Rantasalmen kunnan tietosuoja- ja tietoturvapolitiikka sekä ICT-päätelaitteiden ja tietojärjestelmien käyttöperiaatteet

Yhteistyötoimikunta 18.9.2023 § 22

Kunnanhallitus 2.10.2023

Sisällys

1. Yleistä

Rantasalmen kunnan toiminta ja palvelujen järjestäminen perustuvat hyvään hallintoon, julkiseen ja ei-julkiseen tietoon. Ollakseen tehokkaasti hyödynnettävissä, hyvää hallintoa ja tietoa tukevien järjestelyjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tämä edellyttää tehokasta johtamista luotettavien toteutusten ja osaavan henkilöstön tueksi.

Tämä politiikka ja siihen perustuvat ohjeet ja määräykset, koskevat kaikkia kunnan työntekijöitä, luottamushenkilöitä, työryhmiä, toimielimiä ja sidosryhmän edustajaa (esim. palveluntuottajia), joka työnsä tai toimeksiantonsa puitteissa käsittelee kunnan omistamaa tai hallinnoimaa tietoa. Tätä politiikkaa ja tähän perustuvien ohjeita tulee noudattaa aina käytettäessä kunnan laitteita riippumatta käyttöpaikasta tai yhteydestä.

Politiikka toimii perustana kunnan tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden käytäntöön soveltamisessa. Tietosuoja- ja tietoturvapolitiikka ja sen soveltamisohjeet pidetään käyttäjien saatavilla intranetissä.

Kunnan tietosuoja- ja tietoturvatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- Kuntaa velvoittavat lait ja asetukset
- EU:n Yleinen Tietosuoja-asetus (EU) 2016/679
- Kunnan omat strategiat ja niistä johdetut vaatimukset
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)
- Valtionhallinnon Tietoturvallisuuden johtoryhmän (VAHTI) ohjeet
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010).

Kunnanhallitus on hyväksynyt tietosuoja- ja tietoturvapolitiikan.

Tietosuoja- ja tietoturvapolitiikkaa katselmoidaan vuosittain ja tarvittaessa useammin merkittävien muutosten johdosta tietoturva- tai tietosuojakäytännöissä, lainsäädännössä tai viranomaisohjeistuksessa. Katselmoinnin tarkoituksena on varmistaa politiikan ajantasaisuus ja vaikuttavuus. Tietosuoja- ja tietoturvapolitiikan katselmoinnista vastaa tietosuojavastaava.

2. Tietosuoja- ja tietoturvapolitiikan keskeisiä käsitteitä

Tietosuoja	Tietosuoja tarkoittaa perusoikeutta, joka turvaa jokaisen oikeuksia ja vapauksia henkilötietojen käsittelyssä. Tietosuoja määrittelee ne periaatteet, milloin, millä edellytyksillä ja miten henkilötietoja voidaan käsitellä.
Tietoturva	Tietoturvalla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys. Tietoturvaan sisältyy muun muassa tietojen, tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen, tilojen ja toiminnan turvaaminen. Tietoturva liittyy läheisesti tietosuojaperiaatteiden toteuttamiseen.
Luottamuksellisuus	Luottamuksellisuus eli se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Tiedot suojataan luotettavasti ja oikeus käsitellä tietoja perustuu työtehtävien mukaiseen tarpeeseen ja vähimpien oikeuksien periaatteeseen. Tietojen ja järjestelmien käyttäjät tunnistetaan luotettavasti.

Eheys	Eheys eli se, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut. Tietojen ja tietojen käsittelymenetelmien oikeellisuus, laatu ja kiistämättömyys varmistetaan. Tieto suojataan luvattomalta tai vahingossa tapahtuvalta tiedon muuttamiselta tai poistamiselta.
Käytettävyys	Käytettävyys eli se, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Tiedot ja niihin perustuvat palvelut ovat niihin valtuutettujen henkilöiden käytettävissä oikea-aikaisesti.
Henkilötieto	Henkilötietoa on kaikki tieto, joiden avulla henkilö on tunnistettavissa. Henkilö on tunnistettavissa, jos tieto voidaan liittää henkilöön joko suoraan tai välillisesti esimerkiksi yhdistämällä tieto johonkin toiseen tietoon.
Henkilötietojen käsittely	Henkilötietojen käsittely tarkoittaa kaikkia henkilötietoihin kohdistettavia toimia, kuten kerääminen, tallentaminen, säilyttäminen, muokkaaminen, muuttaminen, hakeminen, luovuttaminen ja poistaminen.
Rekisterinpitäjä	Rekisterinpitäjä tarkoittaa ihmistä tai organisaatiota, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot tai jonka tehtäväksi henkilötietojen käsittely on lailla säädetty. Rekisterinpitäjä on vastuussa suorittamastaan henkilötietojen käsittelystä.
Rekisteröity	Rekisteröity tarkoittaa henkilöä, jonka henkilötietoja rekisterinpitäjä käsittelee. EU:n tietosuoja-asetus antaa erilaisia oikeuksia rekisteröidyille henkilötietojen käsittelyperusteesta riippuen.
Henkilötietojen käsittelijä	Henkilötietojen käsittelijä tarkoittaa ihmistä tai organisaatiota, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Esimerkiksi rekisterinpitäjän käyttämä palveluntarjoaja. Henkilötietojen käsittelijällä ei tarkoiteta organisaation omia työntekijöitä.
Arkaluonteinen tieto	Yksilöä tai organisaatiota koskeva tieto, jonka rekisteröintiä ja käyttöä on rajoitettu lain tai asianomaisen vaatimuksesta. EU:n tietosuoja-asetuksen ja Suomen tietosuojalain (1050/2018) mukaan arkaluonteisia ovat henkilötiedot (erityiset henkilötietoryhmät), jotka kuvaavat tai on tarkoitettu kuvaamaan: · rotua tai etnistä alkuperää · henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista · rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta · henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia · henkilön seksuaalista suuntautumista tai käyttäytymistä Lisäksi Julkisuuslaissa (621/1999) mainittuja salassa pidettäviä tietoja (§24) voidaan pitää arkaluonteisina henkilötietoina, kuten henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Tekniset ja organisatoriset toimet	Teknisillä ja organisatorisilla toimilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutusta, ohjeita ja määräyksiä, salassapitosopimuksia, tilavalvontaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, auditointeja, teknisiä rajoituksia ja kontrolleja, tarkastus- ja valvontajärjestelmiä, käytännesääntöjä ja sertifikaattien käyttöönottoa.
Henkilötietojen tietoturvaloukkaus	Henkilötietojen tietoturvaloukkaus (”tietosuojaloukkaus”) on erheellistä tietojen käsittelyä, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen käyttäminen, tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.
Tietoturvaloukkaus (tekninen)	Tekninen tietoturvaloukkaus on tietoturvajärjestelmään kohdistuva fyysinen tai tekninen loukkaus. Tyypillisiä tietoturvaloukkauksen muotoja ovat esimerkiksi tietomurto, palvelunestohyökkäys ja haittaohjelmat. Tietoturvaloukkauksessa organisaation tietojärjestelmän tietoihin murtaudutaan tai tunkeudutaan ja varastettua tietoa käytetään hyväksi. Tietoturvaloukkaus ei siis aina kohdistu henkilötietoihin.
Tietosuojan vaikutustenarviointi	Tietosuojan riskejä on arvioitava aina, kun henkilötietoja käsitellään. Tietosuojan vaikutustenarviointi on ennen henkilötietojen käsittelyn aloitusta tehtävä arvio, jossa arvioidaan tarkemmin suunnitellun käsittelyn sisältöä, oikeasuhtaisuutta suhteessa rekisteröityyn ja henkilötiedoille aiheutuvia riskejä. Vaikutustenarviointi on tehtävä, mikäli käsittelystä todennäköisesti aiheutuu korkea riski luonnollisen henkilön oikeuksille ja vapauksille.
Päätelaite	Päätelaitteilla tarkoitetaan käytännössä kaikkia laitteita, jotka voi kytkeä tietoverkkoon. Työntekijäkohtaisia päätelaitteita ovat esimerkiksi tietokone ja matkapuhelin.

