkilötietojen käsittelyn ja tietosuojaperiaatteiden noudattamista käytännössä, suojellen rekisteröityjen oikeuksia ja vapauksia. Tietosuojavastaavat huomioivat vastuualueidensa erityislainsäädännön ja -tarpeet. He tukevat ohjaamalla ja kouluttamalla organisaation tietosuojan kehittämistä ja tavoitteiden saavuttamista. Tietosuojavastaavat eivät vastaa toimialan henkilötietojen käsittelystä. Henkilötietojen käsittelystä vastaavat aina rekisterinpitäjä ja sen edustaja.

Tietosuojavastaavat huolehtivat rekisteröityjen informoinnista ja tukevat toimialojen tietosuojasitoumusten ja -sopimusten tekemistä palveluntuottajien kanssa sekä lakisääteisten vaikutustenarviointien toteuttamista. Tietosuojavastaavat ovat mukana toimialakohtaisten henkilötietojen käsittelyn suunnittelussa ja kaupunkitasoisten hallintamallien kehittämisessä sekä linjausten ja ohjeistuksien valmistelussa, ja seuraavat lainsäädännön ajantasaisuutta.

3.6 Esihenkilön tietoturvavastuut

Esihenkilö vastaa tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan. Esihenkilön vastuulla on huolehtia ja noudattaa toimialaa koskevien lakisääteisten tietoturva- ja tietosuojakäytänteiden toteutumisesta sekä huolehtia työntekijän

riittävästä perehdytyksestä ja säännöllisestä koulutuksesta kaupungin tietoturvakäytänteisiin.

Esihenkilöiden tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita.

Esihenkilön tulee varmistaa, että jokainen työntekijä ymmärtää oman tietoturva- ja tietosuojavastuun toiminnassaan ja käsittelee tietoja oikeaoppisesti ja tarkoituksenmukaisesti sekä ymmärtää, että väärinkäytöksillä on rikosoikeudellinen luonne. Työntekijältä voi tarkistaa kehityskeskusteluissa, onko hän suorittanut tietoturva- ja tietosuojakoulutuksen ja perehtynyt työtehtäviensä laajuudessa riittävästi tietoturva- ja tietosuojakäytänteisiin.

Esihenkilön ja tietojärjestelmien pääkäyttäjien vastuulla on huolehtia työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa. 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 kaiken työnantajalle kuuluvan tiedon ja käyttöoikeudet tietojärjestelmistä poistetaan. Esihenkilö varmistaa työ- ja palvelusuhteen tai harjoitteluajan päättymisen yhteydessä, että henkilö on tietoinen vaitiolovelvollisuuden jatkumisesta myös työ- ja palvelusuhteen sekä harjoitteluajan päättymisen jälkeen. Esihenkilöiltä odotetaan esimerkillistä sekä vastuullista tietoturvakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvapoikkeamista omalle esihenkilölle ja tietosuojavastaavalle tai tietoturvapäällikölle.

3.7 Työntekijöiden tietoturvavastuut

Oulun kaupungin työntekijä sitoutuu työsuhteen perustamisen yhteydessä noudattamaan työnantajan sääntöjä ja ohjeita. Työntekijällä on velvollisuus allekirjoittaa tietoturva- ja käyttäjäsitoumus sekä suorittaa säännöllisesti kulloinkin voimassa oleva tietoturva- ja tietosuojakoulutus. Tietoturva- ja tietosuojakoulutuksia voidaan järjestää toimialoille myös kohdennettujen tarpeiden mukaisesti.

Jokaisella työntekijällä on vastuu noudattaa kaupungin tietoturva- ja tietosuojaohjeita sekä huolehtia päivittäisissä työtehtävissä tietojen oikeaoppisesta ja tarkoituksenmukaisesta käsittelystä.

Tavoitteena on, että työntekijä tunnistaa tietojenkäsittelyssä oman oikeusturvansa ja ymmärtää, että väärinkäytöksillä voi olla rikosoikeudelliset seuraukset. Tietoturvaan ja tietosuojaan liittyvissä asioissa jokainen työntekijä on vastuussa riskeistä, jotka liittyvät hänen päätöksentekovaltaansa tai päätöksiin.

