

RANTASALMI



pieni kylä - suuri sydän

TIETOTILINPÄÄTÖS 2024

Yhteistyötoimikunta 13.3.2025 §6

Kunnanhallitus 31.3.2025 §

Kunnanvaltuusto 14.4.2025 §

Sisällys

1	Tietotilinpäättöksen tarkoitus	2
2	Tietosuoja ja tietoturvallisuuden toteuttaminen	2
2.1	Henkilöstön koulutus	3
2.2	Tietosuojaohjeet	4
3	Tiedonhallinta, tietovarannot ja tietovirrat.....	4
3.1	Tietojärjestelmien käyttöoikeudet	4
3.2	Kunnan tietoturvan ja toimialueen modernisointi	4
4	Rekisteröidyn oikeudet ja niiden toteutuminen.....	5
5	Seuranta ja mittaaminen	5
6	Arviointi ja kehittäminen	5

1 Tietotilinpäätöksen tarkoitus

Rantasalmen kunnan tietotilinpäätös laaditaan osana tilinpäätöstä ja sen tarkoitus on kuvata ja arvioida tietosuojan ja tietoturvan tilannetta Rantasalmen kunnassa. Se toimii sisäisen ja ulkoisen valvonnan raporttina, johdon työvälineenä sekä luottamuksen osoituksena rekisteröityjen ja sidosryhmien suuntaan.

Tietotilinpäätöksellä vastataan EU Yleinen tietosuoja-asetuksen osoitusvelvollisuuteen (artikla 24, Rekisterinpitäjän vastuu). Organisaation tulee osoittaa noudattavansa asetusta, lakia ja tietosuojaperiaatteita henkilötietojen käsittelyssä sekä toimivansa niin myös käytännössä. Rekisterinpitäjä vastaa osoitusvelvollisuuden toteuttamisesta.

Rantasalmen kunnan organisaatiossa noudatetaan kunnanhallituksen 2.10.2023 hyväksymää tietosuoja- ja tietoturvapoliittikkaa. Tietosuojan koordinointi ja kehittäminen toteutuvat alueellisessa ja Rantasalmen kunnan omassa tietosuojatyöryhmässä.

Tietotilinpäätöksen laatimisesta vuoden 2024 osalta vastaa hallintojohtaja ja se on oltava kommentoitavana Rantasalmen kunnan yhteistyötoimikunnassa.

Tietotilinpäätös laaditaan kerran vuodessa tilinpäätöksen yhteydessä.

2 Tietosuojan ja tietoturvallisuuden toteuttaminen

Suomessa kansallisena valvontaviranomaisena toimii tietosuojavaaltuutettu.

Toiminnassaan tietosuojavaaltuutettu on itsenäinen ja riippumaton.

Tietosuojavaaltuutettu on Euroopan tietosuojaneuvoston jäsen.

Rantasalmen kunta ottaa huomioon toiminnassaan tietosuoja vaatimukset perustuen EU:n yleiseen tietosuoja-asetukseen (GDPR) ja kansalliseen tiedonhallintalakiin.

Velvoitteiden mukaisesti kuntaan on perustettu tietoturva- ja tietosuojatyöryhmä. Ryhmän puheenjohtajana toimi hallintojohtaja.

Kunnan tietosuoja- ja tietoturvapoliittikka sekä ICT-päätelaitteiden ja tietojärjestelmien käyttöperiaatteet sisältävät:

- Tietoturvan ja tietosuojan periaatteet
- Tietoturva
 - Tietojärjestelmät
 - Tietoturvan hallinnolliset periaatteet
 - Henkilöstöturvallisuus
 - Fyysinen tietoturva
 - Tietoaineistoturvallisuus
 - Laitteistoturvallisuus
 - Ohjelmistoturvallisuus
 - Tietoliikenneturvallisuus
 - Käyttöturvallisuus ja käyttöoikeudet
 - Hankinta ja toimittajahallinta

- Etätyö
 - Seuranta, valvonta ja raportointi
- Tietosuoja
 - Henkilötietojen kerääminen ja käsittely
- Tietoturvariskeihin varautuminen
 - Riskien arviointi
 - Koulutus ja tietoisuuden lisääminen
 - Tietoturvapoikkeamat
- Vastuut ja organisointi

Tietoturvaliikenne tukee Rantasalmen kunnan strategian mukaisesti palvelujen tuottamista asiakaslähtöisesti, tehokkaasti ja turvallisesti. Henkilötietojen käsittelyä ohjaa riskiperusteinen sisäänrakennetun tietosuojan periaate edellyttäen, että tietosuojaperiaatteet ovat osana henkilötietojen käsittelyä niiden kaikissa vaiheissa.

