

RANTASALMI



pieni kylä - suuri sydän

TIETOTILINPÄÄTÖS 2023

Yhteistyötoimikunta 22.2.2024 § xx

Kunnanhallitus 18.3.2024 § xx

Kunnanvaltuusto 22.4.2024 § xx

Sisällys

1	Tietotilinpäätöksen 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 tietosuoja- 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. Tietosuoja- ja tietoturvan kehittäminen toteutuvat alueellisessa ja Rantasalmen kunnan omassa tietosuojatyöryhmässä.

Tietotilinpäätöksen laatimisesta vuoden 2023 osalta on vastannut hallintojohtaja ja se on ollut kommentoitavana Rantasalmen kunnan yhteistyötoimikunnassa. Tietotilinpäätös laaditaan kerran vuodessa tilinpäätöksen yhteydessä.

2 Tietosuoja- ja tietoturvallisuuden toteuttaminen

Suomessa kansallisena valvontaviranomaisena toimii tietosuojavaltuutettu. Toiminnassaan tietosuojavaltuutettu on itsenäinen ja riippumaton. Tietosuojavaltuutettu 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 tietosuojatyöryhmä. Ryhmän puheenjohtajana toimi hallintojohtaja.

Rantasalmen kunnan tietoturvaa ja tietosujaa ohjaa kunnanhallituksen 2.10.2023 hyväksymä tietoturvapoliittikka, joka on laadittu keskeisen lainsäädännön mukaisesti.

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

- Tietoturvan ja tietosujan 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

Tietoturvapoliittikka 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 väriin käsiin.

Outlook -sähköpostissa on käytössä Microsoft 365 salattu sähköposti. Pääsääntönä voidaan ajatella, että sähköposti pitää salata aina, kun se sisältää arkaluontoista tietoa. Rantasalmen kunnan Office 365 -tileissä ei ollut 2023 käytössä monivaiheista tunnistautumista. Monivaiheinen tunnistautuminen (MFA; multifactor authentication, suomeksi monivaiheinen todentaminen) on käyttäjän tunnistamiseen käytettävä tapa, jossa käytetään kahta tai useampaa keinoa tunnistaa käyttäjä tämän kirjautuessa tiettyyn järjestelmään tai palveluun.

2.1 Henkilöstön koulutus

Kunnan henkilökunta sekä luottamushenkilöt on veloitettu suorittamaan vuosittain tietoturva- ja tietosuoja -koulutus eOppiva -koulutusjärjestelmässä. Henkilökunta suorittaa vähintään Tietosuojan ABC julkishallinnon henkilöstölle ja Tietosuojan ABC 2- Syvemmälle tietosuojaan -osiot. Lisäksi vapaaehtoisesti voidaan tehdä omaan toimialaan liittyvä koulutusosio.

Vuonna 2023 pakolliset koulutukset suorittanut henkilöstö:

	suorittaneiden %-osuus
Hallinnon henkilöstö	83
Varhaiskasvatuksen henkilöstö	84
Opetustoimen henkilöstö	5
Luottamushenkilöt	17

Kunnan poikkeusolojen johtoryhmä osallistui Digi- ja väestöviraston (DVV) järjestämään Digitaalisen turvallisuuden Taisto-harjoitukseen 30.11.2023. Suomen suurin digitaalisen turvallisuuden harjoitus Taisto järjestettiin kuudetta kertaa. 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.

Henkilöstöä on muistutettu sähköpostitse erilaisten huijausviestin yleistymisestä ja toimintatavoista viestien kanssa.

Luottamushenkilöille pidettiin koulutus Dynasty 10 asianhallinnan kokoustyötilan (CloudMeeting) käytöstä. Kaikki luottamushenkilöt ovat saaneet käyttäjätunnukset järjestelmään.

2.2 Tietosuojaohjeet

Rantasalmen kunnan tietosuojaa ja tietoturvaa ohjaa tietosuojaan ja tietoturvaan liittyvien lakien lisäksi paikalliset ohjeet ja säännöt:

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

Yleisiä tietosuojaohjeita löytyy eOppiva-oppimisympäristöstä koko henkilökunnan ja luottamushenkilöiden luettaviksi.