Käyttöoikeudet ovat henkilökohtaiset eikä niitä saa luovuttaa kenellekään.

Työntekijän vastuulla on huolehtia käsittelemänsä tiedon oikeellisuudesta, merkinnöistä, saatavuudesta ja luokittelusta sekä huolehtia, että organisaation tietoja käsitellään tietoturva- ja tietosuojakäytänteiden mukaisesti. Tietojen säilytysajan päätyttyä viranomaisen asiakirjat hävitetään käyttöön hyväksytyn tiedonohjaussuunnitelman mukaisesti. Työntekijällä on velvollisuus luovuttaa työsuhteen muutoksissa tai päättyessä kaikki työnantajalle kuuluva tieto. Muiden tietojen siirrosta tai hävittämisestä tulee sopia esihenkilön kanssa ennen työsuhteen päättymistä. Työntekijällä on velvollisuus ilmoittaa tietoturvaan ja tietosuojaan kohdentuvista poikkeamista, puutteista, uhkista ja riskeistä välittömästi omalle esihenkilölle ja tietosuojavastaavalle tai tietoturvapäällikölle.

3.8 Tiedonhallinnan vastuut

Oulun kaupunki on yksi tiedonhallintayksikkö ja kaupunginhallitus vastaa siitä, että tiedonhallinnan vastuut, käytännöt ja valvonta on määritelty viranomaisen tai vastuuhenkilön tehtävissä.

Tiedonhallintayksikkö ylläpitää ja kehittää digitaalisen turvallisuuden ja tiedonhallinnan hallintamallia, johon on määritelty vastuut toimintaprosessi-, tietovaranto- ja tietojärjestelmäkohtaisesti.

Hallintamallia ylläpidetään ja päivitetään tiedonhallinnan vuosikellon mukaisesti, digitaalisen turvallisuuden ja tiedonhallintatyön hallintajärjestelmällä.

Digitaalisen turvallisuuden ja tiedonhallintatyön hallintajärjestel-

mään tallennetuista, jatkuvasti päivittyvistä tiedoista tuotetaan tiedonhallintalain edellyttämät tiedonhallinnan kuvaukset: tiedonhallintamalli ja asiakirjajulkisuuskuvaus. Vastuu kuvausten sisällöstä on tiedon omistajalla. Kuvausten ylläpitäminen edellyttää poikkihallinnollista ja moniammatillista asiantuntemusta.

Oulun kaupungin jokaiselle tietojärjestelmälle ja tietovarannolle nimetään omistaja. Omistajalla on vastuu tietojärjestelmän toimintavarmuudesta, dokumentoinnista ja riskienhallinnasta, mikä pitää huomioida myös palvelu- ja alihankintasopimuksissa. Omistaja vastaa:

- Tietojärjestelmän yhteentoimivuudesta sekä tietoturvan, tietosuojan, varautumisen ja jatkuvuudenhallinnan toteutumisesta.
- Tietovarantojen yhteentoimivuudesta sekä tietojenkäsittelyn oikeellisuudesta, luottamuksellisuudesta ja käyttövaltuuksien hallinnasta.
- Tietoaineistojen käsittelyn lainmukaisuudesta, tietoaineistojen muuttumattomuudesta, alkuperäisyydestä, ajantasaisuudesta, virheettömyydestä ja arkistoitavuudesta yhteistyössä konsernihallinnon asianhallintayksikön kanssa.

Tietojärjestelmät ja tietovarannot luokitellaan käsiteltävien tietojen kriittisyyden, tunnistettujen tietoturvariskien ja kokonaisarkkitehtuurin mukaisesti. Riskitekijät ja häiriötilanteiden toimintamallit selvitetään yhteistyössä konsernihallinnon Digi ja ICT -vastuualueen palveluvastaavan, digiasiantuntijan, tietosuojavastaavan, tietoturvapäällikön tai palvelu- ja järjestelmätoimittajan kanssa.