Lukollinen tietoturva-astia on käytössä kunnanvirastolla. Koululla ja lukiolla on paperisilppurit. Kaikki arkaluonteinen asiakirjamateriaali laitetaan tietoturva-astioihin tai asiakirjasilppureihin. Tietoturva-astioiden tyhjennyksestä ja materiaalin tietoturvallisesta hävittämisestä vastaa L&T Ympäristöpalvelut Oy. Hävitysprosessi varmistaa, ettei arkaluontoinen tieto päädy väärin käsiin.

Outlook -sähköpostissa on käytössä Microsoft 365 salattu sähköposti. Pääsääntönä voidaan ajatella, että sähköposti pitää salata aina, kun se sisältää arkaluontoista tietoa. Rantasalmen kunnan Microsoft 365-tileissä on käytössä monivaiheinen tunnistautuminen. Monivaiheinen tunnistautuminen (MFA; multifactor authentication, *suom. monivaiheinen todentaminen*) on käyttäjän tunnistamiseen käytettävä tapa, jossa käytetään kahta tai useampaa keinoa tunnistaa käyttäjä tämän kirjautuessa tiettyyn järjestelmään tai palveluun.

Lisäksi käyttöön on otettu turvasähköpostin lähettämiseen ja vastaanottamiseen hankittu järjestelmä, tietoturvallinen työtila sekä vahvan tunnistautumisen vaativa sähköinen lomakeratkaisu.

Vuonna 2024 ICT-ympäristön osalta otettiin käyttöön laiterakisteri.

2.1 Henkilöstön koulutus

Kunnan henkilökunta sekä luottamushenkilöt on veloitettu suorittamaan vuosittain tietoturva- ja tietosuoja -koulutus eOppiva -koulutusjärjestelmässä. Henkilökunta on suorittanut vähintään Tietosuojan ABC julkishallinnon henkilöstölle ja Tietosuojan ABC 2- Syvemälle tietosuojaan -osiot. Lisäksi vapaaehtoisesti on voinut tehdä omaan toimialaan liittyviä koulutusosioita.

Kunnanviraston henkilökunnalle on lisäksi järjestetty Frendyn kautta tietoturva-koulutus sekä SamiEdun kautta hallinnon digitaito- ja tietotekniikkakoulutus, jossa on suoritettu Tieke-merkkejä.

Johtavat viranhaltijat, kunnan tietosuojavaikuttavan yhteyshenkilö ja SamiEdun teknisenä asiantuntijana osallistuivat Digi- ja väestöviraston järjestämään Digitaalisen turvallisuuden Taisto-harjoitukseen 28.11.2024. Taisto on kaikille julkisen sektorin organisaatioille avoin ja maksuton harjoitus, jossa organisaatiot pääsivät valmiiseen harjoitukseen testaamaan ja kehittämään omia toimintatapojaan kuvitteellisten häiriötilanteiden kautta. Taisto tarjosi turvallisen tilaisuuden harjoitella, testata ja kehittää organisaation omia digiturvan

toimintamalleja poikkeuksellisissa olosuhteissa. Harjoitus keskittyi erityisesti häiriötilanteiden hallintaan, johtamiseen ja viestintään. Kokemukset harjoituksesta olivat tietoa lisäävät ja hyödylliset.

Luottamushenkilöille pidettiin koulutus Dynasty 10 asianhallinnan kokoustyötilan (CloudMeeting) käytöstä sekä hyväksyttiin Luottamushenkilön muistilista (valtuusto 4.11.2024 § 86) vahvistamaan luottamushenkilöiden tietojen käsittelyn käytäntöjä.

Kaikki luottamushenkilöt ovat saaneet käyttäjätunnukset järjestelmään.

2.2 Tietosuojaohjeet

Rantasalmen kunnan tietosuoja ja tietoturva ohjaa tietosuojaan ja tietoturvaan liittyvien lakien lisäksi paikalliset ohjeet ja säännöt:

- Rantasalmen kunnan tietosuoja- ja tietoturvapoliittika
- Rantasalmen kunnan asiakirjajulkisuuskuvaukset
- eri tietojärjestelmäkohtaiset ohjeet

Tietosuojaohjeet on päivitetty ja löytyvät kunnan henkilöstön käyttöön tarkoitetusta intrasta. Yleisiä tietosuojaohjeita löytyy eOppiva-oppimisympäristöstä koko henkilökunnan ja luottamushenkilöiden luettaviksi.