3. Tietosuoja- ja tietoturvapolitiikan merkitys

Tietosuoja- ja tietoturvapolitiikka on ylin tietosuojan ja tietoturvan toteutusta ja hallintaa määrittävä dokumentti. Tietoturvallisuuden tavoitteena on tukea Rantasalmen kunnan strategisten tavoitteiden toteutumista sekä tukea kokonaisturvallisuutta ja turvallisuuskulttuuria.

Tietosuojan osalta tavoitteena on määritellä ne keinot, joilla Rantasalmen kunta osoittaa noudattavansa henkilötietojen käsittelyssä tietosuoja-asetusta ja muuta henkilötietojen käsittelyyn soveltuvaa lainsäädäntöä.

Rantasalmen kunnan tietosuoja- ja tietoturvapolitiikka määrittää periaatteet, toimintatavat, vastuut ja valvonnan, joita noudatetaan Rantasalmen kunnan tietosuojan ja tietoturvan toteuttamisessa, kehittämisessä ja suojaamisessa.

Tietoturvallisuus perustuu lainsäädäntöön, normiohjaukseen ja sopimuksiin. Tietosuoja- ja tietoturvapolitiikan soveltaminen ei ole sidoksissa tiedon muotoon tai sen käsittely- tai esitystapaan ja sitä sovelletaan kaikkiin tiedon elinkaaren eri vaiheisiin.

Tietosuoja- ja tietoturvapolitiikan mukaisia periaatteita ja niiden soveltamista voidaan tarkentaa linjauksilla ja vaatimuksilla, käytännöillä, ohjeistuksilla ja muulla tietosuojan ja tietoturvan dokumentaatiolla.

4. Tietosuoja ja tietoturvan roolit ja vastuut

Tietosuojan ja tietoturvan roolit ja vastuut jakautuvat Rantasalmen kunnassa alla olevan taulukon mukaisesti. Mikäli kunnan hallinto- tai muissa säännöissä ei ole määritelty kenelle roolin vastuu kuuluu, on hallintopäällikkö vastuussa tehtävän osaamisvaatimukset parhaiten täyttävän henkilön nimeämisestä kyseiseen rooliin.

Rantasalmen kunnan henkilötietorekisterien listaus ja rekisterien yhteyshenkilöt löytyvät kunnan julkisilta internetsivuilta. Kunnan sisäinen tietosuojadokumentaatio julkaistaan organisaation sisäisissä kanavissa.

Kunnanhallitus	Vastaa tietosuoja-asioiden ja tietoturvan johtamisesta ja resursoinnista sekä valvonnasta.
Kunnanjohtaja	Toimii tietosuojan ja tietoturvan omistajana kunnassa luoden edellytykset tietoturvan asianmukaiselle toimeenpanolle. Tarvittaessa kunnanjohtaja asettaa ryhmän seuraamaan tietoturvan ja -suojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan toimialojen tietosuojavastaavien sekä järjestelmien pääkäyttäjien tukena.
Tietosuoja- ja tietoturvatyöryhmä	Työryhmän tehtävänä on seurata tietosuojan ja tietoturvan toteutumista, tehdä kehitysehdotuksia ja toimia tietosuojavastaavan sekä järjestelmien pääkäyttäjien tukena. Työryhmä toimii tietosuojan kehityksen asiantuntijana ja edistäjänä organisaatiossa sekä sovittaa yhteiset mallit oman organisaation toimintaan. Vastaa tietoturvaprosessien ohjauksesta ja integroimisesta muihin kokonaisturvallisuuden osa-alueisiin sekä tietoturvaa koskevasta viestinnästä johdolta saamiensa resurssien ja toimivaltuuksien puitteissa. Tehtävään sisältyy tietoturvatyön suunnittelu, ohjeistus, seuranta ja kehittäminen sekä tietoturvariskien ja -poikkeamien hallinnan koordinointityöryhmä ja tietotekniikan palveluntuottajat työryhmän ohjeistamana vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin. Työryhmän puheenjohtajana toimii hallintopäällikkö.
Tietosuojavastaava	Rantasalmen kunnalle nimetty tietosuoja-asetuksen mukainen tietosuojavastaava on ilmoitettu tietosuojasta vastaavalle valvontaviranomaiselle. Tietosuojavastaavan tehtäviin kuuluu tietosuoja-asetuksen mukaiset lakisääteiset tehtävät.