Käyttäjille annetaan tietoturva- ja tietosuojaohjeet ja huolehditaan, että työntekijät saavat niihin riittävän koulutuksen.

Tiedonhallintaan liittyvät roolit vastuineen:

Rekisterinpitäjä

Vastaa henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä vastaa sisäänrakennetun ja oletusarvoisen tietoturvan ja tietosuojan toteutumisesta, mikä sisältää tarvittavat tekniset ja organisatoriset toimenpiteet. Rekisterinpitäjä vastaa tiedon käsittelystä, luovuttamisesta, säilyttämisestä ja hävittämisestä noudattaen kulloinkin voimassa olevien lainsäädännön vaateita huomioiden erityisesti tiedon käsittely ja tallennuspaikat. Rekisterinpitäjä huolehtii osoitusvelvollisuuden toteutumisesta, käsittelytoimien kuvauksista, toiminnan riippuvuuksien tunnistamisesta, rekisteröityjen informoinnista ja oikeuksista. Rekisterinpitäjällä on velvollisuus tehdä tietosuojan vaikutustenarviointi, kun uutta teknologiaa otetaan käyttöön, käsitellään arkaluonteisia tai muutoin hyvin henkilökohtaisia tietoja tai henkilötietoja käsitellään laajamittaisesti (Tietosuojalaki 1050/2018 ja EU:n yleinen tietosuoja-asetus 679/2016).

Tiedon, palvelun tai prosessin omistaja

Vastuu tiedon elinkaaren hallinnasta, luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön. Vastaa palvelun riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Pääkäyttäjä

Tietojärjestelmän omistajan nimeämä henkilö, jonka vastuulla on huolehtia järjestelmän käyttövaltuuksista. Pääkäyttäjältä vaaditaan hyvää tietoturva- ja tietosuojaosaamista. Lisäksi tiedon omistaja ja pääkäyttäjä huolehtivat tiedon koko elinkaaren hallinnasta ja ovat mukana ICT-varautumissuunnitelmien laadinnassa, missä kuvataan vastuuhenkilöt, roolit ja toimintamallit riskien arvioinnin perusteella.

Rekisterinpitäjän edustaja

Rekisteröityjen informointi vastuualueen rekisterin osalta. Rekisteröity voi kääntyä edustajan puoleen saadakseen tarkempia tietoja rekisteristä tai omista oikeuksistaan. Vastuuhenkilöiden lisäksi on oltava riittävästi avustavaa henkilökuntaa, joka osallistuu erityisesti rekisteröityjen tekemiin tiedusteluihin vastaamiseen.

Palveluvastaava tai digiasiantuntija

Konsernihallinnon Digi ja ICT-vastuualueen asiantuntija, joka huolehtii tai järjestää järjestelmien teknisen ylläpidon ja tietojen siirron sekä yhteydenpidon toimittajan kanssa sekä muut seikat siinä laajuudessa kuin järjestelmän omistajan ja pääkäyttäjän kanssa on tehtävienjaosta sovittu.

3.9 Palvelujen ja hankintojen tietoturvavastuut

Uusia järjestelmiä hankittaessa tai palveluita suunniteltaessa omistaja tai tilaaja huolehtii, että hankinnassa huomioidaan tiedonhallintalain ja toiminnan vaatimukset tietoturvallisuudesta, tietosuojasta, varautumisesta ja jatkuvuudesta, lokitietojen keräämisestä ja mahdollisesta tiedon siirtämiseen liittyvistä rajapinnoista. Uutta järjestelmää hankittaessa arvioidaan, käytetäänkö järjestelmää tai palvelua asiankäsittelyyn tai palveluiden tiedonhallintaan tai molempiin. Arvioinnin perusteella hankinnassa huomioidaan asianmukaiset tiedonhallintalain vaatimukset. Jos hankittava järjestelmä sisältää asiankäsittelyä, siitä tulee osa tiedonhallintayksikön asiarekisteriä. Uutta järjestelmää hankittaessa tulee myös huolehtia käytöstä poistuvan järjestelmän tietoaineiston käyttö- ja säilytystarpeesta.

