



TIETOTILINPÄÄTÖS

2025

Sisällys

Tiivistelmä.....	4
1 Yleiskatsaus	5
1.1 Tietotilinpäätöksen tarkoitus	5
1.2 Merkittävimmät muutokset ja tapahtumat vuonna 2025	5
2 Tietosuojan ja tietoturvallisuuden toteuttaminen.....	7
2.1 Kaupungin hallinnollinen organisaatio	7
2.2 Tietohallinnon organisointi	8
2.3 Tietoturvan ja tietosuojan organisointi.....	8
2.4 Tekniset ja organisatoriset toimenpiteet	11
2.5 Riskienhallinta.....	12
2.6 Tarkastukset	13
2.7 Tietoturvapoikkeamien käsittely.....	14
3 Tiedonhallinta, tietovarannot ja tietovirrat.....	14
3.1 Tiedonhallinnan organisointi	14
3.2 Tiedonhallinnan ohjaus	15
3.3 Tiedon elinkaaren hallinta.....	15
3.4 Tietovarannot.....	16
3.5 Asianhallinta ja sähköinen asiointi.....	16
3.6 Asiakirjahallinto ja arkistotoimi.....	16
4 Lainsäädäntö ja linjaukset.....	16
4.1 Lainsäädäntö	16
4.2 Poliitikat ja kaupungin säännöstö	16
5 Koulutus, ohjeistus ja harjoitukset	17
5.1 Koulutus.....	17
5.2 Ohjeistus.....	17
5.3 Harjoitukset.....	17

6 Rekisteröidyn oikeuksien toteutuminen	18
6.1 Tietosuojaa koskevat periaatteet	18
6.2 Rekisteröityjen informointi asiointipalveluissa	18
6.3 Selosteet ja niiden ajantasaisuus	18
7 Kehittäminen ja tiedon hyödyntäminen	19
7.1 Tiedonhallinta ja kokonaisarkkitehtuuryö, tiedon hyödyntämisen kehittäminen ..	19
7.2 Tietojärjestelmien kehittäminen, hankinta ja ylläpito	19
7.3 Tietoturvallisuuden ja tietosuojan kehittäminen	19
8 Seuranta ja mittarit	20
8.1 Toimintaympäristö	20
8.2 Tietovarannot	20
8.3 Riskit, vaikutustenarvioinnit ja turvallisuusselvitykset	21
8.4 Tietopyynnöt ja rekisteröityjen oikeuksien käyttö	21
8.5 Tietoturvapoikkeaminen käsittely	22
8.6 Tarkastukset	22
8.7 Tietoturva- ja tietosuojakoulutukset	22
9 Todennetut merkittävimmät kehityskohteet tulevalle vuodelle	22
9.1 Asianhallintajärjestelmän kilpailutus ja käyttöönotto	22
9.2 Tekoälyn käyttöönoton jatkaminen	23
9.3 Tiedolla johtaminen	23
9.4 Tietoturva- ja tietosuojatyön resurssointi	23
9.5 Suomi.fi Viestit -palvelun käyttöönotto	24
9.6 ICT-palveluiden uudelleenjärjestämisen selvitys	25

Tiivistelmä

Tietotilinpäätös tarjoaa katsauksen Rovaniemen kaupungin vuoden 2025 tiedonhallinnan, tietoturvan ja tietosuojan tilasta. Tietotilinpäätös toimii myös osana EU:n yleisen tietosuoja-asetuksen määrittelemää osoitusvelvollisuutta.

Rovaniemen kaupungin organisaation tietosuojan ja tietoturvan tila on kehittynyt merkittävästi EU:n tietosuoja-asetuksen voimaantulon jälkeen. Asetus on edellyttänyt olemassa olevien käytäntöjen tarkastelua, ja ohjeistusten päivittämistä sekä tuonut uusia näkökulmia henkilötietojen käsittelyyn. Tietosuojatietoisuus on lisääntynyt, ja asenne tietosuojaa kohtaan on kehittynyt myönteisesti. Tietosuojatyö kehittyy jatkuvasti sekä organisaation ulkopuolelta tulevien vaatimusten että sisäisten, organisatoristen muutosten vaikutuksesta.

Tietosuoja koskee koko henkilöstöä ja on olennainen osa jokaisen työntekijän päivittäistä työtä. Jokaisen työntekijän tulee tuntea omaa työtään koskevat tietosuoja-vaatimukset ja ymmärtää niiden vaikutus työarkeen. Henkilöstön tietosuojatietoisuutta vahvistetaan perehdyttämällä uudet työntekijät sekä tarjoamalla jatkuvaa koulutusta. Digitaalisten palvelujen määrän kasvaessa henkilöstöltä edellytetään osaamisen jatkuvaa ylläpitämistä ja organisaatiolta kykyä seurata kehitystä. Tämä edellyttää järjestelmällistä havainnointia ja seurantaa tietoturvan ja tietosuojan eri osa-alueilla, jotta toiminta ja toimintatavat pysyvät tietoturvallisina.

Tietotilinpäätöksen laatimisesta on vastannut tietoturva- ja tietosuojatyöryhmä yhteistyössä tietosuojavastaavan kanssa. Tietotilinpäätös käsitellään vuosittain tietoturva- ja tietosuojatyöryhmässä, kaupungin johtoryhmässä sekä kaupunginhallituksessa, ja se saatetaan tiedoksi kaupunginvaltuustolle.

Tietotilinpäätöksen tarkoituksena on kuvata, miten tietoturva ja tietosuoja ovat toteutuneet Rovaniemen kaupungissa vuonna 2025. Lisäksi siinä esitetään keskeiset kehittämistarpeet ja suunnitelmat vuodelle 2026. Tietotilinpäätöksessä tarkastellaan ajankohtaisia tietoturvaan ja tietosuojaan liittyviä teemoja sekä arvioidaan muutoksia edelliseen tietotilinpäätökseen verrattuna. Tietotilinpäätös on julkinen asiakirja ja kokonaisuudessaan luettavissa kaupungin verkkosivuilla.

1 Yleiskatsaus

1.1 Tietotilinpäätöksen tarkoitus

Tietotilinpäätöksen tarkoituksena on antaa yleiskuva kaupungin tiedonhallinnan sekä tietoturvan ja tietosuojan tilasta. Sen tavoitteena on edistää luottamusta ja tukea hyvää tiedolla johtamista. Tietotilinpäätöksen sisältö kokoaa yhteen keskeiset havainnot, toteutetut toimenpiteet sekä tulevien vuosien kehittämistarpeet tietosuojan, tietoturvan, riskienhallinnan, tiedonhallinnan, tietovarantojen ja arkistotoimen osalta.

Julkaistavan tietotilinpäätöksen tavoitteena on lisätä johdon, luottamushenkilöiden, henkilöstön, kuntalaisten ja muiden sidosryhmien tietoisuutta tietosuojasta ja tietoturvasta sekä tuoda näkyväksi Rovaniemen kaupungissa näiden teemojen eteen tehtyä työtä ja toteutettuja toimenpiteitä.

Tietotilinpäätöksessä kuvataan, miten tietosuoja ja tietoturva ovat toteutuneet Rovaniemen kaupungin toiminnassa ajanjaksolla 1.1.–31.12.2025.

1.2 Merkittävimmät muutokset ja tapahtumat vuonna 2025

Siirtyminen M365-järjestelmään ja tekniset tietosuojaratkaisut

Vuonna 2024 Rovaniemen kaupunki siirtyi digitaalisissa työskentelyalustoissa Google Workspacen palveluista Microsoftin M365 palveluun. Siirtymisen yhteydessä tietoturvan ja tietosuojan näkökulmasta otettiin käyttöön M365-lisenssipalveluun kuuluva Purview-tekniinen valvontatyökalu. Purview mahdollistaa dokumenttien ja tiedostojen automaattisen luokittelun ja leimauksen, mikä parantaa tietojen käsittelyn laatua ja varmistaa tietosuojavaatimusten toteutumisen.

Taloushallintopalveluiden siirto

Rovaniemen kaupungin kirjanpito-, reskontrat ym. taloushallintopalvelut ovat olleet ulkoistettuna Numeran Palvelut Oy:lle (ent. Sarastia Oy, ent. Taitoa Oy). Kaupunginhallitus on päätöksellään 17.12.2024 §342 päättänyt irtisanoa sopimuksen Numeran kanssa talouspalveluiden osalta 31.5.2026 ja toteuttaa talouspalvelut omana toimintana 1.1.2026.

Järjestelmähankinta on toteutettu talous- ja rahoituspalveluiden toimesta alkuvuonna 2025. Uuden tietojärjestelmän käyttöönotto alkoi 6/2025 ja ensimmäiset osat olivat tuotannossa 1.1.2026 alkaen. Käyttöönottoprojekti jatkuu taloussuunnittelun ja konsernikirjanpidon osioilla vuonna 2026. Sarastian palveluista luovutaan taloushallinnossa kokonaan vuoden 2026 aikana, ja tiedot Sarastian käyttämistä järjestelmistä konvertoidaan arkistoon.