	Tietosuojavastaava neuvoo henkilötietojen lainmukaisessa käsittelyssä, valvoo tietosuojalainsäädännön ja hyvien tietosuojakäytänteiden noudattamista ja toimii yhteyspisteenä valvontaviranomaiselle. Tietosuojavastaava ylläpitää kunnan tietoutta tietoturvallisuuteen ja tietosuojaan vaikuttavista laeista, säädöksistä ja määräyksistä, sekä huolehtii niiden huomioimisesta tietoturvallisuus- ja tietosuojatyössä. Tietosuojavastaava raportoi tietosuojan toteutumisesta kunnan ylimmälle johdolle.
Toimialan johto	Vastaa tietosuojan ja tietoturvallisuuden toteutuksesta johtamansa toiminnan osalta ja siitä, että järjestelmien omistajat sekä pääkäyttäjät on nimetty.
Esihenkilöt	Vastaavat tietoturvan toteutumisesta alaisessaan toiminnassa. Esihenkilöt raportoivat näistä asioista toimialajohdon lisäksi tietoturvatiimille.
Viranhaltijat, työntekijät, luottamushenkilöt ja muut palvelussuhteeseen rinnastettavat henkilöt	Vastaavat omalta osaltaan tietosuojan ja tietoturvan toteutumisesta omissa työtehtävissään. Jokaisen vastuulla on havaitsemiensa tietosuojaan ja tietoturvaan liittyvien uhkien, riskien tai rikkomusten ilmoittaminen viipymättä esihenkilölle, palvelusta tai toiminnasta vastuulliselle taholle ja tietosuojavastaavalle.
Tytäryhteisöjen hallitukset ja toimitusjohtajat	Vastaavat tietosuojan ja tietoturvallisuuden toteutumisesta sekä kokonaisturvallisuuden toteutumisesta omissa organisaatioissaan.
Tiedon, tietojärjestelmän tai palvelun omistaja	Vastaa omistukseensa liittyvästä käyttäjien ja heidän käyttöoikeuksiensa määrittelystä ja hyväksynnästä, riskienhallinnan toteuttamisesta, tiedon eheyden varmistamisesta, tietojen luokittelusta (julkisuuden ja salassapidon määrittely sekä arkistonmuodostus), tiedon hävittämisestä ja käyttöönoton tai muutosten vaatimista sääntelyn velvoittamien menettelyjen huomioinnista sekä rekisteriselosteen tai tietoturvaselosteen laadinnasta ja nimeää rekisterin yhteyshenkilön.
Tietojärjestelmän pääkäyttäjä	Valvoo tietoturvan ja käyttöoikeuspolitiikan toteutumista omalla vastuualueellaan. Pääkäyttäjä huolehtii sovelluksen ylläpitotoiminnoista ja toimii yhdyshenkilönä järjestelmätoimittajaan. Pääkäyttäjä tiedottaa käyttäjiä vikatilanteista ja käyttökatkoista ja huolehtii käyttökatkojen aikataulutuksista.
Kunnan keskushallinto	Ohjaa ja koordinoi henkilöstöturvallisuutta sekä henkilötietojen käyttöä työsuhteen kaikissa vaiheissa (kuten työsuhteen solmiminen, perehdytys, työsuhteen päättäminen).
Kunnan arkisto	Ohjaa ja neuvoo yksiköiden arkistonmuodostusta sekä huolehtii ja antaa tietoja kunnan arkistoon siirretyistä asiakirjoista.
Hankintoja ja sopimuksia tekevät	Vastaava siitä, että tietosuojan ja tietoturvallisuuden taso vastaavat hankittavien tuotteiden, palveluiden ja kumppanuus- ja ulkoistusratkaisujen osalta kunnan vaatimuksia, määräyksiä ja ohjeita.

Viestinnästä vastaava	Tukee tietoturvallisuuteen ja tietosuojaan liittyvästä viestinnästä vastaavia toimijoita
Järjestelmätoimittaja ja palvelun tuottaja	Vastaa tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä heitä velvoittavien sopimusten ja sääntelyn puitteissa sekä asiakaslähtöisestä kehittämisehdotusten tekemisestä tietosuojan ja tietoturvallisuuden toteuttamiseksi.

5. Suunnittelu ja raportointi

Rantasalmen kunta suunnittelee tietosuoja- ja tietoturvatyötä vuosittaista tietosuojan vuosisuunnitelmaa hyväksikäyttäen. Suunnitelmassa tietosuoja- ja tietoturvatyössä toteutettavat tehtävät on jaettu toteutettavaksi pitkin vuotta. Vuosisuunnitelman pohjalta tehtäviä voidaan delegoida vastuussa oleville tahoille. Tietosuojaa ja tietoturvaa koskevien toimenpiteiden suunnitelmat voivat olla erilliset.

Vuoden lopussa kunnan tietosuojatyö kootaan tietotilinpäätökseen. Tietotilinpäätös on kunnan tilinpäätöksen liitteenä, jonka hyväksyy kunnan valtuusto.

6. Henkilötietojen käsittelyn periaatteet

Rantasalmen kunta noudattaa asiakkaiden, kuntalaisten, kunnan henkilöstön ja muiden sidosryhmien henkilötietojen käsittelyssä voimassa olevaa lainsäädäntöä. Rantasalmen kunta noudattaa alla olevia tietosuoja-asetuksen mukaisia henkilötietojen käsittelyn periaatteita kaikessa henkilötietojen käsittelyssä.