3 Tiedonhallinta, tietovarannot ja tietovirrat

Rantasalmen kunnassa on vuonna 2024 käytössä tietojärjestelmäluettelon mukaiset tietojärjestelmät, joissa käsitellään henkilötietoja. Tietojärjestelmäluettelo on ylläpidettävänä omana asiakirjanaan, josta selviää tietojärjestelmän tarkoitus, vastuuyksikkö, pääkäyttäjä, toimittaja, tuki sekä tietosuoja koskevat vaatimukset.

Rantasalmen kunnan tiedonhallinnan, tietovarantojen sekä niihin liittyvien tietovirtojen kokonaistilanteen kuvausta ei ole vielä laadittu, mutta tietojärjestelmäluettelo on ja sitä on hyödynnetty henkilötietojen kartoituksessa.

Vuonna 2024 tehtiin Rantasalmen kunnan tekoälylinjaus (hallintojohtajan päätös 26.3.2024 § 23/2024) ohjaamaan tekoälyn suositeltua käyttöä kunnassa.

Vuoden 2024 aikana on toteutettu asianhallintajärjestelmän tiedonhallinnan kehittämissuunnitelmaa yhdessä konsultin kanssa. Tiedonhallinnan kehittämissuunnitelman keskeisimpänä sisältönä on ollut asian elinkaaren kokonaisuuden ymmärtäminen ja asianhallintajärjestelmän tehokkaampi käyttö.

Digitiekartta ja sen hyväksymisen (pätös kh 20.5.2024 § 137) mukainen eteneminen ja seuranta on osa tietotilinpäätöstä. Digitiekartta on tietotilinpäätöksen liitteenä.

3.1 Tietojärjestelmien käyttöoikeudet

Vuoden 2024 alusta käyttöön on valmistunut tietojärjestelmien käyttöoikeuslomake, jolla esihenkilöt voivat hakea käyttöoikeudet ja roolit alaisilleen. Pyyntöjä toteutetaan jatkossa pääsääntöisesti vain esihenkilöiden pyynnöstä. Lisäksi on suoritettu Microsoft Entra ID ja M365:n pääsyoikeuksien katselmus, jossa käytiin läpi tietojärjestelmien käyttöoikeudet sekä käyttäjien roolit. Kaikki turhat käyttäjätunnukset ja roolit poistettiin.

3.2 Kunnan tietoturvan ja toimialueen modernisointi

Vuoden 2024 aikana vanha JJR-kuntayhteinen ICT-ympäristö on ajettu hallitusti alas ympäristön palvelujen jäätyä tarpeettomiksi järjestelmien siirtyessä pilviratkaisuiksi. Asianhallinnan keskeinen järjestelmä siirrettiin järjestelmäntarjoajan käyttöpalveluun ja järjestelmiin otettiin käyttöön Entra ID-pohjainen kertakirjautuminen.

Microsoft 365-ympäristössä otettiin käyttöön Traficomien suosittelemien tietoturvaa koskevien M365-tietoturvaa lisäävät asetukset. Tekniseen tietoturvaan tehtiin panostuksia keskitetyn päätelaitehallinnan ja sekä kunnan tietoliikenne- ja tietoliikenneoperaattorimuutoksella. Lisäksi vuonna 2024 tarpeettomista tietoliikenneliittymistä ja vanhentuneista tietoliikennelaitteista luovuttiin.

Kunnantalon, päiväkodin ja yhtenäiskoulun monitoimilaitteissa on käytössä turvatulostus, jolloin tulostetut asiakirjat saa tulostimelta vain tunnisteen kanssa. Tällä estetään, ettei arkaluontoisia asiakirjoja jää kopiokoneeseen ilman valvontaa.

4 Rekisteröidyn oikeudet ja niiden toteutuminen

Rantasalmen kunta noudattaa henkilötietojen käsittelyssä läpinäkyvyyttä ja tietojen täsmällisyyttä asetuksen mukaisesti (artikla 5). Informointivelvoitteen täyttämiseksi käytetään toistaiseksi tietosuojaselosteita. Tietosuojaselosteet löytyvät kunnan nettisivuilta (artiklat 13 ja 14).

Rantasalmen kunnan nettisivuille on avattu tietosuojasivusto asian tiedottamista varten. Kuntaan ei tullut vuoden 2024 aikana yhtään tietopyyntöä henkilötietojen käsittelystä.