TE-palveluiden siirto

TE-palvelut siirtyivät valtiolta kuntien vastuulle ja Rovaseudun työllisyysalue aloitti toimintansa 1.1.2025. Tietoturva ja tietosuoja ovat olleet keskeisessä roolissa, ja se on otettu huomioon sekä työntekijä- että organisaatiotasolla. Organisaatiotasolla tämä on tarkoittanut järjestelmien ja toimintojen suunnittelemista niin, että työnhakija- että yritysasiakkaiden tietoja käsitellään huolellisesti ja sähköiset järjestelmät ovat suojattuja. Palveluiden tasolla tehdään vaikutustenarvioita riskien havaitsemiseksi,

näin minimoidaan mahdollisuus tietoturva- ja tietosuojaloukkauksiin. Mahdollisiin tietoturva- ja tietosuojaloukkauksiin reagoidaan kaupungin ohjeiden mukaisesti.

Työllisyyspalveluiden esihenkilöt seuraavat, että jokainen työntekijä suorittaa pakollisen tietoturva- ja tietosuojakoulutuksen ja lisäksi asiaa käsitellään perehdytyksissä. Jokainen on ollut velvollinen ottamaan käyttöön myös kaksivaiheisen tunnistautumisen kaupungin ohjeen mukaisesti.

Suostumus-käytäntöjä on tarkennettu ja hankittuihin järjestelmiin on tehty vaikutustenarviointeja. Asiakastyö ja siihen liittyvä tiedonvaihto perustuu ensisijaisesti lakiin, tietojen vaihdossa voidaan tarvittaessa käyttää valmiita suostumuslomakkeita, jolloin toiminta on asiakkaalle läpinäkyvää ja turvallista.

Kuntatietojärjestelmän kilpailutus

Kaupungin nykyinen Trimble Locus kuntatietojärjestelmä kilpailutettiin vuoden 2024 aikana. Kilpailutuksen voitti Trimble Locus SaaS -palvelu ja sen käyttöönotto alkoi ensimmäisen moduulin osalta lokakuussa 2025. Kokonaisuudessa järjestelmän käyttö aloitettiin joulukuussa.

Henkilöstöhallinnon älykkäät lomakkeet

Vuoden 2025 aikana otettiin henkilöstöhallinnon järjestelmässä Personec ESS:ssä käyttöön älykkäät lomakepohjat poissaolo- ja koulutusilmoituksiin sekä työsopimusten ja virkamääräysten laadintaan. Älykkäät lomakepohjat ohjaavat käyttäjää lomakkeen täyttämässä ja täyttävät eräitä tietokenttiä valmiiksi edellisten valintojen perusteella. Tämä helpottaa käyttäjän työtä, ja toisaalta vähentää myös manuaalisten- tai asiavirheiden todennäköisyyttä.

Tekoälyratkaisut

Kaupunki otti vuoden 2025 aikana hallitusti käyttöön tekoälyjärjestelmiä toiminnan tehostamiseksi ja resurssien paremmaksi hyödyntämiseksi. Käyttöönotto edellytti uudenlaista osaamista, ulkopuolisten asiantuntijoiden hyödyntämistä sekä henkilöstön kouluttamista. Tekoälyn käyttöönotto tehtiin vastuullisesti ja lainsäädäntö huomioiden.

Tekoälyn käyttöönoton pohjana toimi kaupunginhallituksen vuonna 2025 hyväksymä tekoälypolitiikka, joka määritteli periaatteet, vastuut ja tavoitteet sekä toimi perustana tarkentaville ohjeille. Tavoitteena oli toiminnan tehostaminen ja resurssien järkevä käyttö. EU:n tekoälyasetuksen edellyttämänä kaupunki kehitti henkilöstön tekoälylukutaitoa koulutuksella ja ohjeistuksilla. Tavoitteena on työntekijöiden vastuullinen, turvallinen ja kriittinen tekoälyn käyttö.

Hankinnat

Vuoden 2025 alussa otettiin käyttöön päivitettyt hankintoihin liittyvät henkilötietojen käsittelyä säätelevät tietojenkäsittelysopimus -liitteet. EU:n tietosuoja-asetus edellyttää, että henkilötietojen käsittelyn lainmukaisuus varmistetaan erityisesti silloin, kun ulkoinen toimija käsittelee tietoja hankintasopimuksen perusteella. Tietosuojavaatimukset tulee sisällyttää hankinnan suunnitteluun. Aina kun palveluntuottaja käsittelee henkilötietoja kaupungin puolesta, käsittelystä on sovittava erikseen.

Tiedonhallinta

Kaupungin sopimushallinnan ohjetta täydennettiin vuonna 2025 sopimusasiakirjojen säilytys- ja arkistointiohjeella, joka tuli voimaan 1.1.2025 alkaen. Ohjeen mukaisesti sopimusasiakirjat on tullut tallentaa vuoden 2025 alusta alkaen asianhallintajärjestelmään.

Asiakirjojen ja muun aineiston tietoturvallisen tuhoamispalvelun uusi palvelusopimus tuli voimaan helmikuussa 2025. Palvelun kautta tuhotaan tietoturvallisesti paperi-, kartonki- ja muoviasiakirjat sekä tietoturvallista tuhoamista edellyttävä SER-jäte.

Kaupungissa otettiin käyttöön ohje asiakirjojen käsittelystä toimitilamuuttojen yhteydessä vuoden 2025 marraskuussa, jonka tarkoituksena on ohjeistaa asiakirjojen oikeanlaisesta käsittelystä ja muuttamisesta toimitilamuutoissa.

Vuoden 2025 aikana sivistys- ja hyvinvointipalveluissa on tarkasteltu henkilötietojen kirjaamisen prosesseja ja käytänteitä sekä annettu ohjeistusta niiden toteuttamiseen. Tavoitteena on ollut varmistaa, että henkilötietojen käsittely tapahtuu johdonmukaisesti ja tietosuojavaatimusten mukaisesti kaikissa palveluissa.

Opetustoimessa otettiin käyttöön sähköinen allekirjoitus perusopetuksen ja lukiokoulutuksen todistusten osalta.

Muita keskeisiä kehittämistoimia vuoden 2025 aikana:

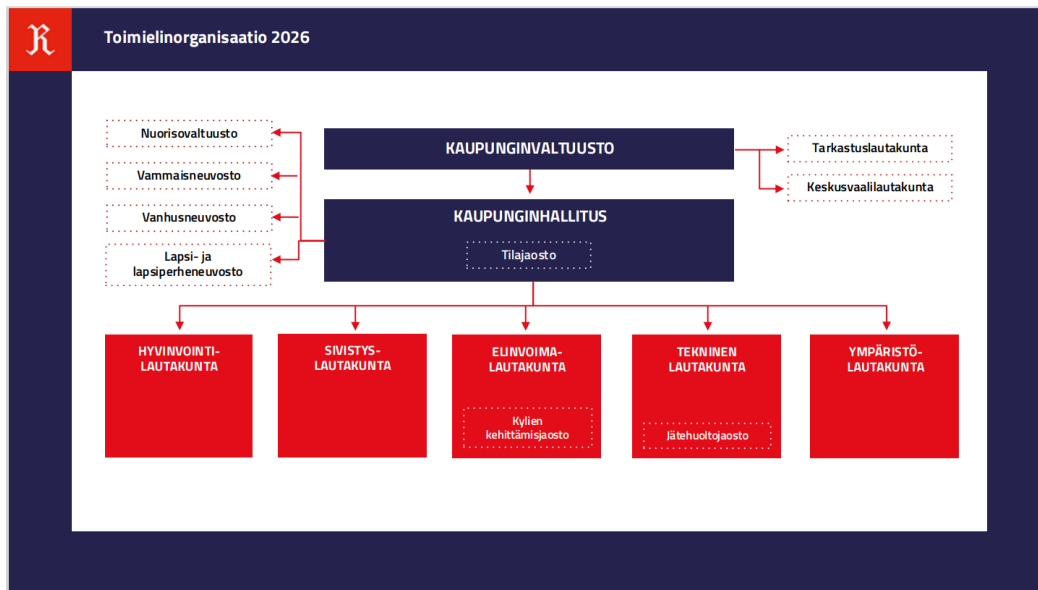
- jatkettiin kokonaisarkkitehtuurin mallintamista
- laajennettiin sähköisen arkiston käyttöä
- otettiin käyttöön uusia sähköisiä asiointipalveluita

2 Tietosuoja ja tietoturvallisuuden toteuttaminen

2.1 Kaupungin hallinnollinen organisaatio

Kaupungin hallinto-organisaation muodostavat: konsernihallinto, elinvoimapalvelut-, tekniset palvelut- ja sivistys- ja hyvinvointipalvelut toimialat.

Hallintosäännön 22 §:ssä määriteltyt toimialat voivat palveluiden tuottamiseksi jakaantua tarkoitustaan vastaaviin palvelualueisiin, jotka voivat edelleen jakaantua tarkoitustaan vastaaviin yksiköihin.



2.2 Tietohallinnon organisointi

Kaupungissa on keskitetty tietohallinto, jonka tehtävänä on johtaa kaupungin tietohallintoa ja ICT-kokonaisarkkitehtuuria. Tietohallinto- ja ICT-toimintoihin käytettävien tietohallinnon henkilöresurssien, hankkeiden, investointien, määrärahojen ja sopimusten ohjauksesta vastaa tietohallintojohtaja.