3 Tiedonhallinta, tietovarannot ja tietovirrat

Rantasalmen kunnassa oli vuonna 2023 käytössä tietojärjestelmäluettelon mukaiset tietojärjestelmät, joissa käsitellään henkilötietoja. Tietojärjestelmäluetteloä ylläpidetään omana asiakirjanaan, josta selviää tietojärjestelmän tarkoitus, vastuuyksikkö, pääkäyttäjä, toimittaja, tuki sekä tietosuojaa koskevat vaatimukset.

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

3.1 Tietojärjestelmien käyttöoikeudet

Vuoden 2023 lopussa käyttöön valmisteltiin tietojärjestelmien käyttöoikeuslomake, jolla jatkossa esihenkilöt voivat hakea käyttöoikeudet ja roolit alaisilleen. Pyyntöjä toteutetaan jatkossa pääsääntöisesti vain esihenkilöiden pyynnöstä. Suoritettiin AD:n 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 2023 aikana vanhaa JJR-kuntayhteistä ICT-ympäristöä on aloitettu ajamaan hallitusti alas ympäristön palvelujen jäätyä tarpeettomiksi järjestelmien siirtyessä

pilviratkaisuiksi. Asianhallinnan keskeinen järjestelmä siirrettiin järjestelmäntarjoajan käyttöpalveluun ja järjestelmiin otettiin käyttöön AAD-pohjainen kertakirjautuminen. Tekniseen tietoturvaan tehtiin panostuksia keskitetyn päätelaitehallinnan ja tietoliikenteen suodatuksen käyttöönotolla. Lisäksi loppuvuonna on valmistauduttu Ad-ympäristön modernisointiin ja tietoturvahavennuksiin mm. käyttäjätunnistuksen kehittämisellä.

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 2023 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 2023 aikana.

5 Seuranta ja mittaaminen

Henkilökunnan tietosuojakouluttautumista 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.

Tietosuojaselosteita päivitetään tarpeen mukaan ja ajantasaiset tietosuojaselosteet julkaistaan kunnan verkkosivulla.

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.

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 on pidettävä lukittuina, kun työhuoneesta poistutaan. Lähetettäessä sähköpostissa salassa pidettävää tietoa, on käytettävä viestin salausta. Tiedonhallintaa ja turvallista jakelua varten kuntaan rakennetaan 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 asiantuntijaa niin, että Dynasty 10 asiantuntijajärjestelmään kirjataan kaikki saapuneet asiakirjat. Asiantuntijajärjestelmään kirjataan myös kaikki tietopyynnöt niin, että jokainen tietopyyntö käynnistää uuden aktin eli asian. Kaikki ko. tietopyyntöön liittyvät asiakirjat liitetään asiaan.

Luottamushenkilöiden Dynasty 10 asiantuntijajärjestelmän käyttöönottoa jatketaan ja tarvittaessa järjestetään koulutustilaisuus.

Tiedonhallintalain vaatimusten mukaisten toimenpiteiden toteuttamista jatketaan vuonna 2024.

Seudullinen tietosuojatyöryhmä kokoontuu joka toinen kuukausi käsittelemään ajankohtaisia tietosuoja- ja tietoturva-asioita. Kokouksissa saadaan ajankohtaista tietoa ja käsitellään yhdessä mahdollisia tietoturvapoikkeamia.

Kunnan oma tietosuojatyöryhmä kokoontuu tarvittaessa ja pohtii tietosuojan kehittämistä eri toimialoille. Laaditaan tarvittaessa paikallisia tietosuoja- ja tietoturvaohjeita, joita lähetetään sähköpostitse henkilöstölle tietoisuutena sekä kirjataan Dynasty 10 asiantuntijajärjestelmään.

Osallistutaan Digi- ja väestöviraston järjestämään Taisto-harjoitukseen vuonna 2024.

Kunnantalon monitoimilaitteeseen hankitaan turvatulostus, jolloin tulostetut asiakirjat saa tulostimelta vain tunnusteen kanssa. Tällä estetään, ettei arkaluontoisia asiakirjoja jää kopiokoneeseen ilman valvontaa.