Lainmukaisuus, asianmukaisuus ja läpinäkyvyys	Henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta ja muuta henkilötietojen käsittelyyn soveltuvaa sääntelyä. Henkilötietoja käsitellään asianmukaisesti ja kohtuullisesti suhteessa käsittelyn tarkoituksiin, ottaen huomioon informointivelvollisuus ja käyttötarkoitussidonnaisuus. Käsittelystä kerrotaan rekisteröidyille selkeällä ja ymmärrettävällä tavalla.
Käyttötarkoitussidonnaisuus	Henkilötietojen käsittely suunnitellaan etukäteen ja käsittely perustuu aina tiettyyn selvästi määritettyyn ja nimenomaiseen sekä lailliseen tarkoitukseen. Henkilötietoja ei käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin. Uusista käyttötarkoituksista kerrotaan rekisteröidylle ennen käsittelyn aloittamista.

Täsmällisyys, minimointi ja säilytyksen rajoittaminen	Henkilötietojen oikeellisuus pyritään varmistamaan. Virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Henkilötietoja kerätään ja käsitellään vain siinä määrin, kuin on tarkoituksenmukaista ja välttämätöntä tarkoitukseen nähden. Käsiteltyjen tietojen tulee olla asianmukaisia eli tiedoille on oltava olemassa määritetty käyttötarkoitus. Tietojen on oltava olennaisia ja rajoitettuja eli välttämättömiä käyttötarkoituksen kannalta. Henkilötietoja säilytetään ainoastaan niin kauan kuin on tarpeen määritetyn käyttötarkoituksen kannalta. Henkilötietojen säilytysajat määritetään ja dokumentoidaan.
Tiedon luottamuksellisuus ja turvallisuus	Tietoja käsitellään luottamuksellisesti ja turvallisesti. Suojatoimenpiteet suhteutetaan arvioimalla käsittelyyn liittyvät riskit ja käsittelyyn liittyvät olosuhteet. Henkilötiedot suojataan teknisillä ja organisatorisilla suojatoimilla asianmukaisen eheyden, luottamuksellisuuden ja turvallisuuden varmistamiseksi, mukaan lukien suojaus luvattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta katoamiselta, tuhoutumiselta tai vahingoittumiselta. Henkilöstön ja sopimuskumppaneiden on noudatettava käsittelyyn liittyviä ohjeita ja tietoturvakäytäntöjä.

Riskiperusteinen lähestymistapa ja riskien hallinta
Rantasalmen kunta noudattaa riskiperusteista lähestymistapaa kaikessa henkilötietojen käsittelyssä ja suunnittelee toimenpiteet sekä suojakeinot suhteuttaen ne käsittelyyn liittyviin tietosuojariskeihin. Henkilötietojen käsittely suunnitellaan ja toteutetaan koko elinkaaren ajan tietosuojaperiaatteiden ja muiden käsittelyyn soveltuvien vaatimusten mukaisesti, jotta sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet toteutuvat.

Rantasalmen kunta arvioi henkilötietojen käsittelyyn liittyviä riskejä toiminnassaan, mukaan lukien uusien järjestelmien hankinta, yhteistyö uusien toimittajien kanssa sekä olemassa olevat käsittelytoimet. Riskitasoa arvioidaan ja lain edellyttämissä tilanteissa käsittelytoimille tehdään tietosuoja-asetuksen mukainen tietosuojan vaikutustenarviointi. Vaikutustenarvioinnin tulosten avulla määritellään hallintakeinoja, joilla henkilötietojen käsittelystä aiheutuvia riskejä minimoidaan.

Sisäänrakennettu ja oletusarvoinen tietosuoja
Rantasalmen kunta noudattaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen mukaisia henkilötietojen käsittelyn periaatteita ja muuta henkilötietojen käsittelyyn soveltuvaa sääntelyä.
Teknisillä ja organisatorisilla toimilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kannalta tarpeellisia tietoja. Tietosuojaperiaatteet huomioidaan kaikessa toiminnassa mahdollisimman varhaisesta vaiheesta lähtien ja riskitasoon nähden asianmukaiset tekniset ja organisatoriset toimenpiteet toteutetaan.

Tietosuojaperiaatteiden noudattaminen henkilötietojen keräämisessä ja käsittelyssä toteutetaan muun muassa varmistamalla, että

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja käsitellään vain suunnitellun käsittelytarkoituksen kannalta
- tietoja ei kerätä suurempia määriä eikä niitä säilytetä kauemmin kuin on välttämätöntä kyseiseen käyttötarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin.

Rekisteröityjen oikeudet
Rantasalmen kunta varmistaa tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisen ylläpitämällä ja kehittämällä tarvittavia käytäntöjä.

Rekisteröityjen oikeudet toteutetaan siten, kuin ne kussakin tilanteessa soveltuvat huomioiden käsittelyn oikeusperusteen ja käsittelytilanteen. Rekisteröityjä informoidaan henkilötietojen käsittelystä läpinäkyvästi. Rekisteröidyllä on käsittelyn oikeusperusteiden mukaisesti oikeus saada tietoa henkilötietojensa käsittelystä, oikeus saada tutustua omiin tietoihinsa, oikaista tietojaan, poistaa tiedot, rajoittaa tietojensa käsittelyä, siirtää tiedot järjestelmästä toiseen, vastustaa tietojensa käsittelyä ja olla joutumatta automaattisen päätöksenteon kohteeksi.

Rekisteröityjen pyynnöt käsitellään lain edellyttämällä tavalla ja aikarajoissa. Rekisteröityjen pyyntöjen käsittelylle on määritetty asianmukaiset toimintaprosessit.

Henkilötietojen tietoturvaloukkaukset
Rantasalmen kunnan tavoitteena on minimoida henkilöihin kohdistuvia tietoturvaloukkauksia suunnittelemalla henkilötietojen käsittelyn tietosuojaperiaatteiden mukaisesti sekä toteuttamalla tekniset ja organisatoriset suojatoimenpiteet, jotka suhteutetaan henkilötietojen käsittelyyn liittyvään riskiin rekisteröidyille.

Henkilötietojen tietoturvaloukkausten havaitsemiseen, ilmoittamiseen ja käsittelyyn on asianmukaiset prosessit, ohjeet ja dokumentointikäytännöt. Henkilötietojen tietoturvaloukkaukset käsitellään lain edellyttämällä tavalla ja aikarajoissa. Jos henkilötietojen tietoturvaloukkaus on jo tapahtunut, toimitaan tilanteisiin laaditun ohjeistuksen mukaan.