Tietohallintopalveluiden toiminta perustuu kaupunkistrategiaan, talousarvion täytäntöönpano-ohjeisiin, digiohjelmaan, palvelualueiden ja toimintayksiköiden kanssa sovittuun asiakkuuden hoitomalliin ja tietohallintoyksikön vuosikelloon. Tietohallintopalveluissa toimi vuonna 2025 tietohallintojohtaja ja viisi (5) vakituista tietohallintoasiantuntijaa. ICT-hankinnat suunnitellaan ja tehdään tietohallintopalveluiden kanssa.

Vuoden 2025 syksyllä kaupunki teki ulkopuolisen konsultin toimesta tietohallinnon arvioinnin. Sen keskeisempänä tuloksena on selkeyttää ICT tuotannon ja tietohallinnon keskeisiä toimia. Lisäksi organisointia koskien tuli esitys mm. tietoturvan, kokonaisarkkitehtuurin, tietojohdamisen ja projektinhallinnan osalta.

2.3 Tietoturvan ja tietosuojan organisointi

Kokonaisvastuu tietoturvan ja tietosuojan toteutumisesta on kaupunginhallituksella ja kaupunginjohtajalla. Kaupungin johdon vastuulla on huolehtia tietoturva- ja tietosuojatyön riittävästä resursoinnista.

Kaupunginhallitus on tiedonhallintalain tarkoittama tiedonhallintayksikön johto kaupungissa. Kaupunginhallitus seuraa tietoturvallisuuden sekä tietosuojan toteutumista kaupungissa. Kaupunginhallitus hyväksyy tietoturva- ja tietosuojapolitiikan. Kaupunginhallitus vastaa rekisterinpitäjänä kaupunginhallituksen alaisten toimintojen henkilötietojen käsittelystä.

Kaupunginhallitus vastaa siitä, että tiedonhallintalain 4.2 §:n vastuut, käytännöt ja valvonta on määritelty.

Lautakunta vastaa rekisterinpitäjänä toimialansa palvelujen henkilötietojen käsittelystä. Poikkeuksena jätehuoltojaosto, joka toimii rekisterinpitäjänä vastuualueensa henkilötietojen käsittelyssä.

Kaupunginjohtaja vastaa tietoturvallisuuden sekä tietosuojan toteuttamisesta kaupungin organisaatiossa ja kaupunginhallituksen esittelijänä näiden toteutumisen raportoinnista sekä edellä kaupunginhallituksen vastuulle määriteltyjen tehtävien valmistelun johtamisesta. Kaupunginjohtaja nimeää tietoturva- ja tietosuojatyöryhmän.

Henkilöstö- ja hallintojohtaja hyväksyy koko kaupunkia koskevat tietoturva- ja tietosuojaohteet.

Toimialajohtaja vastaa toimialansa tietoturvallisuuden ja tietosuojan toteutumisesta. Toimialajohtajan tehtäviin kuuluu lisäksi varmistaa tietoturvaan ja tietosuojaan liittyvän lainsäädännön, linjausten, periaatteiden ja ohjeistusten noudattaminen toimialallaan.

Tytäryhtiöiden ja -säätiöiden hallitukset ja toimitusjohtajat vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta omissa organisaatioissaan.

Rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta koko käsittelyn elinkaaren ajan. Rekisterinpitäjä hyväksyy kaupunginhallituksen päättämien tietoturvan ja tietosuojan keskeisten periaatteiden pohjalta omaa sektoriaan koskevat tietosuojan ja tietoturvan keskeiset periaatteet sekä täydentävät erityismääräykset.

Rekisterin vastuuhenkilö vastaa omalta osaltaan kyseisen rekisterin tietosuojasta, riskienhallinnasta ja tietosuojaselosteen lainmukaisuudesta. Palvelualuepäällikkö toimii vastuullaan olevan palvelualueen henkilötietojen käsittelyn vastuuhenkilönä. Vastuualuepäällikkö toimii vastuualueensa henkilötietojen käsittelyn vastuuhenkilönä. Mikäli palvelualuepäällikköä tai vastuualuepäällikköä ei ole nimetty, tällöin rekisterinpitäjä nimeää rekisterin vastuuhenkilön.

Rekisterin vastuuhenkilö

- nimeää rekisterin yhteyshenkilön
- määrittelee ja hyväksyy toiminnassaan tarpeelliset eri tehtävissä muodostuvat henkilörekisterit
- huolehtii, että henkilötietojen käsittelyn vaiheet sekä seloste käsittelytoimista on kuvattu Rovaniemen kaupungin tiedonhallintamallissa ja että rekisteröidyn informointi on ajantasainen
- hyväksyy omaa sektoriaan koskevat tietosuojaan liittyvät ohjeet henkilötietojen käsittelyyn.

Rekisterin yhteyshenkilö avustaa rekisterin vastuuhenkilöä rekisteröityjen informoinnista kyseisen rekisterin osalta. Rekisteröity voi kääntyä rekisterin

yhteyshenkilön puoleen saadakse tarkempia tietoja rekisteristä tai omista oikeuksistaan. Esihenkilö vastaa tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan. Esihenkilön keskeisimmät tehtävät on huolehtia

- oman yksikkönsä henkilöstön perehdyttämisestä kaupungin tietoturva- ja tietosuojaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin
- oman yksikkönsä henkilöstön tietoturva- ja tietosuojakoulutusten suorituksen seurannasta
- oman yksikkönsä lainsäädännön mukaisesta tiedon käsittelystä
- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
 - työnantajalle kuuluvan tiedon ja muun omaisuuden palauttamisesta
 - työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta

Luottamushenkilö vastaa

- omasta perehtymisestään kaupungin tietoturva- ja tietosuojaohjeisiin
- tietosuoja- ja tietoturvakoulutuksen suorittamisesta
- luottamustehtävänsä hoitaessaan lainsäädännön mukaisesta tiedon käsittelystä
- luottamustehtävän päättyessä kaupungille kuuluvan tiedon ja muun omaisuuden palauttamisesta

Henkilöstö ja luottamushenkilöt vastaavat omalta osaltaan tietoturva- ja tietosuojaohjeiden noudattamisesta. Jokaisen vastuulla on lisäksi tietoturvallisuuteen ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi kaupungin intranetistä löytyvän tietoturvapoikkeamien ohjeistuksen mukaisesti. Jokaisella on vastuu työtehtävänsä liittyvän tietosuojan toteuttamisesta sekä tiedon ja tietojärjestelmien asianmukaisesta käytöstä.

Tiedon laatija vastaa tiedon elinkaaren hallinnasta, luokittelusta (julkisuuden ja salassapidon määrittely) ja eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

Tietojärjestelmästä vastaava viranhaltija tai hänen määräämä vastuuhenkilö vastaavat tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy käyttöoikeuden hakijan esihenkilö.

Tietohallintojohtaja johtaa tietohallintoyksikön ja tietoturva- ja tietosuojatyöryhmän toimintaa. Hän vastaa tietoturvallisuuden arjen toimivuudesta sekä tietoturva- ja tietosuojapolitiikan ja kaupunkitasoisen tietoturvadokumentaation valmistelusta ja kehittämisestä. Lisäksi hän johtaa ja valvoo kaupungin ICT-teknologista arkkitehtuuria mukaan lukien pilvipalvelut. Tietohallintojohtaja raportoi tieto- ja kyberturvallisuuden toteutumisesta kaupunginjohtajalle ja kaupunginhallitukselle.

Sisäinen tarkastaja vastaa toiminnan tuloksellisuuden tarkastamisesta ja arvioinnista. Tähän kuuluu myös tietoturvallisuuden asianmukaisuuden ja riittävyyden arviointi ja tarkastaminen.

Tietosuojavastaava toimii kaupunkiorganisaation tukena ja antaa neuvoa sekä ohjausta tietosuojan toteuttamisesta. Tietosuojavastaava seuraa ja valvoo kaupungin tietojenkäsittelyyn liittyviä toimintatapoja ja tuo esille havaitsemiaan puutteita. Tietosuojavastaava toimii kaupungin yhteyshenkilönä sekä valvontaviranomaisiin että rekisteröityihin. Tietosuojavastaava raportoi tietosuojan toteutumisesta kaupungin johdolle. Kaupunkikonsernin tytäryhtiöt ja säätiöt vastaavat tietosuojavastaavan nimittämisestä EU:n tietosuoja-asetuksen edellyttämällä tavalla.

Tietoturva- ja tietosuojatyöryhmä seuraa tietoturvallisuuden yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden toteutumista kaupungissa. Ryhmä analysoi ja arvioi edellä mainittua kokonaisuutta ja valmistelee siihen perustuen kehitysehdotuksia ja linjauksia tietoturvallisuuden parantamiseksi. Työryhmä seuraa osaltaan tietosuojan toteutumista kaupungissa. Ryhmä valmistelee tietosuojaan liittyviä ohjeita ja toimintatapoja, tuottaa raportteja sekä analysoi toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietosuojariskejä.