Merkittävissä uusissa tietojärjestelmähankinnoissa tai hallinnollisissa muutoksissa tehdään omistajan toimesta tiedonhallinnan muutosvaikutusten arviointi (Laki julkisen hallinnon tiedonhallinnasta 906/2019), jossa 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 on sovittava esimerkiksi RACI-mallilla. Palvelun tuottaja nimeää tietoturvan ja tietosuojan yhteyshenkilöt, joiden tehtävä on huolehtia sovitun tietoturva- ja tietosuojatason noudattamisesta sekä raportoida viipymättä tietoturvapoikkeamista tai henkilötietoihin kohdentuneista tietoturvaloukkauksista palvelusopimuksessa määritellyille Oulun kaupungin yhteyshenkilöille ja tietoturvapäällikölle.

Palvelun tilaajan tulee huolehtia, että tarjouspyyntöihin ja palvelusopimuksiin sisällytetään Oulun kaupungin tietoturvan ja tietosuojan vaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla. Tarkoitukseen on saatavissa pohjadokumentteja intranetista tai tietosuojavastaavilta ja tietoturvapäälliköltä.

On ensiarvoisen tärkeä huolehtia jo olemassa olevan tai hankittavan palvelun tai ratkaisun sisäänrakennetun oletusarvoisen tietoturvan toteuttamisesta.

Sopimuksissa tulee huomoidan lainsäädännön velvoitteet, häiriö- ja poikkeustilanteiden toimintamallit ja selkeä toiminnallinen vastuunjako läpi koko palveluketjun.

4. Digitaalisen turvallisuuden seuranta ja tilannekuva

Digitaalisen turvallisuuden hallintaa kehitetään ja arvioidaan säännöllisesti tiedonhallinnan vuosikellon mukaisesti. Tietoturvapolitiikan ja muiden ohjeiden noudattaminen, seuranta ja niistä raportointi on tärkeä osa kaupunkikonsernin sisäistä valvontaa, toiminnan laatua ja riskienhallintaa.

Digitaalisen turvallisuuden tilannekuva muodostetaan hallintokuntien ja tytäryhteisöiden tietoturva- ja tietosuojavastaavien sekä ICT-palveluntuottajien raportoinnin perusteella. Tilannekuvan muodostamisessa hyödynnetään myös kansallisia ja kansainvälisiä tietoturvaverkostoja.

Konsernihallinnon Digi ja ICT -vastuualue ja tietoturvapäällikkö laativat kokonaisuudesta digitaalisen turvallisuuden tilannekuvan ja raportoivat siitä kaupungin johdolle ja päätöksentekoelimille.

Raportointitietojen ja tilannekuvan perusteella tehdään tarvittaessa kehitystoimenpiteitä, kohdennettuja arviointeja tai auditointeja.

4.1 Tietoturva-arvioinnit

Tietoturvatason arvioinnit ja auditoinnit ovat osa digitaalisen turvallisuuden hallintaa. Toimenpiteiden tavoitteena on todentaa, miten tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta on huolehdittu. Arvioinnit tuottavat järjestelmällistä tilannetietoa, jonka avulla pyritään tunnistamaan tietoturvaan kohdentuvia uhkia ja haavoittuvuuksia. Arviointien tavoitteena on varmistaa palveluiden jatkuvuus ja toiminnan laatu. Arviointeja voidaan kohdentaa myös ICT-palvelutuottajiin, joka huomioidaan kaupungin ja palvelutoimittajan välisissä sopimuksissa. Arviointikohteet priorisoidaan kriittisyyden perusteella ja käsitellään Digi ja ICT -vastuualueella ja kohdealueella.