Jokaisella organisaation palveluksessa olevalla ja sen lukuun työskentelevällä on velvollisuus ilmoittaa huomaamastaan henkilötietoihin kohdistuvasta riskistä, havaitsemastaan poikkeamasta tai muusta vastaavasta tilanteesta.

Mikäli organisaatio havaitsee tietoturvaloukkauksen, joka voi aiheuttaa erillisen riskin arvion perusteella rekisteröityjen oikeuksille ja vapauksille, tulee ilmoitus tehdä GDPR:n mukaan Suomen tietosuojavaltuutetulle viimeistään 72 tunnin kuluessa loukkauksen havaitsemisesta.

Kolmannet osapuolet ja henkilötietojen siirrot
Tietosuoja huomioidaan kunnan ja eri osapuolten välisissä sopimuksissa. Sopimuksia tehdessä varmistetaan, että sopimusehdoissa varmistutaan tietosuojasäädöksien vaatimusten noudattamisesta. Kirjalliset ja tietosuojalainsäädännön mukaiset tietojenkäsittelysopimukset solmitaan kaikkien Rantasalmen kunnan käyttämien henkilötietojen käsittelijöiden kanssa.

Kolmansiin osapuoliin liittyviä tietosuojariskejä arvioidaan ja hallitaan tekemällä asiaankuuluvia riskiarviointeja ja asettamalla vähimmäisvaatimukset tietojen käsittelylle ennen kuin aloitetaan yhteistyö kolmansien osapuolten kanssa.

Rantasalmen kunta ei lähtökohtaisesti siirrä henkilötietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle. Mahdollisten siirtojen osalta noudatetaan voimassa olevia lakeja ja asetuksia ja tietojen siirto toteutetaan asianmukaisella siirtoperusteella.

Tietosuojan keskeiset dokumentit
Rantasalmen kunta sitoutuu tietosuoja-asetuksen edellyttämän osoitusvelvollisuuden mukaisesti näyttämään, että se noudattaa toiminnassaan tietosuojalainsäädäntöä.

Rantasalmen kunnan ylläpitämät keskeiset dokumentit tietosuojaa koskevan vaatimuksenmukaisuuden ja osoitusvelvollisuuden täyttämiseksi ovat:

Tietosuoja- ja tietoturvapolitiikka	Tietosuoja- ja tietoturvapolitiikka kuvaa tietosuojan ja tietoturvan periaatteet, tietosuojan hallinnan tavoitteet, tietosuojan ja tietoturvan organisoinnin ja vastuut sekä toimintatavan.
Seloste käsittelytoimista	Seloste käsittelytoimista on sisäinen kuvaus organisaation tekemästä henkilötietojen käsittelystä ja käsittelyn tarkoituksista.
Rekisteröityjen informointidokumentit	Tietosuojaselosteet ja muut rekisteröityjen informointiin tarkoitetut dokumentit, joilla kerrotaan rekisteröidyille henkilötietojen käsittelystä läpinäkyvästi.
Tietosuojan arvioinnit ja riskiarvioinnit	Kunnan suorittamat tietosuojan esiarvioinnit, tietosuojan vaikutustenarvioinnit ja oikeutetun edun tasapainotestit.
Tietosuojan ja tietoturvan vuosisuunnitelma	Tietosuojan ja tietosuojan vuosisuunnitelmaan kirjataan tietosuojatyölle suunnitellut tehtävät kuukausitasolla. Tietosuojan ja tietoturvan vuosisuunnitelman avulla seurataan tietosuoja- ja tietoturvatyön etenemistä. Suunnitelma voi olla erillinen tietosuojan ja tietoturvan osalta.
Henkilöstö- ja koulutussuunnitelma	Määrittelee kunnan henkilöstölle suunnitellut tietosuojan ja tietoturvan koulutukset.
Tietojenkäsittelysopimuspohja	Määrittää henkilötietojen käsittelijöiden kanssa sovellettavat sopimusehdot.
Käsittelyn oikeusperusteeseen liittyvät dokumentit	Suostumukseen liittyvä dokumentaatio ja tarvittavat arvioinnit, kuten oikeutetun edun tasapainotestit.
Rekisteröityjen pyyntöjen käsittelyyn liittyvät dokumentit	Rekisteröityjen oikeuksien toteuttamiseen liittyvät ohjeistukset, pyyntöihin liittyvät lomakkeet ja dokumentointiin liittyvät asiakirjapohjat.
Tietoturvaloukkausten käsittelyyn liittyvät dokumentit	Tietoturvaloukkausten hallintaan liittyvät ohjeet ja dokumentointi.

7. Tietoturvaperiaatteet

Tietoturvaperiaatteita noudatetaan kaikissa tietojen käsittelyn elinkaaren eri vaiheissa ja tiedon kaikissa olomuodoissa. Tiedon elinkaarella tarkoitetaan kaikkia tiedon käsittelyn vaiheita tiedon keräämisestä tiedon hävittämiseen.

Tietoturvaperiaatteilla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys ja tätä kautta kunnan palvelutuotannon, prosessien ja muiden toimintojen luotettavuus, laatu sekä jatkuvuus. Lähtökohtana tietoturvaa koskevissa päätöksissä ovat viranomaissäädökset sekä hyvä tiedonhallinta- ja käsittelytapa.

Tiedon suojaaminen on oleellinen osa kunnan kokonaisturvallisuutta ja päivittäistä toimintaa. Tietoturvallisuuden perustana on osaava ja tietoturvaan sitoutunut henkilöstö. Tietoturvaperiaatteilla ohjataan tietojen suojaamista ja niitä edistetään tuomalla tietoturvaperiaatteet osaksi henkilöstön perehdytystä ja koulutusta.

Tietoturvaperiaatteiden noudattaminen on edellytys tietosuojaperiaatteiden toteutumiselle ja uuden teknologian turvalliseen käyttämiseen.