Työryhmä valmistelee vuosittaisen toimintasuunnitelman, jossa yhtenä tehtävänä on valita keskeinen tietoturvan ja/tai tietosuojan kehittämiskohde. Kohteen, joka voi olla hallinnollinen (esimerkiksi henkilöstön osaaminen) tai tekninen (esimerkiksi pääsynhallintaratkaisut), keskeiset tavoitteet ja linjaukset tarkistetaan ja päivitetään. Tietosuoja- ja tietoturvatyöryhmän jäsenet nimetään asemansa ja asiantuntemuksensa perusteella.

Tietosuojan ja tietoturvan yhdyshenkilöt nimetään palvelualue- tai yksikkökohtaisesti, joka osaltaan tukee toimialakohtaista tietoturva- ja tietosuojakäytäntöjen jalkautumista ja ajantasaisen tietosuojatietoisuuden ylläpitämistä henkilöstölle. Yhdyshenkilöiden koordinoijana toimii tietosuojavastaava ja tietohallintoasiantuntija. Tietosuojan ja tietoturvan yhdyshenkilö jakaa tietoa ja seuraa tietosuojan ja tietoturvan toteutumista sekä kehittää ja lisää tietosuoja- ja tietoturvatietoisuutta edustamallaan alueella.

2.4 Tekniset ja organisatoriset toimenpiteet

Tietoturvaan ja tietosuojaan liittyviä riskejä pienennetään mm. seuraavilla hallintakeinoilla:

Henkilöstön käytössä on:

- Sähköinen tietoturvallisuuden ja tietosuojan koulutusympäristö
- Henkilöstön tietoturva- ja tietosuojaopas
- Kirjallinen tietoturva- ja tietosuojoinen politiikka
- Turvapostipalvelu
- Sähköinen palvelu tietoturvapoikkeamien ilmoittamiseen
- Turvatulostus
- Intranet erilaisille käytännön ohjeille
- Kaksi- tai monivaiheinen tunnistautuminen (ei vielä kaikilla)
- Häiriötilanteiden toimintakortit, tilanpäiväkirjat

Muita hallintakeinoja:

- Työasemilta turvallinen ja salattu VPN-etäyhteyshetvratkaisu kaupungin verkkoon
- Kannettavien työasemien kiintolevyt on kryptattu
- Älypuhelimissa on käytössä Intune laitehallinta (lukituskoodi, puhelin voidaan poistaa etänä, sovellusten jakelu keskitetysti etänä)
- Tietoturvallisuuden ja tietosuojan osalta palvelusopimuksissa käytetään kaupungin omia vakioituja liitteitä
- Keskitetty IDM-ratkaisu (Identity Management), jolla hallitaan käyttövaltuuksia/käyttöoikeuksia sekä niiden voimassaoloa

2.5 Riskienhallinta

Riskienhallinta on osa sisäistä valvontaa. Se on dynaaminen prosessi, jossa tunnistetaan tavoitteiden saavuttamiseen vaikuttavia riskejä ja arvioidaan riskien merkittävyttä suhteessa määriteltyyn riskiensietokykyyn. Riskienhallinnassa huomioidaan niin ulkoisen kuin sisäisen toimintaympäristön muutosten vaikutuksia kaupungin toimintaan. Hyvällä riskienhallinnalla pyritään riskien tunnistamiseen ennalta, riskien luokitteluun ja vaikutusten arviointiin ja riskienhallintatoimenpiteiden toteuttamiseen. Tavoitteena on riskien toteutumisen ennaltaehkäisemiseen tai niiden vaikutusten minimoiminen.

Rovaniemen kaupungilla riskienhallinnan vuosikelloon kuuluu riskien tunnistaminen ja arviointi sekä riskienhallintasuunnitelmien koostaminen vuoden alussa. Riskienhallintasuunnitelman muodostamisessa auttaa edellisen vuoden riskien raportointi, mutta näiden lisäksi on arvioitava, onko toimintaympäristön jatkuvassa muutoksessa muodostunut uusia riskejä tai miten aiemmin arvioinnin kohteena olevat riskit ovat muuttuneet. Riskienhallintasuunnitelmat hyväksytään toimialojen osalta lautakunnissa ja konsernihallinnon osalta kaupunginhallituksessa. Lisäksi riskejä ja riskien hallintaa käsitellään kaupungin johtoryhmässä. Tietosuoja- ja tietoturvariskejä on tunnistettu sekä konsernihallinnon, että toimialojen raportoinnissa ja niiden hallintakeinoja on pohdittu riskienhallintasuunnitelmissa. Loppuvuodesta 2025 kaupunki hankki riskienhallintaohjelman, joka yhtenäistää riskien arviointia, kuvaamista ja hallintakeinoja koko kaupunkiorganisaatiossa. Riskien esittäminen johdolle ja päätöksentekijöille on jatkossa visuaalisempaa ja riskienhallintatahot ovat helpommin vastuutettavissa.

Viimeaikainen Euroopan geopolittisen tilanteen muuttuminen on muodostanut enenevässä määrin epävarmuus- ja riskitekijöitä myös tietohallinnolle. Tietohallinnon tulee näiltä osin edelleen tarkentaa varautumistaan erilaisiin tilanteisiin ja skenaarioihin liittyen.

Varautumissuunnittelu vaatii ICT-palveluihin liittyvien uhka-arvioiden tuntemusta eli sitä, millaisiin häiriötilanteisiin kaupungissa varaudutaan. Häiriötilanne on uhka tai tapahtuma, joka voi koskettaa sekä kaupungin työntekijöitä että kuntalaisille tarjottavia palveluita. Ongelmia syntyy tai erilaisia skenaarioita voi pahentaa, mikäli esimerkiksi puhelin- sähkö- tai tietoliikenneverkkoihin kohdentuu häiriöitä.

Näiden osalta kaupunki ottaa varmuuskopiot M365 palveluista kotimaan varmuuskopiointi palvelimille. Lisäksi kaupunki suunnittelee ja toteuttaa peruskorjauksen yhteydessä kaupungintalolle nykyaikaisen palvelinsalin.

Kaupungintalon peruskorjaus aiheutti riskin kaupunginarkiston aineistojen säilyvyydelle vuonna 2025. Riskin pienentämiseksi osa kaupunginarkiston aineistoista siirrettiin kaupungintalolta väistötiloihin peruskorjauksen ajaksi ja kaupungintalolla olevien aineistojen osalta on tehty organisatorisia, sopimuksellisia ja fyysisiä toimenpiteitä arkistoaineistojen luottamuksellisuuden ja eheyden turvaamiseksi peruskorjauksen ajan. Toimenpiteillä saatiin vähennettyä arkistoaineistoon kohdistuvia riskejä huomattavasti.

Tietosuojaan riskienhallinnan tulee olla kiinteä, hallittu ja jatkuva osa organisaation toimintaa, jotta tietosuojariskeihin voidaan vastata muuttuvassa ja lisääntyvien uhkien toimintaympäristössä. Tietoturvan riskienhallinta on olennainen osa tietosuojaan riskienhallintaa, ja toimiva riskienhallinta on edellytys hyvän tietosuojatason saavuttamiselle organisaatiossa. Tietosuoja-asetuksen velvoitteet ja suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröityjen oikeuksille ja vapauksille aiheutuvaan riskiin. Rekisterinpitäjän on tämän vuoksi arvioitava henkilötietojen käsittelyyn liittyvät riskit järjestelmällisesti, jotta sisäänrakennettu ja oletusarvoinen tietosuoja sekä muut asetuksen mukaiset velvoitteet voidaan toteuttaa asianmukaisesti.

Tietosuojaan vaikutustenarviointi tukee tietosuoja-asetuksen vaatimusten noudattamista ja osoitusvelvollisuuden toteuttamista. Vaikutustenarviointi on tehtävä, jos henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille. Rovaniemen kaupungilla on käytössään oma ohjeistus ja prosessi tietosuojaan vaikutustenarvioinnin toteuttamiseen. Vuoden 2025 aikana tietosuojaan vaikutustenarviointeja toteutettiin riskinarviointiin perustuen tarpeen mukaisesti kaupungin eri toimialoille.

Tietohallinnon riskienhallintasuunnitelmassa on arvioitu keskeisimmät riskit, niiden toteutumisen todennäköisyys, vaikutukset, vakavuus ja toimenpiteet riskien pienentämiseksi.

Sisäinen valvonta ja riskienhallinta päivittäisessä toiminnassa toteutuu:

- esihenkilöiden ja henkilöstön suorittamana riskien tunnistamisena ja arviointina
- riskien hallintatoimenpiteiden toteuttamisena ja valvontana
- valtuuksien, päätösten ja ohjeiden noudattamisena
- prosessien ja tietojärjestelmien kontrolleina

2.6 Tarkastukset

Kaupungissa tehdään tietojärjestelmiin ja prosesseihin liittyviä sisäisiä ja ulkoisia tarkastuksia ja auditointeja. Sisäisiä tarkastuksia suorittaa sisäinen tarkastaja ja tietosuojaan osalta tietosuojavastaava valvoo organisaation toimintaa. Sisäisen tarkastuksen toimintasuunnitelmassa ei ollut vuodelle 2025 tietojärjestelmiin ja prosesseihin kohdistuvia tarkastuksia.