4.2 Digitaalisen turvallisuuden tavoitteet

Tietoturvan kehittämisen tavoitteet tarkennetaan vähintäänkin vuosittain johtamalla kehittämistoimenpiteet tietoturvapolitiikan tavoitteista ja toimintaympäristön vaatimuksista (Taulukko 1). Konsernihallinnon Digi ja ICT -vastuualue seuraa tietoturvalle asetettujen tavoitteiden toteutumista osana toimintaansa ja raportoi niistä osana talousarvioprosessia.

Taulukko 1. Digitaalisen turvallisuuden hallinnan tavoitteet ja toimenpiteet

Strateginen tavoite	Tavoite	Toimenpiteet
Tietoturvaan kohdistuvien uhkatekijöiden tunnistaminen	• Digitaalisen turvallisuuden johtaminen ja varautuminen on suunnitelmallista • Vakavien uhkatekijöiden tunnistaminen, hallinta ja toimenpiteet on suunniteltu	• Digitaalisen turvallisuuden tilannekuvan ylläpitämisen ja raportoinnin jatkuva kehittäminen • Digitaalisen turvallisuuden hallintamallin jatkuva kehittäminen • ICT-riskienhallinnan ja varautumisen jatkuva kehittäminen
Palveluiden jatkuvuuden ja tietojen turvaaminen	• ICT-infrastruktuurin ja digitaalisen toimintaympäristön luotettava toiminta • Häiriö- ja poikkeustilanteiden hallinta on hyvällä tasolla • ICT-monitoimittajaympäristössä on sovittu selkeät vastuunjaot	• Häiriötilanteiden ja tietoturvapoikkeamien hallintamallit • Varautumis-, toipumis- ja viestintäsuunnitelmat • Tietojen ja tietojärjestelmien kriittisyysluokittelu • Sisäisten roolien selkeät mallit: Digi Turjo, OUKA-turvallisuusjohtaminen ja varautuminen • Palvelusopimukset ja vastuidenjako kunnossa (RACI)
Henkilöstön tietoturvaosaamisen kehittäminen	• Tietoturvatietoisuuden lisääminen • Positiivisen ja kannustavan tietoturvakulttuurin luominen • Työntekijät noudattavat tietoturvapolitiikkaa ja toimivat vastuullisesti tietoturvallisilla toimintatavoilla	• Säännöllinen kouluttaminen, tiedottaminen ja ohjaaminen tietoturva- ja tietosuojakäytänteisiin • Positiivisen ja vastuullisen tietoturvakäyttäytymisen tukeminen ja yhteisen ymmärryksen lisääminen

Strateginen tavoite	Tavoite	Toimenpiteet
Tietoturvan varmistaminen läpi toimintaketjujen	• Tietoturva ja tietosuoja otetaan huomioon hankinnoissa, palveluostoissa ja kumppanuuksissa • Häiriötilanteiden hallinta, varautuminen ja jatkuvuus • Sopimukset ja vastuidenjako on kunnossa (RACI)	• Hankintadokumentaation kehittäminen ja ylläpito • Muutosvaikutusten arviointi • Tietosuojan vaikutustenarviointi • Tietoturva- ja tietosuojatarkastukset ja auditoinnit • Palvelutasojen ja sopimusten arviointi ja toteutuminen
Tietoturva toiminnan kehittämisen mahdollistajana	• Digitaalista toimintaympäristöä kehitetään tietoturvallisuus ja lainsäädännön velvoitteet huomioiden • Tietoturvaratkaisut ovat luotettavia ja palvelutoimintaa tukevia	• Digikehittämisessä oikea-aikainen suunnittelun tuki ja vaikutusten arviointi • Tietoturvan kypsyys huomioidaan osana kokonaisarkkitehtuuria
Kansallisten suositusten mukainen toiminta	• Oulun kaupungin digitaalisen turvallisuuden taso on kansallisesti hyvällä tasolla • Aktiivinen osallistuminen ja verkostoituminen digitaalisen turvallisuuden kehittämiseen yhteiskunnassa	• Digitaalisen turvallisuuden tilannekuvan tuottaminen ja säännöllinen raportointi • Toiminnan jatkuva kehittäminen ja arviointi sekä voimassa olevien tietoturvavelvoitteiden noudattaminen

5. Normaaliolojen häiriötilanteisiin varautuminen

5.1 Häiriötilanteiden toimintamalli

Oulun kaupunki varautuu turvaamaan ensisijaisesti kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä valmiussuunnitelmia ja harjoittelemalla säännöllisesti. Tavoitteena on varautua toiminnan häiriöitilanteisiin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti rajoittamalla haittavaikutuksia ja toipua tilanteesta mahdollisimman nopeasti.