Alla olevassa taulukossa esitellään Rantasalmen kunnan keskeisimmät tietoturvaperiaatteet:

Hallinnollinen tietoturva	Hallinnollinen tietoturva koostuu johdon hyväksymistä periaatteista, vastuunjaosta, toimintatavoista, ohjeistuksista, tarkoitukseen varatuista resursseista sekä riskien arvioinnista ja valvonnasta.
Henkilöstöturvallisuus	Henkilöstöturvallisuuden pääpaino on riskien välttäminen ennakkoon varmistamalla työprosessien ja käsittelyketjujen tietovirtojen turvallisuus, työtehtävien riittävä eriyttäminen, jatkuva valvonta sekä varmistamalla henkilöstön riittävä ja ajantasainen tietoturvaosaaminen.
Fyysinen tietoturva	Fyysiseen tietoturvaan kuuluvat kaikki ne keinot, joilla pyritään suojaamaan henkilöiden, tietoaineistojen, laitteiden, toimitilojen ja omaisuuden turvallisuus. Fyysinen turvallisuus turvataan muun muassa rakennus- ja toimitilaratkaisuilla, fyysisen ja teknisen kulunvalvonnan, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan turvallisuuskäytännöillä.
Tietoaineistoturvallisuus	Tietoaineistoturvallisuus sisältää tietoaineistojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamisen. Tavoitteena on estää tietojen tuhoutuminen tai tahaton muuttuminen sekä varmistaa tietoaineistojen luokitus, suojaaminen, oikeanlainen käsittely, säilyttäminen ja hävittäminen.
Käyttöturvallisuus	Käyttöturvallisuuteen sisältyy muun muassa järjestelmien turvalliset käyttöperiaatteet, käytössä olevien järjestelmien osaaminen, tietojenkäsittelytapahtumien valvonta, laitteiden käyttövarmuus ja tietoturvapäivitykset, salasanakäytännöt, työtehtäviin perustuvien käyttöoikeuksien hallinta, jatkuvuuden turvaaminen sekä keskeisimpien toimintojen ja prosessien kuvausten ja ohjeistusten ylläpito.

Laitteistoturvallisuus	Laitteistoturvallisuus sisältää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.
Ohjelmistoturvallisuus	Ohjelmistoturvallisuus sisältää käyttöjärjestelmiin ja ohjelmistoihin kohdistuvat ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja valvontatoimet, lokimenettelyt, laadunvarmistusmenettelyt sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden varmistamiseksi.
Tietoliikenneturvallisuus	Tietoliikenneturvallisuudella varmistetaan verkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys tiedon liikkuessa järjestelmän sisällä tai organisaatioiden välillä. Keskeisenä tavoitteena on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus.

8. ICT-päätelaitteiden ja tietojärjestelmien käyttöperiaatteet

Rantasalmen kunnassa noudatetaan lainsäädännön tarkoittamaa hyvää tietojenkäsittelyn ja –hallinnan tapaa. Kunnan tietoja ja tietojärjestelmiä käytettäessä tulee noudattaa seuraavia tietoturvallisuutta edistäviä periaatteita. Päätelaitteiden ja tietojärjestelmien käytöstä annetaan yksityiskohtaisempia ja tarkentavia ohjeistuksia ja ohjeita erikseen kunnan tietohallinnosta vastaava taho.

Laitteiden hankinta ja asennukset

Kunnan työntekijöillä ja luottamushenkilöillä on tehtäviensä edellyttämät ajanmukaiset, tehtävään soveltuvat ja kustannustehokkaat välineet myös, liikkuvassa työympäristössä. Päätelaitteet ja niihin tallennetut työtiedostot ovat kunnan omaisuutta. Kunnan käytössä oleva tieto sekä tietojärjestelmät, laitteet ja ohjelmistot on tarkoitettu ensisijaisesti työtehtävien suorittamista varten.

Päätelaitteet ja mobiililaitteet hankitaan kunnan kilpailuttamien hankintasopimusten kautta. Hankittavat päätelaitteet tukevat tietoturvallista käyttöä. Rantasalmen kunnan hankkimat päätelaitemallit olla soveltuvia työtehtävien tarkoituksenmukaisen hoitamiseen. Kaikki kunnan omistamat laitteet tulee olla kirjattuna laiterekisteriin.

Kaikkien kunnan työtehtävien hoitamiseen hankittavien laitteiden pitää mahdollistaa keskitetty valvonta ja hallinta.

Kaikki työtehtävien hoitamiseen tarkoitetut päätelaitteet viedään hallintajärjestelmään ja hallintajärjestelmän kautta laitteille tuodaan keskitetysti tietoturvan ylläpitämiseen tarkoitettuja asetuksia ja sovelluksia.

Laitehallinnan avulla mobiililaitteisiin voidaan asettaa erilaisia sääntöjä tai estoja, sekä asentaa sovelluksia tai estää niiden asentaminen. Säännöt liittyvät pääosin tietoturvaan (esimerkiksi suojakoodi puhelimen käynnistämiseksi). Mahdolliset estot voivat liittyä tietoturvaan tai työnantajan direktio-oikeuteen kunnan hallitsemien laitteiden osalta. Laitteen sisältö salataan ja työtiedot eriytetään henkilökohtaisista tiedoista, jos se on teknisesti mahdollista.

Hallintosihteeri vastaa hankittavien laitteiden säännöllisestä katselmoinnista.

Esihenkilö tekee laitteen tilauksen erillisen ohjeistuksen mukaisesti.

Kunnan tietojärjestelmäympäristössä saa käyttää ainoastaan kunnan hankkimia tietojärjestelmiä, laitteita ja ohjelmistoja. Asennustyön saa suorittaa vain kunnan tietohallinnosta vastaavan valtuuttama taho.

Tietojärjestelmät, sovellukset ja niiden käyttöoikeudet
Rantasalmen kunta määrittelee työtehtäviin käytettävät tietojärjestelmät ja sovellukset. Kunnan toimintaa ja palveluita tukevat tietojärjestelmät tunnistetaan, luokitellaan kriittisyyden perusteella ja niille nimetään omistaja ja pääkäyttäjä.