Tilintarkastukseen liittyen tehtiin talouden järjestelmiin it-tarkastus, jossa nousi muutamia kehittämiskohteita esille. Käyttöoikeushallinta oli tarkastuksen mukaan asiallisella tasolla.

Ulkoisia tarkastuksia tekevät kaupungin tilintarkastajat. Tietohallintopalvelut tilaa tietojärjestelmiä koskevia teknisiä ja toiminnallisia auditointeja ulkopuolisilta asiantuntijoilta.

2.7 Tietoturvapoikkeamien käsittely

Työntekijöillä on velvollisuus ilmoittaa kaikista tietoturvaan tai tietosuojaan liittyvistä havaitsemistaan puutteista, väärinkäytöksistä tai epäillyistä rikkomuksista esihenkilölleen. Esihenkilön vastuulla on viipymättä tiedottaa tietosuojavastaavaa kaikista tapauksista, joissa puutteet, väärinkäytökset tai rikkomukset kohdistuvat tietosuojaan eli henkilötietoihin. Rekisterinpitäjän tulee dokumentoida kaikki tietoturvaloukkaukset, mukaan lukien loukkauksen yksityiskohdat, vaikutukset sekä toteutetut korjaavat toimenpiteet. Työntekijän tai esihenkilön on tehtävä tietoturvapoikkeamailmoitus kaupungin käytössä olevan sähköisen ilmoituskanavan kautta. Tämä kanava mahdollistaa poikkeamien järjestelmällisen dokumentoinnin, käsittelyn ja seurannan. Saadun ilmoituksen pohjalta poikkeamatilanteisiin reagoidaan asianmukaisesti ja ryhdytään tarvittaessa oikea-aikaisiin toimenpiteisiin, jotta poikkeaman vaikutukset voidaan minimoida ja vastaavat tilanteet ehkäistä jatkossa.

3 Tiedonhallinta, tietovarannot ja tietovirrat

3.1 Tiedonhallinnan organisointi

Viranomaisorganisaatioiden tiedonhallintaa säätelevät tiedonhallinnan yleislait ja toimialakohtaiset erityislait. Keskeisiä tiedonhallintaan vaikuttavia yleislakeja ovat tiedonhallintalaki, arkistolaki, Euroopan unionin yleinen tietosuoja-asetus, tietosuojalaki, julkisuuslaki, digipalvelulaki ja sähköinen asiointilaki.

Vuoden 2025 aikana eduskunnan käsittelyyn tuotiin arkistolain uudistus, jonka tarkoituksena on lisätä viranomaisten sähköistä arkistointia sekä kuntien osalta mahdollisuutta käyttää Kansallisarkiston sähköistä arkistointipalvelua asiakirjojen arkistointiin. Lakiuudistuksen eduskuntakäsittely oli vuoden 2025 lopulla yhä kesken.

Tiedonhallinnalla tarkoitetaan viranomaisorganisaatioissa tehtävien hoitoon tai muun toiminnan tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä tietoaaineistojen, niiden käsittelyvaiheiden ja niiden sisältämien tietojen hallinnoimiseksi riippumatta tietoaaineistojen tallentamistavasta ja muista käsittelytavoista. Tiedonhallinnan kohteena ovat asiakirjat, niiden sisältämät tiedot ja muut vastaavat tiedot, kuten tietokantojen sisältämät tietueet, jotka eivät itsessään muodosta asiakirjoja.

Kaupungin tiedonhallinnan ohjausta hoitavat tiedonhallintapalvelut ja tietohallintapalvelut. Tietohallintapalveluiden vastuualueella on kokonaisarkkitehtuurin (yhteentoimivuuden), tietojärjestelmien ja

tietoturvallisuuden ohjaus. Tiedonhallintapalveluiden vastuualueella on asianshallinnan, asiakirjahallinnon ja arkistotoimen ohjaus.

Tiedonhallintapalvelut-tiimi sijoittuu organisaatiossa hallintopalvelut-yksikön alaisuuteen osana Tiedonhallinta- ja asiointipalveluja. Tiedonhallintapalvelut huolehtii kaupungin kirjaamo- ja arkistopalveluista ja sen henkilöstö työskentelee kaupunginkirjaamossa ja kaupunginarkistossa.

3.2 Tiedonhallinnan ohjaus

Kaupungin tiedonhallintaa ohjataan määräyksillä, ohjeilla ja kuvauksilla.

Tiedonhallintalain edellyttämän tiedonhallintamallin koostamiseksi otettiin käyttöön Digiturvamalli-järjestelmä vuonna 2021. Järjestelmään oli tarkoitus kuvata kaupungin tiedonhallintamalli, asiakirjajulkaisuuskuvaus sekä kerätä keskeiset tietoturvaa ja tietosuojaa koskevat prosessit ja asiakirjat. Asiakirjajulkaisuuskuvaus on julkaistu kaupungin verkkosivuilla vuonna 2022, mutta vaatii säännöllistä päivittämistä.

Tiedonhallintamallin siirtäminen osaksi kaupungin kokonaisarkkitehtuurikuvausta QPR-sovellukseen aloitettiin vuoden 2024 aikana. Tarkoituksena on, että tiedonhallintamalli olisi kuvattuna QPR-sovellukseen kokonaisarkkitehtuurikuvauksen yhteyteen vuosina 2025–2026.

Kaupunki sai vuonna 2025 julkisen hallinnon tiedonhallintalautakunnalta huomautuksen tiedonhallintamallin laatimiseen ja ylläpitoon liittyvistä puutteista. Asiaa käsiteltiin kaupunginhallituksen kokouksessa 24.3.2025 ja tarkastuslautakunnan kokouksessa 8.4.2025. Tarkastuslautakunnan kokouksessa annettiin arvio, että tiedonhallintamalli saataisiin kuvattua valmiiksi QPR-sovellukseen vuoden 2026 loppuun mennessä.

3.3 Tiedon elinkaaren hallinta

Tiedon elinkaari ja tietoaineistojen säilytysajat on määritelty tehtäväkohtaisesti ja niiden sisältämän tiedon mukaan. Tiedon säilyttämisestä ja arkistoinnista sekä asiakirjahallinnon vastuista on laadittu kaupungin asiakirjahallinnon ja arkistotoimen toimintaohje vuonna 2016. Asiakirjahallinnon ja arkistotoimen toimintaohje on tarkoitus uudistaa vuoden 2026 aikana.

Asianshallintajärjestelmässä olevien tietojen elinkaarta ohjaa tiedonohjaussuunnitelma, johon on määritelty asioiden, käsittelyvaiheiden ja asiakirjojen elinkaarta ohjaavia metatietoja, kuten säilytysaikatiedot ja säilytysajan laskentaperusteet. Tiedonohjaussuunnitelman runkona toimii kaupungin tehtäväluokitus, johon on määritelty Kuntien yhteisen tehtäväluokituksen pohjalta kaupungin tehtävät. Vuoden 2025 aikana tiedonohjaussuunnitelmaa päivitettiin esiopetuksen, kaavoituksen, katu- ja puistosuunnittelun, rekrytoinnin, tarkastustoimen ja varhaiskasvatuksen tehtävien osalta.

Tietojen säilytysajat ja -tavat merkitään kaupungin arkistonmuodostussuunnitelmaan. Koko kaupungin arkistonmuodostussuunnitelma on päivitetty kokonaisuudessaan vuonna 2016. Vuonna 2025 arkistonmuodostussuunnitelmaa päivitettiin samojen tehtävien osalta, kuin tiedonohjaussuunnitelmaa. Arkistonmuodostussuunnitelmalla ei voida ohjata tietojärjestelmissä olevien tietojen elinkaarta teknisesti. Elinkaaren vaiheiden hallinta ja tietojen tuhoaminen tietojärjestelmistä on riippuvainen tietojärjestelmien toiminnoista.

3.4 Tietovarannot

Tiedonhallintamallin päivitystyön yhteydessä tietovarannot määriteltiin osin uudelleen vuonna 2024. Osa tietovarannoista yhdistettiin uudelleen määrittelyssä, minkä tuloksena kaupungilla on tällä hetkellä 24 tunnistettua tietovarantoa.

3.5 Asianhallinta ja sähköinen asiointi

Asiarekisteröintiä toteutetaan kaupungilla pääasiassa asianhallintajärjestelmässä. Asianhallinnan tarkoituksena on hallita ja seurata viranomaisen käsiteltäväksi saapuneita ja otettuja asioita sekä niiden käsittelyvaiheita ja niihin liittyviä asiakirjoja.

Asianhallintajärjestelmäkokonaisuuteen kuuluvaa sähköisen asiointipalvelun käyttöä laajennettiin ottamalla käyttöön uusia asiointilomakkeita vuoden 2025 aikana.

3.6 Asiakirjahallinto ja arkistotoimi

Sähköinen arkisto on otettu käyttöön, ja sinne on viety käytöstä poistuneen asianhallintajärjestelmän aineisto sekä rakennettu rajapinta tällä hetkellä käytössä olevaan asianhallintajärjestelmään. Sähköisen arkiston käyttöönottoa laajennetaan asteittain muihin järjestelmiin ja tietoaaineistoihin.