Oulun kaupungin toimintaympäristöön kohdentuvissa tietoturvaloukkauksissa tai muissa tietoturvaa kohdentuvissa uhkatilanteissa vastatoimenpiteet on aloitettava välittömästi ja niistä on raportoitava ensi tilassa tietoturvapäällikölle.

Kaupungin toimintaympäristöön kohdentuvissa akuuteissa uhkatilanteissa tai merkittävissä häiriötilanteissa (Major Incident Management) tietohallintojohtajalla, tietoturvapäälliköllä ja ICT-palvelupäälliköllä on oikeus sulkea tietoliikenneyhteys, järjestelmä, käyttäjätunnus tai laite vahinkojen minimoimiseksi.

Turvaamistoimenpiteiden järjestys ja priorisointi uhkatilanteissa on: hengen tai terveyden turvaaminen, arkaluonteisen tai muuten salassa pidettävän tai erittäin merkittävän tiedon turvaaminen, tietojärjestelmien ja henkilörekistereiden eheyden turvaaminen, käyttö- ja toimintaympäristön saatavuuden turvaaminen. Häiriötilanteiden toimintamalli etenee kaupungin turvallisuusjohtamisen hallintamallin mukaisesti. Suoritetuista toimenpiteistä ja mahdollisista jatkotoimenpiteistä informoidaan turvallisuusjohtamisen käytänteiden mukaisesti.

Konsernihallinnon Digi ja ICT -vastuualueella toimiva turvallisuusjohtamisen tiimi (Digi Turjo) päättää, kuinka kaupunkiin kohdentuviin digitaalisen turvallisuuden uhkatilanteisiin reagoidaan ja mitä toimenpiteitä käynnistetään, jotta vakavien haittatekijöiden syntyminen estetään tai minimoidaan. Tiimi toimii uhkatilanteissa päätösvaltaisesti arvioiden ja raportoiden häiriötilanteen toimenpiteistä.

5.2 Tietoturva-asioista tiedottaminen

Oulun kaupungin sisäisestä tietoturvatiedottamisesta ja ICT-palvelutuotannon häiriötilanteiden tiedottamisesta vastaa Digi ja ICT -vastuualue. Tiedottamista hoitaa tietoturvapäällikkö ja ICT-palvelupäällikkö yhteistyössä tietoturvan ja tietosuojan vastuuhenkilöiden ja kaupungin viestinnän kanssa, tarvittaessa myös ICT-palveluntuottajan kanssa. Yleisistä informatiivisista asioista tiedotetaan säännöllisesti ja tietoturvapoikkeamista tarpeiden mukaisesti. ICT-palvelutuotannon häiriötilanteista (esim. käyttökatkot) tiedottaminen on ICT-palveluntuottajan tai tietojärjestelmän omistajan tai sen sopimuksin valtuuttaman tahon vastuulla. Kaupungin hallintokunnat ja tytäryhteisöt vastaavat omalla toimialallaan tiedottamisesta tai tiedon välittämisestä.

Ulkoisesta tietoturvatiedottamisesta vastaavat tietohallintojohtaja, tietoturvapäällikkö tai ICT-palvelupäällikkö yhteistyössä kaupungin viestinnän kanssa.

Vakavissa Oulun kaupunkia koskevissa häiriö- tai poikkeustilanteissa tiedottaminen tapahtuu turvallisuusjohtamisen käytänteiden mukaisesti.


OULU