Rantasalmen kunta vastaa hankkimiensa asennettujen sovellusten tietoturvasta. Kaikkien laitteelta työntekoon käytettävien sovellusten pitää salata oma tietoliikenteensä (HTTPS) tai VPN-yhteyden kautta.

Käyttöoikeudet kunnan tietoon ja tietojärjestelmiin myönnetään työtehtävien/luottamustoimen hoitoon tarvittavassa laajuudessa. Käyttäjä voivat käyttää tai jakaa muille työasemalla olevia tietoja vain siinä määrin kuin se on valtuutettua ja tarpeen ennalta määritettyjen työtehtävien suorittamiseksi.

Toteutuksesta riippuen käyttöoikeudet hyväksyvät käyttäjän esihenkilön hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.

Laitteiden ja järjestelmien käyttö
Päätelaite tulee säilyttää turvallisesti ja ulkopuolisten henkilöiden pääsy tulee estää. Käyttäjän tulee huolehtia työskentelynsä ja työskentely-ympäristönsä riittävästä tietosuojasta ja tietoturvasta. Käyttäjän tulee huomioida tietojen, tietojärjestelmien ja laitteiden käytöstä annetut ohjeistukset ja huolehdittava asianmukaisesta käytöstä.

Päätelaitteen saa liittää ainoastaan tunnettuihin verkkoihin, joiden tarjoamat yhteydet tulee olla luotettavasti salattuja. Salaamatonta WiFi-yhteyttä ei saa käyttää Rantasalmen kunnan päätelaitteilla.

Rantasalmen kunnan tietojärjestelmiä saa käyttää vain kunnan hankkimalla laiterekisterissä olevilla päätelaitteilla.

Käyttäjällä on velvollisuus ilmoittaa viipymättä työasemaan kohdistuneesta varkaudesta, sen katoamisesta tai työasemassa olleen tiedon luvattomasta paljastumisesta.

Tietoturvatyökalut
Ympäristön suojauksessa käytetään monitasoista suojausta. Päätelaitteita suojataan perinteisen virustorjunnan lisäksi työasemien ja palvelimien käyttäytymistä sekä haavoittuvuuksia analysoivilla työkaluilla.

Käyttäjiä suojataan älykkäällä sähköpostin suodatuksella, joka analysoi viestien sisältöä, liitteitä sekä linkkejä. Lisäksi identiteetin suojauksessa käytetään monivaiheista tunnistautumista ja käyttäjän kirjautumisten analyysiin perustuvia menetelmiä.

Työasemia sekä verkon laitteita suojataan teknisellä järjestelmällä, joka suodattaa laitteiden ja järjestelmien tekemät DNS-suodatukset. DNS-suodatus palauttaa vain turvallisia osoitteita ja estää haittaohjelmien aktivoitumisen ja kontrolliyhteydet.

Tietoturvatyökalut pystyvät analysoimaan käyttäjien ja päätelaitteiden toimintaa, mutta niillä ei kerätä tietoja käyttäjien omasta toiminnasta. Kerättyä tietoa käytetään vain vianselvityksessä ja tietoturvan kehittämisessä. Tietoihin pääsee käsiksi vain henkilöt tai kumppanit, kenellä siihen on roolinsa perusteella oikeutus.

Tietoturvatyökalujen keräämää tietoa analysoi myös ulkopuolinen SOC-kumppani, joka reagoi kriittisiin uhkiin ja tapahtumiin.

Kielletyt käyttötarkoitukset
Seuraavat käyttötarkoitukset ovat lähtökohtaisesti kiellettyjä kunnan päätelaitteilla:

- Muiden kuin työtarkoitukseen tarkoitettujen ohjelmistojen asentaminen ja käyttäminen.
- Kunnan työasemilla olevien sovellusten sekä tiedon käyttö muuhun tarkoitukseen, kuin kunnan toiminnan tai päätöksenteon tarpeisiin. Pois lukien käyttäjän tavanomainen henkilökohtaisen pankkiasioinnin tai muiden välttämättömien henkilökohtaisten asioiden hoito.
- Päätelaitteen tai tietojärjestelmän käyttöön liittyvän käyttäjätilin ja/tai siihen liittyvän salasanan paljastaminen muille henkilöille.
- Henkilökohtaisen päätelaitteen käytön salliminen muille henkilöille.
- Tietoturvaloukkausten tai verkkoviestinnän häiriöiden aiheuttaminen.
- Kirjautuminen työasemalta palvelimelle tai yhteiskäyttötilille, johon käyttäjällä ei ole nimenomaisesti oikeutta esimerkiksi työtehtävien puolesta.
- Työaseman käyttö erilaisten verkkomonitorointien suorittamiseen sekä työasemaan kohdistuvan liikenteen tallentaminen.
- Työasemassa olevien suojausmekanismien tarkoituksenmukainen kiertäminen tai niiden ominaisuuksien muokkaaminen.

Käyttö yksityisiin tarkoituksiin
Tietokoneelle ei saa asentaa omaan henkilökohtaiseen käyttöön tarkoitettuja sovelluksia. Rantasalmen kunnan hankkimia järjestelmiä ja/tai sovelluksia ei saa asentaa omaan henkilökohtaiseen päätelaitteeseen.

Henkilökohtaiset tiedot on pidettävä erillään kunnan omistamista ja hallinnoimista tiedoista.

9. Toimittajahallinta

Tietoturvaan ja tietosuojaan liittyvät vastuut ja velvoitteet huomioidaan kunnan ja eri osapuolten välisissä sopimuksissa. Riskiarvion edellyttämien tietoturvavaatimusten täyttyminen sopimusehdoissa varmistetaan sopimuksia tehdessä. Hankinta- ja ulkoistussopimuksia tekevät vastaavat siitä, että tietoturvan taso vastaa ostopalveluissa määräyksiä, ohjeita ja voimassa olevia säännöksiä sekä sopimuksen tekohetkellä että toimeksiannon aikana. Sopimuksilla varataan toimittajaan kohdistuva auditointioikeus ja tätä oikeutta käytetään tarvittaessa. Toimittajan kanssa pidetään säännöllisesti suunnittelu- ja seurantapalavereita, joissa käsitellään myös tietoturvallisuusasiat.