Kaupunginarkistossa on valmisteltu sosiaali- ja terveydenhuollon tietoaaineistoja valmiiksi tietoaaineiston siirtoja varten Lapin hyvinvointialueelle. Tietoaaineistojen siirtosopimus luonnosteltiin vuonna 2024, mutta Lapin hyvinvointialue toi vuoden 2025 syksyllä käsiteltäväksi oman versionsa sopimuksesta, jonka pohjalta sopimusneuvotteluja on jatkettu. Tavoitteena on, että sopimus saadaan aikaiseksi vuoden 2026 aikana.

Kaupungintalon peruskorjauksen johdosta kaupungintalolta jouduttiin siirtämään asiakirjoja väistötiloihin. Samassa yhteydessä Lapin hyvinvointialueelle luovutettiin sen arkistoihin 240 hyllymetriä sosiaali- ja terveydenhuollon asiakirjoja, jotka olivat siirtyneet sen rekisterinpitöön ja vastuulle Sosiaali- ja terveydenhuolto ja pelastustoimea koskevan uudistuksen toimeenpanosta ja sitä koskevan lainsäädännön voimaantulon jälkeen annetun lain 64 §:n perusteella.

4 Lainsäädäntö ja linjaukset

4.1 Lainsäädäntö

Julkishallinnon organisaatiot noudattavat Suomen ja EU:n lainsäädäntöä. Kuntia ohjaavat muun muassa kuntalaki, hallintolaki, julkisuuslaki, EU:n yleinen tietosuoja-asetus, tietosuojalaki, arkistolaki sekä lukuiset muut yleis- ja erityislait. Lisäksi sisäisillä ja ulkoisilla rahoittajilla (projektit, hankkeet) on omat ohjeistuksensa henkilötietojen käsittelystä, säilyttämisestä ja arkistoinnista. Tämän lisäksi Rovaniemen kaupungilla on omia käytännönsäätöjä ja ohjeistuksia. Kaupungilla on myös omavalvontaa sekä virallisempia auditointeja.

4.2 Poliitikat ja kaupungin säännöstö

Rovaniemen kaupungin tietoturva- ja tietosuojapolitiikan hyväksyy kaupunginhallitus. Edellinen tietoturva- ja tietosuojapolitiikka on hyväksytty 30.9.2024.

Rovaniemen kaupungin hallintosäännössä on oma erillinen luku tiedonhallinnan ja asiakirjahallinnon järjestämisestä. Luku uudistettiin kaupunginvaltuuston päätöksellä 9.12.2024 § 101, ja uudistettu hallintosääntö tuli voimaan 1.1.2025 alkaen.

Asiakirjahallinnosta ja arkistotoimesta on määrätty ja ohjeistettu kaupunginhallituksen 26.11.2016 § 477 hyväksymässä asiakirjahallinnon ja arkistotoimen toimintaohjeessa. Arkistonmuodostuksen rakenteesta kaupunginhallitus on päättänyt päätöksellään 28.11.2016 § 476.

5 Koulutus, ohjeistus ja harjoitukset

5.1 Koulutus

Tietoturvaan, tietosuojaan ja tekoälyyn liittyvää koulutusympäristöä uudistettiin vuoden 2025 aikana. Kaupunki otti käyttöön uuden tietoturvan ja tietosuojan sähköisen verkkokoulutusympäristön, jossa jokaisen kaupungin viranhaltijan, työntekijän ja luottamushenkilön tulee suorittaa hyväksytysti koulutus. Kaupunginjohtajan päätöksellä tietoturva- ja tietosuojakoulutus tulee uusia yhden (1) vuoden välein. Koulutuksen suorittaminen uusille työntekijöille on edellytyksenä käyttäjätunnuksia tilattaessa.

5.2 Ohjeistus

Kaupungin Intranetissä on julkaistu sekä esihenkilön että työntekijän muistilistat, joihin on koottu tärkeimmät asiat palvelussuhteen alkua, päättymistä tai muuta muutostilannetta varten. Näitä ovat esimerkiksi työvälineiden ja tunnusten tilaaminen (ja palauttaminen), tietoturva- ja tietosuojakoulutus, kulkuoikeudet / avaimet sekä työajanseurantaan liittyvät asiat.

Kaupungin intranet sivuilla oleva tietopankki sisältää keskeiset tietoturvaan ja tietosuojaan liittyvät ohjeistukset. Ohjeita tarkastellaan vuosittain ja päivitetään tarvittaessa.

Kaikissa kaupungin hankinnoissa noudatetaan ensisijaisesti kaupungin omia sopimusmalleja sekä julkishallintoon soveltuvia, kulloinkin voimassa olevia yleisiä ehtoja. ICT-hankintojen osalta sovelletaan tarvittavilta osin JIT-ehtoja, jotta varmistetaan tietoteknisten palveluiden ja tuotteiden hankintojen yhteensopivuus ja laatu. Mikäli hankinnassa toimittaja käsittelee henkilötietoja kaupungin puolesta tai lukuun, sopimukseen liitetään Rovaniemen kaupungin laatimat erityisehdot henkilötietojen käsittelystä. Näissä erityisehdoissa määritellään tarkasti henkilötietojen käsittelyn edellytykset ja käsittelytoimien kuvaus. Henkilötietojen käsittelyn ehdot ja käsittelytoimien kuvaus on päivitetty vuoden 2025 alussa, jotta ne vastaavat ajantasaisia vaatimuksia ja varmistavat henkilötietojen asianmukaisen käsittelyn kaikissa kaupungin hankkeissa.

5.3 Harjoitukset

Harjoituksen avulla reagointi häiriötilanteissa voidaan hoitaa tositilanteessa hallitummin, jolloin toipuminen on nopeampaa ja harjoituksessa tehtyjen havaintojen pohjalta suunnitellaan tarvittavia kehittämistoimenpiteitä.

Harjoitustoiminnan tavoitteena on, että

- kaupungin johto tunnistaa kyberturvallisuusuhat sekä osaa varautua niihin
- selvittää millä tavalla ja missä vaiheessa kaupungin valmiusorganisaatio lähtee toimimaan häiriötilanteessa
- kaupungin varautumisen ja valmiussuunnitelmien kehittäminen
- valmiuksien parantaminen uudentilanteissa häiriötilanteissa
- kaupungin, sen sidosryhmien ja toimijoiden välisen yhteistoiminnan edistäminen
- tunnistaa eri toimijoiden kannalta kriittisiä toimintoja ja järjestelmiä sekä niiden haavoittuvuuksia uhkamallien mukaisissa tilanteissa

Helmikuussa 2025 Rovaniemen kaupunki osallistui laajalla asiantuntijaryhmällä Jyväskylässä järjestettyyn Kyha25-kyberturvaharjoitukseen, joka oli suunnattu kriittisen infrastruktuurin ja kuntien yhteiseen valmiuden kehittämiseen. Viikon mittaisen harjoituksen aikana simuloitiin erilaisia kyberturvallisuustilanteita, joissa kaupungin eri toimialat – kuten tietohallinto, viestintä, tekninen toimiala, tietosuoja ja riskienhallinta – saivat mahdollisuuden testata osaamistaan ja toimintamallejaan. Harjoitus tarjosi turvallisen ja asiantuntevasti ohjatun ympäristön kyberturvallisuuteen liittyvien skenaarioiden käsittelyyn. Kyha-harjoitukset toteutetaan Suomen Kyberturvallisuuskeskuksen järjestämänä ja rahoittamana.

6 Rekisteröidyn oikeuksien toteutuminen

6.1 Tietosuoja koskevat periaatteet

Jokaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, jonka tavoitteena on turvata rekisteröityjen oikeuksien ja vapauksien toteutuminen henkilötietojen käsittelyssä.

Tietosuojaperiaatteiden mukaisesti henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidylle läpinäkyvällä tavalla. Henkilötietoja saa kerätä ja käsitellä vain ennalta määritellyn, nimenomaiseen ja lailliseen tarkoitukseen, ja käsittelyn tulee rajoittua tarkoituksen kannalta tarpeellisiin tietoihin. Henkilötietojen on oltava täsmällisiä ja päivitettävä aina tarvittaessa. Virheelliset tai epätarkat tiedot on oikaistava tai poistettava viivytyksettä. Henkilötietoja saa säilyttää tunnistettavassa muodossa vain niin kauan kuin se on käsittelyn tarkoituksen toteuttamiseksi tarpeen. Lisäksi henkilötietoja on käsiteltävä luottamuksellisesti ja tietoturvallisesti.

6.2 Rekisteröityjen informointi asiointipalveluissa

Kuntalaisten informointiin tarkoitetut julkiset tietosuojaselosteet löytyvät kaupungin verkkosivuilta. Kaupungin intranet -sivuilta löytyvät työntekijöiden henkilötietoja sisältävät tietosuojaselosteet.

6.3 Selosteet ja niiden ajantasaisuus

Rovaniemen kaupungilla on käytössä yleisen tietosuoja-asetuksen vaatimukset täyttävä tietosuojaselostepohja, jonka sisällöstä vastaa rekisterinpitäjä tai hänen nimeämänsä vastuhenkilö. Selosteita päivitetään säännöllisesti ja tarpeen mukaan, jotta ne vastaavat yleisen tietosuoja-asetuksen vaatimuksia.