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa 72 tunnin kuluessa tietosuojavastaavalle, mikäli loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä silloin, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittaminen (artikla 33) tapahtuu tietosuojavastaavan harkinnan mukaan. Tietoon ei ole tullut yhtään tietoturvaloukkausta vuoden 2024 aikana.

5 Seuranta ja mittaaminen

Henkilökunnan tietosuojakoulutustautumista eOppiva-koulutusympäristössä seurataan säännöllisesti ja tarvittaessa muistutetaan testin suorittamisesta. Henkilökunnalle annetaan ohjeita henkilötietojen käsittelystä ja niiden noudattamista seurataan. Tietojärjestelmien pääkäyttäjät huolehtivat, että henkilöstön käyttövaltuudet ohjelmissa pidetään ajan tasalla.

Tietosuojavastaava pitää kirjaa tietopyynnöistä ja tietosuojapoikkeamista. Tietojen kalasteluviestejä tulee aika ajoin sähköpostiin. Niistä on varoitettu henkilökuntaa sekä annettu tarvittaessa toimintaohjeita.

Tiedonhallintamallin laadinnassa on täydennetty tietojärjestelmälistauksia,

määritelty tietojärjestelmien omistajia ja tunnistettu tarvittavaa kuvausdokumentaatiota.

Tietosuojaselosteita päivitetään tarpeen mukaan ja ajantasaiset tietosuojaselosteet julkaistaan kunnan verkkosivulla.

Sopimukset henkilötietojen käsittelystä kuntayhteistyössä (Juva, Joroinen ja Sulkava) ja sidosryhmätyöskentelyssä (Järvi-Saimaan Palvelut Oy) on saatu hyväksytyiksi yhteistyötahojen kanssa.

Organisaatiolla on velvoitteita kuvata erilaisilla mittareilla toimintaansa. Osa mittaristoista palvelevat organisaation omaa tarvetta ja osa mittareista ovat sellaisia, joita joudutaan raportoimaan muulla. Ilman mittareita on vaikea tietää, miten organisaatio on kehittynyt ja mitä osa-alueita tulee vielä kehittää.

Rantasalmen kunnassa on tarpeen ottaa käyttöön alla kuvatut mittarit, koska aiemmin luotettavaa ja mitattavissa olevaa vertailuaineistoa ei ole käytettävissä. Mittareiden avulla pystytään seuraamaan henkilöstön koulutuksiin osallistumista ja oman tietosuojasaamisen kehittämistä.

Tietohallinnon osalta on kartoitettu henkilöstön käytössä olevaa tietotyön vaatimaa kalustoa ja sitä varten on hankittu irtaimiston hallintaan suunniteltu ohjelmisto, josta on saatavissa ajan tasaista tietoa matkapuhelimien ja työasemien määristä.

Tärkeänä arvioinnin seurantakohteena esiin on noussut riskien arviointi ja siihen liittyvä tarkastus. Kunnan käytössä olevaan riskienhallintajärjestelmään on lisätty myös tietosuoja- ja tietoturvariski-osio, josta saadaan mitattavissa olevaa tietoa.

Mittarit:

Tunnusluku	Mittari	Hallinto ¹	Varhaiskasvatus	Opetustoimi	Luottamushenkilöt
Osaaminen ja ohjeistus					
Henkilöstön koulutukset	%	71	40	82	42

Tunnusluku	Mittari	Hallinto ¹	Varhaiskasvatus	Opetustoimi	Luottamushenkilöt
Tietohallinto					
Työasemat	lkm	38	9	221	25
Käyttäjien (Entra ID-tunnuksia)	lkm	29	18	56	30
Matkapuhelimia	lkm	45	11	21	

Tunnusluku	Mittari	Hallinto ¹	Varhaiskasvatus	Opetustoimi
Riskien arviointi ja tarkastukset				
Tehdyt riskianalyytit	lkm	1 ²		
Tehdyt vaikutustenarvioinnit	lkm	1		1

¹ hallintopalvelut, hyvinvointi, nuoristoimi, kirjastotoimi, tekninen ja ympäristö, maaseutuhallinto

² Kunnanviraston tietoliikenne

Tehdyt ennakkokuulemiset	lkm			
Tehdyt turvallisuusselvitykset	lkm	2		
Tehdyt tarkastukset ja omavalvonta	lkm			

Keskeisimmät tietoturva- ja tietosuojapoikkeamat havaittiin, kun tietoliikennekumppanin edustaja paljasti vahingossa hallinnon wlan-verkon salasanan sekä muutamia vuosia sitten kesken jäänyt kirjastojen looginen erottaminen ja kiinteistöautomaation vajavainen dokumentaatio paljastuivat tietoliikenneoperaattorin vaihdon yhteydessä. Lisäksi tietotekniikkakumppanin laatuhaasteet muodostivat potentiaalisen tietosuojauhkan. Kaikki tietoon tulleet tapaukset on käsitelty ja niiden osalta on tehty korjaus- ja parannustoimenpiteet.