10. Toiminnan jatkuvuuden hallinta

Kunnan toiminnassa tunnistetaan jatkuvuutta uhkaavat riskit sekä varaudutaan niihin jatkuvuus- ja toipumissuunnitelmilla sekä niihin liittyvillä varajärjestelyillä. Jatkuvuuden varmistamisessa keskitytään ongelmien ja riskien ennalta ehkäisyyn sekä nopeaan toipumiseen poikkeamatilanteista. Jatkuvuuden hallintaan sisältyy kyberuhkiin varautuminen ja kyberturvallisuuden suojauskäytäntöjen riittävyyden arviointi.

Myös sopimuskumppaneilta edellytetään toiminnan jatkuvuutta uhkaavien riskien säännöllistä tunnistamista sekä ajan tasaisia jatkuvuus- ja toipumissuunnitelmia.

11. Tietoturvan tai tietosuojan rikkomukset

Tietoturva- ja tietosuojajärjestelyt toteutetaan siten, että turvallisuusloukkausten selvittäminen on jälkikäteen kohtuudella mahdollista. Tietoturvallisuushäiriöt, -poikkeamat ja tietoturvaloukkaukset hallinnoidaan hallintaprosessin mukaisesti.

Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi kunnan normaalein kurinpidollisin keinoin tai lainsäädännön edellyttämällä tavalla.

Tämän politiikan voi olla seurauksena käyttöoikeuksien rajoituksia, työsuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia. Työsuhteeseen vaikuttavista seuraamuksista on säädetty ensi sijassa työsopimuslaissa ja viranhaltijalaissa. Sovellettavaksi voivat tulla myös rikos- ja vahingonkorvauslainsäädäntö. Tietoturvarikkomuksista ilmoitetaan aina esihenkilölle.

Jokaisella organisaation työntekijällä on velvollisuus ilmoittaa huomaamastaan tietoturvaan kohdistuvasta riskistä, havaitsemastaan poikkeamasta tai muusta vastaavasta tilanteesta.

Tietoturvatyöryhmä huolehtii, että tietoturvaloukkaukset kirjataan, selvitetään viipymättä ja havaitut riskit saatetaan hallintaan.

Henkilötietojen tietoturvaloukkausten ilmoittamisessa valvontaviranomaisille ja rekisteröidylle toimitaan lainsäädännön ja kunnan ohjeistuksen mukaisesti.

Rantasalmen kunnan tietosuojavastaava toimii yhteyshenkilönä valvontaviranomaisen suuntaan.

12. Riskiperusteinen lähestymistapa ja tietoturvariskien hallinta

Kunta rekisterinpitäjänä arvioi tietojenkäsittelyyn ja henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallinta- ja tietoturvallisuustoimenpiteet.

Tietoturvan toteutumista tarkastellaan riskilähtöisesti. Kunnan järjestelmät luokitellaan niiden kriittisyyden mukaan. Kriittisten järjestelmien turvajärjestelyt tarkistetaan säännöllisesti ja niiden toimivuus testataan tarvittaessa.

Tietoturvallisuutta ja sen hallintakeinoja kehitetään jatkuvasti tietoturvariskien arvioinnin ja analysoinnin, käytännön kokemusten ja tietoturvallisuuden yleinen kehitys huomioiden.

13. Koulutus ja tietoisuuden lisääminen

Tietosuoja- ja tietoturvaan liittyvät ja koko kuntaa ohjaavaa ohjeistukset laaditaan hallinnollisessa yhteistyössä. Erityisesti henkilötietojen käsittelyyn liittyvää ohjeistusta tehdään sellaisiin työtehtäviin, joissa henkilötietoja käsitellään. Julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri) avulla parannetaan omaa riskitietoisuutta ja kehittämisen painopisteitä pohjautuen valittuihin Julkrin riskiperustaiseen arviointiin. Tietosuojaan ja tietoturvaan liittyvää ohjeistusta sisällytetään kunnan muihin ohjeistuksiin ja prosessien eri vaiheisiin tämän politiikan periaatteet huomioiden.

Rantasalmen kunnan tulee osoittaa, että henkilöstön tietoturva- ja tietosuojaosaaminen on ajantasaista.

Rantasalmen kunta velvoittaa jokaisen työntekijän hyväksymään tietoturvasitoumuksen palvelussuhteen alkaessa. Rantasalmen kunta järjestää tietosuojan peruskoulutuksen henkilöstölleen perehdytyksen yhteydessä. Tietosuoja- tietoturvapolitiikan sisällön omaksuminen on yhtenä osana uuden työntekijän perehdytystä. Osaamisen varmistamiseksi koko henkilöstöltä edellytetään vuosittain tietoturva- ja tietosuojakoulutuksen suorittamista. Tietoturva- ja tietosuojakoulutusta edellytetään myös luottamushenkilöiltä.

Poikkeamiin ja häiriöihin varaudutaan ennakolta ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuus- ja muita suunnitelmia. Tietoturva- ja tietosuojakoulutusta kohdennetuille henkilöstöryhmille osana kunnan yleistä henkilöstö- ja koulutussuunnittelua ja sen säännöllistä seurantaa.

Esihenkilöiden valvontaoikeuteen ja -velvollisuuteen kuuluu tietoturvallisuusohjeiden noudattamisen valvonta.

14. Tietosuojaa ja tietoturvaa koskevista asioista viestiminen

Tietosuojaa ja tietoturvaa koskevista asiaoista viestitään organisaatiossa läpinäkyvästi. Tietoturvapolitiikka määrittää voimassa olevat tietoturvan periaatteet ja dokumentista tiedotetaan koko henkilöstöä. Hyväksytty politiikka julkaistaan kunnan intranetissä ja verkkosivuilla ja siitä tiedotetaan henkilöstöä myös muilla keinoilla. Yleisesti tietoturva-asioissa tiedottaminen tapahtuu hallinnon ja esihenkilöjen kautta.