7 Kehittäminen ja tiedon hyödyntäminen

7.1 Tiedonhallinta ja kokonaisarkkitehtuuryö, tiedon hyödyntämisen kehittäminen

Tietohallintopalvelut on aloittanut vuonna 2023 kaupungin kokonaisarkkitehtuurikuvauksen laatimisen ja työtä jatkettiin vuonna 2025. Tiedonhallintamalli ja kokonaisarkkitehtuurikuvaus ovat luonteeltaan samankaltaisia ja niillä on samoja päämääriä. Tiedonhallintamalli on lakisääteinen kuvaus, johon kuvataan tiedot toimintaprosesseista, tietovarannoista, tietojärjestelmistä ja tietoturvaluustoimenpiteistä. Kokonaisarkkitehtuuri on kuvauksena laajempi ja sisältää myös tietojärjestelmäarkkitehtuurin ja teknologioiden yksityiskohtaisempia kuvauksia. Tiedonhallintopalvelut ja tietohallintopalvelut aloittivat vuoden 2024 aikana tiedonhallintamallin kuvaamisen osana kokonaisarkkitehtuurikuvausta. Työ jatkuu vuosille 2025 ja 2026.

Tiedonhallintamallin ja kokonaisarkkitehtuurikuvauksen suunnittelun ja ylläpidon tulevaa resursointia on tarpeen tarkastella ja arvioida lisäresursoinnin tarvetta.

Rovaniemen digiohjelmaa vuosille 2023–2026 valmisteltiin vuoden 2023 aikana, jonka kaupunginhallitus hyväksyi 27.5.2024. Digiohjelman toimenpiteitä ohjaamaan ja toteuttamaan on perustettu digiohjelman ohjaus- ja valmisteluryhmä. Digiohjelmassa on määritelty keskeisimmät kehittämistoimet tuleville vuosille. Kun digiohjelman kokonaisuuksia kehitetään ja uudistetaan, edellyttää se jatkuvaa arviointia myös tietoturva- ja tietosuoja-riskien näkökulmasta. Tietoturvaluus ja tietosuoja korostuvat esim. hankinnoissa, joihin liittyy sähköistä tiedonsiirtoa, käyttäjän tietojen tallentamista sähköisiin välineisiin tai muuta tiedon käsittelyä sähköisillä välineillä ja erityisesti, jos käsitellään salassa pidettävää/ei julkista tietoa. Panostamalla arviointiin, voidaan kaupungin digitaalisia palveluita käyttää turvallisesti.

Tiedolla johtamisen merkitys korostuu, kun organisaatioilla on paineita tehostaa toimintaa ja saada säästöjä. Kaupungilla on selvitelty erilaisia vaihtoehtoja tiedolla johtamiseen, ja ulkopuolisen konsultin johdolla on valmisteltu tiekarttaa.

7.2 Tietojärjestelmien kehittäminen, hankinta ja ylläpito

Tietojärjestelmät pyritään hankkimaan palveluna. Hankinnoissa tulee ottaa huomioon riittävät taloudelliset- sekä henkilöresurssit hankinnan määrittelyvaiheessa, jolla varmistetaan kaupungin vaatimuksia vastaava hankinta ja sujuva käyttöönotto. Tietojärjestelmälle tai palvelulle tulee nimetä aina omistaja/vastuutaho, jolla on kokonaisvaltainen vastuu kehittämisestä.

Tietoturvaluuden ja tietosuojan osalta uusissa sopimuksissa käytetään vakioituja liitteitä. Korkeariskisissä henkilötietoja sisältävissä hankinnoissa tehdään vaikutustenarviointi. IT-omaisuus on kirjattu konfiguraationhallintajärjestelmään ja leasing-sopimuksiin. Asennus- ja poistoprosessit on kuvattu.

7.3 Tietoturvaluuden ja tietosuojan kehittäminen

Tietosuojan ja tietoturvan yhdyshenkilöt on nimetty palvelualue- tai yksikkökohtaisesti tukemaan toimialakohtaisten tietoturva- ja tietosuojakäytäntöjen jalkauttamista sekä ylläpitämään henkilöstön ajantasaista tietosuojatietoisuutta. Yhdyshenkilötoimintaa koordinoivat tietosuojavastaava ja tietohallintoasiantuntija.

Yhdyshenkilöt välittävät tietoa, seuraavat tietosuojan ja tietoturvan toteutumista sekä edistävät tietosuoja- ja tietoturvaosaamista edustamallaan alueella. Yhdyshenkilöt ovat motivoituneita ja kiinnostuneita tietoturvan ja tietosuojan kehittämisestä.

8 Seuranta ja mittarit

8.1 Toimintaympäristö

Kaupungilla on sekä kaupungin hallintoverkko, että erillinen opetukseen ja asiakkaiden käyttöön tarkoitettu verkko. Koulujen henkilöstöllä on tunnukset molempiin verkkoihin. Kaupungin perus ICT-palvelut sekä käyttö- ja sovelluspalvelut on pääosin ulkoistettu, lukuun ottamatta mobiililaitteita.

Tunnusluku	Toteuma 2023	Toteuma 2024	Toteuma 2025
Työasemien lkm, henkilökunta	878	852	896
Käyttäjien lkm, (AD-tunnuksia)	2586	2648	2595
Työasemien lkm, opetus ja muut (sis. Chromebook, iPad, Mac -laitteet)	5840	6267	7126
Matkapuhelinten lkm (keskitetty hallinta)	1462	1204	1121
Turvapostin käyttäjät, lkm	496	477	600
Tietohallinnon henkilöstö, htv	7	7	6
Tietoturva ja tietosuojahenkilöstö, htv	1,25	0,75	1,25
Palvelupyyntöjen lkm (ServiceDesk)	2149	4306	4119
Häiriöilmoitusten lukumäärä (ServiceDesk)	1315	1551	1623

8.2 Tietovarannot

Tunnusluku	Toteuma 2023	Toteuma 2024	Toteuma 2025
Tietovarantojen lkm	28	24	24
Tietojärjestelmien lkm	180	192	336
Tietosuojaselosteiden lkm	38	43	52

8.3 Riskit, vaikutustenarvioinnit ja turvallisuusselvitykset

Tunnusluku	Toteuma 2023	Toteuma 2024	Toteuma 2025
Rekistereiden tietosuojaa koskevien vaikutustenarviointien (DPIA) lkm	6	3	12
Turvallisuusselvitykset	0	0	2 *)

*) Toisen viranomaisen teettämänä. Kaupunki ei itse tilaa turvallisuusselvityksiä.

8.4 Tietopyynnöt ja rekisteröityjen oikeuksien käyttö

Tunnusluku	Toteuma 2023	Toteuma 2024	Toteuma 2025
Julkisuuslain mukaiset tietopyynnöt, lkm	368	630	778
Julkisuuslain mukaiset tietopyynnöt (rakennusvalvonnan arkisto), noin lkm	~360	~500	~800
Kaavaotteita ja -määräyksiä koskevat tietopyynnöt, lkm	-	-	~220
Numeerista kartta-aineistoa koskevat tietopyynnöt, lkm	212	188	258
Rekisteritietojen tarkistuspyynnöt, lkm	3	15	22
Henkilötietojen korjaus- ja poistopyynnöt (kirjaamon kautta tulleet), lkm	0	1	0
Käyttö- ja luovutuslokitietopyynnöt, lkm	0	0	0

8.5 Tietoturvapoikkeaminen käsittely

Tunnusluku	Toteuma 2023	Toteuma 2024	Toteuma 2025
Tietoturvapoikkeama ilmoitukset, lkm	25	33	57
Valvontaviranomaiselle (Tietosuojavaltuutettu) ilmoitettujen tietoturvaloukkausten lkm	1	0	5
Tietoturvaloukkausten lkm, joissa ilmoitus rekisteröidyille	0	2	6
Valvontaviranomaiselle (Traficom/Kyberturvallisuuskeskus) ilmoitettujen tietoturvaloukkausten lkm	1	0	0

8.6 Tarkastukset

Tunnusluku	Toteuma 2023	Toteuma 2024	Toteuma 2025
Tietojärjestelmä- ja tietoturva-auditoinnit, sisäinen tarkastus lkm	0	1	0
Tietojärjestelmä- ja tietoturva-auditoinnit, ulkoinen tarkastus lkm	1	1	1

8.7 Tietoturva- ja tietosuojakoulutukset

Tunnusluku	Toteuma 2023	Toteuma 2024	Toteuma 2025
Sähköinen tietoturva- ja tietosuojakoulutus, suoritusten lkm	423 *)	248 *)	2189

*) vain uusien työntekijöiden suoritukset

9 Todennetut merkittävimmät kehityskohteet tulevalle vuodelle

9.1 Asianhallintajärjestelmän kilpailutus ja käyttöönotto

Asianhallintajärjestelmäkokonaisuuksista suoritettiin markkinakartoitus vuonna 2024. Markkinakartoituksen tuloksena kaupungin johtoryhmä linjasi, että asianhallintajärjestelmäkokonaisuus kilpailutetaan. Kilpailutus oli tarkoitus toteuttaa vuoden 2025 aikana, mutta järjestelmäkokonaisuuden laajuuden vuoksi kilpailutuksen toteutus siirtyi vuodelle 2026. Vuoden 2025 aikana toteutettiin kaksi

markkinavuoropuhelua asianhallintajärjestelmäkokonaisuuden hankinnasta ja markkinavuoropuhelua oli tarkoitus jatkaa vuodelle 2026. Tarkoituksena oli, että uusi asianhallintajärjestelmäkokonaisuus saataisiin otettua käyttöön joko vuoden 2027 alussa tai viimeistään vuoden 2027 kesällä.