6 Arviointi ja kehittäminen

Henkilökunnan ja luottamushenkilöiden tietosuoja- ja tietoturvakoulutukset toteutettiin ensimmäisen kerran vuonna 2023 Rantasalmen kunnassa. Tarkoituksena on toteuttaa koulutukset vuosittain ja kasvattaa tietosuoja- ja turvallisuuskulttuuria.

Tietosuoja- ja tietoturvapoliittikan mukaisten koulutusten suorittaminen 2024-kunnanjohtajan viranhaltijapäätös (10.6.2024 § 17/2024) ohjaa koko kunnan henkilöstöä ja luottamushenkilöitä huolehtimaan tietosuojakoulutuksen ajan tasalla pitämisestä. Tietosuojakoulutusten suorittamatta jättäminen lisää osaltaan tietosuojan ja tietoturvan riskejä organisaatiossa.

Käyttäjiä muistutetaan edelleen ottamaan huomioon tietosuoja- ja tietoturvalliset toimintatavat työskentelyssään. Henkilötietoja sisältäviä papereita ei saa jättää pöydälle työpaikalta poistuttaessa niin, että niihin pääsee asiaankuulumattomat käsiksi. Työhuoneiden ovet ja erityisesti työasemat on pidettävä lukittuina, kun työhuoneesta poistutaan. Lähetettäessä sähköpostissa salassa pidettävää tietoa, on käytettävä viestin salausta. Tiedonhallintaa ja turvallista jakelua varten kuntaan on rakennettu henkilöstölle ja luottamushenkilöille omia intranet-ratkaisuja. Kokoushallintaa tullaan keskittämään entistä enemmän sähköisiin ympäristöihin.

1.1.2020 voimaan astunut tiedonhallintalaki velvoittaa organisaatioilta tiedon elinkaaren hallinnan perusvaatimusten kuvantamista ja julkistamista yhtenäisenä kokonaisuutena. Kehitetään asianhallintaa niin, että Dynasty 10 asianhallintajärjestelmään kirjataan kaikki saapuneet asiakirjat. Lisäksi huomioidaan, että henkilökohtainen sähköposti ei ole asianhallintajärjestelmä. Asianhallintajärjestelmään kirjataan myös kaikki tietopyynnöt niin, että jokainen tietopyyntö käynnistää uuden aktin eli asian. Kaikki ko. tietopyyntöön liittyvät asiakirjat liitetään asiaan.

Luottamushenkilöiden Dynasty 10 asianhallinnan kokoustyötilan käyttöönottoa jatketaan ja tarvittaessa järjestetään koulutustilaisuus.

Kunnan tietoturva- ja tietosuojatyöryhmä (kunnanjohtajan viranhaltijapäätös 13.8.2024 § 22/2024) kokoontuu säännöllisesti ja pohtii tietosuojan kehittämistä eri toimialoille. Työryhmässä laaditaan tarvittaessa paikallisia tietosuoja- ja tietoturvaohjeita, joita julkaistaan kunnan sisäisessä intrassa henkilöstölle tietoisuina.

Henkilöstön tietoisuutta tietosuoja- ja tietoturva-asioista pyrittiin lisäämään tiedottamalla esimerkiksi Digiturvaviikkojen webinaaritarjonnasta.

Toimittajahallinnalla on keskeinen merkitys tietosuojan ja tietoturvan toteutumisessa niin teknisessä tukipalvelussa kuin muissa kunnalle tai kunnan kanssa tuotettavissa palveluissa.

Tiedonhallintalain vaatimusten mukaisten toimenpiteiden toteuttamista jatketaan vuonna 2025. Vuoden 2025 loppuun mennessä tavoitteena on asiakirjajulkisuuskuvauksen julkaiseminen kunnan verkkosivustolle tarkoitukseen hankitun järjestelmän avulla.

Tietosuojan vuosikello toteutetaan vuoden 2025 aikana, jolloin pystytään ylläpitämään ja seuraamaan tietosuojan kehittymistä kuntaorganisaatiossa.