9.2 Tekoälyn käyttöönoton jatkaminen

Kaupunki jatkaa tekoälyjärjestelmien hallittua käyttöönottoa tavoitteena tehostaa toimintaa ja käyttää resursseja entistä vaikuttavammin. Käyttöönotto tehdään vaiheittain, vastuullisesti ja voimassa olevan lainsäädännön edellytykset huomioiden. Tavoitteena on, että työntekijät osaavat hyödyntää tekoälyä turvallisesti, ymmärtäen sen mahdollisuudet ja siihen liittyvät riskit.

Tekoälyn käytön lisääntyessä kaupungilta edellytetään aktiivista tekoälyratkaisujen hallintaa, käyttöön liittyvää seurantaa sekä systemaattista riskienhallintaa. Lisäksi tekoälyn liittyvien säädösten ja vaatimusten seurannalle tulee määrittää selkeät vastuutahot. Näiden tehtävänä on varmistaa, että kaupungin käyttämät tekoälyratkaisut ovat turvallisia, luotettavia ja eettisesti kestäviä.

9.3 Tiedolla johtaminen

Rovaniemen tiedolla johtamisen kypsyystasoa tulee edelleen nostaa tietojohdamisen kulttuuriin, työkalujen, resursoinnin ja toimintamallien yhteisen sopimisen kautta. Tietotarpeita ja tietolähteitä on kartoitettu loppuvuodesta 2025. Muutamia tiedolla johtamisen raportteja on julkaistu käyttöön liittyen talouteen ja koulutuspalveluiden tarpeisiin. Tiedolla johtamista edistetään yhteistyössä Lapin Oy:n kanssa. Tietovarastoon siirretään enemmän dataa vuonna 2026, ja priorisoidaan aiemmin kerättyjä tietotarpeita tiedolla johtamisen työn edistämiseksi.

9.4 Tietoturva- ja tietosuojatyön resurssointi

Pilvipalveluiden käytön lisääntyminen, tekoälyn hyödyntäminen, kyberturvallisuuden lisääntyneet riskit, tuleva digilainsäädäntö mm. tiedon avaamiseen liittyvä regulaatio, NIS2 sekä muu kansallinen ja EU-lainsäädäntö asettavat kunnille merkittävää painetta tunnistaa, hallita ja ymmärtää edellä mainittuihin liittyvät tietoturvaan ja tietosuojaan liittyvät ulottuvuudet. Edellä kerrotut muutokset tulevat lisäämään resursoinnin tarvetta tietoturva- ja tietosuojatyössä.

Vuoden 2025 alusta lähtien tietosuojavastaavan tehtävä on ollut kokoaikaisesti täytettynä, jonka myötä resurssia on voitu kohdistaa lakisääteisten velvoitteiden lisäksi myös kaupungin tietosuojatyön kehittämiseen. Tietosuojatoiminnan kehittämistä vahvistamaan kaupunki on myös ostanut tietosuojakonsultoinnin palveluja Netum Oy:ltä.

Rovaniemen kaupungissa tietoturvaluuteen liittyviä tehtäviä hoidetaan pääsääntöisesti oman toimen ohessa. Tilintarkastuksen yhteydessä arvioitiin myös tietohallinnon palveluita ja lausunnossa todettiin, että tietoturvaluuden hallinnan järjestämiseen tulisi kiinnittää huomiota.

Tiedonhallintalaissa on määritelty tietoturvaluussäännökset, joita tiedonhallintayksikössä on toteutettava tiedonhallintalain vaatimusten

toteuttamiseksi. Yhtenäinen tietoturvaluustehtävien kuvaus tukee tiedonhallintalain vaatimusten toteutumista tiedonhallintayksiköissä ja siten edistää digitaalisen turvallisuuden kehittymistä. Noudattamalla tiedonhallintalain vaatimuksia ja annettuja suosituksia tiedonhallintayksiköt voivat määritellä tietoturvastuuden toteuttamisen ja varmistua siitä, että roolikuvaus on tiedonhallintalain vaatimusten mukainen ja että tietoturvaluuden kehittämisen, toteutuksen, valvonnan ja raportoinnin vastuut on määritetty riittävän tarkasti.

Maailman muuttuneen kyberturvallisuus uhkatilanteen vuoksi kaupungin on kiinnitettävä huomioita kyberturvallisuuden valmiuden kohentamiseen, jossa keinoja ovat mm:

- Kaupungin ja palveluntarjoajien väliset sopimukset
- Riskien ja niiden vaikutusten arvioinnit
- ICT-palveluiden auditoinnit
- Viranomaisten kyberturvallisuus toimijoiden verkostoituminen
- Tietohallintoasiantuntijoiden syventävät koulutukset ja kyberturvallisuuden tapahtumat
- Kaupungin sisäiset harjoitukset
- Muut kansalliset harjoitukset, kuten esimerkiksi TAISTO ja KYHA

9.5 Suomi.fi Viestit -palvelun käyttöönotto

Eduskunnan käsittelyssä on hallituksen esitys sähköisen tiedoksiannon ensisijaisuutta viranomaistoiminnassa koskevaksi lainsäädännöksi (HE 124/2025 vp). Hallituksen esityksen pääasiallisena tavoitteena on muuttaa viranomaisten tiedoksiannonmenettelyä koskevaa lainsäädäntöä siten, että jatkossa sellaiset asiakirjat, jotka tulee hallintolain 54 §:n tai erityislainsäädännön perusteella antaa hallinnossa asioivalle tiedoksi, annettaisiin tiedoksi ensisijaisesti hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3.1 §:n 7 kohdassa tarkoitetun viestinvälityspalvelun eli Suomi.fi Viestit -palvelun kautta. Uudistus koskisi asiakirjojen tiedoksiantoa pääasiassa yksityishenkilöille, koska yksityisillä ja julkisilla yhteisöillä ei ole käyttövelvoitetta tiedoksiantoasiakirjojen vastaanottamisessa Suomi.fi Viestit -palveluun. Lakimuutosten seurauksena yksityishenkilöille avattaisiin Suomi.fi Viestit -tilit ilman suostumusta, kun nämä asioivat ensimmäisen kerran sähköisesti viranomaisen sähköisissä asiointipalveluissa, joissa on käytössä Suomi.fi Tunnistautuminen.

Mikäli lakimuutokset hyväksytään eduskunnassa, tulisi Rovaniemen kaupungin lähettää hallintopäätökset (toimielinten päätökset ja viranhaltijapäätökset) sekä hallintoasian käsittelyyn liittyvät ilmoitukset, kutsut ja muut asian käsittelyyn vaikuttavat asiakirjat sähköisesti asioivalle yksityishenkilölle ensisijaisesti Suomi.fi Viestit -palveluun. Jotta asiakirjojen tiedoksianto olisi mahdollista Suomi.fi Viestit -palveluun edellyttää tämä, että:

- Tietojärjestelmässä, josta asiakirjat annetaan tiedoksi asioijalle, on rajapinta Digi- ja väestötietoviraston ylläpitämään Suomi.fi Viestit -palveluun.
- Asian käsittelijällä on tiedossa asioijan henkilötunnus, koska tämä tarvitaan, että asiakirjat saadaan teknisesti lähetettyä Suomi.fi Viestit -palveluun oikealle henkilölle.

9.6 ICT-palveluiden uudelleenjärjestämisen selvitys

Rovaniemen kaupunki on hankkinut ulkopuolisen konsultin tekemään selvityksen ja suunnitelman siitä, kuinka Rovaniemen kaupungin tietohallinto- ja ICT-palvelut tulisi järjestää tulevaisuudessa, huomioiden pilvipalveluiden laajan hyödyntämisen.

Selvityksen tavoitteena on, että tulevaisuudessa kaupungin ICT-palvelut ovat:

- kustannustehokkaammin tuotettuja
- ICT-arkkitehtuuriltaan selkeämmät
- paremmin hallittavissa

Tavoitteena on, että tulevaisuuden ICT-kokonaisuus ja osa-alueet ovat tehokkaasti kilpailutettavissa. ICT-palveluiden uudelleen järjestämisen selvitys mahdollistaa tarveperusteisten, kustannustehokkaiden ja tietoturvallisten ICT-palveluiden hankinnan, mutta antaa myös kattavan kuvan ICT-palveluiden nykyisen ympäristön kehityskohteista, mikäli ICT-palvelutuotantoa ei päätetä lähteä uudelleen järjestämään. Selvitys on valmistunut syyskuussa 2025.