RANTASALMI

Kestävä luonnostaan

Rantasalmen kunnan tietosuoja- ja tietoturvapolitiikka

ICT-käyttöperiaatteet, tekoälylinjaus ja kameravalvonta

Yhteistoimintaryhmä xx.xx.2026 § x
Kunnanhallitus xx.xx.2026 § x

Sisällysluettelo

Rantasalmen kunnan tietosuoja- ja tietoturvapolitiikka 1

Kansitiedot 1

OSA I: Tietosuoja- ja tietoturvapolitiikka 2

1. Yleistä 2
   Viitekehys 2
   Hyväksyminen ja katselmointi 2
2. Keskeiset käsitteet 3
   Tietoluokat 4
3. Politiikan tavoitteet 5
4. Roolit ja vastuut 5
5. Suunnittelu ja raportointi 7
6. Henkilötietojen käsittelyn periaatteet 7
   Riskiperusteisuus ja sisäänrakennettu tietosuoja 8
   Rekisteröityjen oikeudet 8
   Henkilötietojen tietoturvaloukkaukset 8
   Kolmannet osapuolet ja tietojen siirrot 8
   Keskeiset dokumentit 9
7. Tietoturvaperiaatteet 9
8. Riskienhallinta 10
9. Toimittajahallinta 10
10. Toiminnan jatkuvuus ja varautuminen 11
11. Tietoturvapoikkeamat ja rikkomukset 11
12. Koulutus ja tietoisuus 11
13. Viestintä 12

OSA II: ICT-päätelaitteiden ja tietojärjestelmien käyttöperiaatteet 13

14. Laitteet ja niiden hallinta 13
15. Omat laitteet 13
16. Tietojärjestelmät ja käyttöoikeudet 14
17. Laitteiden ja tietojen käyttö 14
18. Paperiset ja muut analogiset aineistot 15
19. Kameravalvonta 15
20. Tietoturvatyökalut ja tekninen valvonta 16
21. Kielletty käyttö 16
22. Käyttö yksityisiin tarkoituksiin 16

OSA III: Tekoälylinjaus 17

23. Tarkoitus ja soveltamisala 17
24. Periaatteet 17
25. Mitä tekoälyyn saa syöttää 18
26. Hyväksytyt palvelut ja käyttötavat 18
27. Tekoäly viranomaistoiminnassa ja päätöksenteossa 19
   Kiellettyä on käyttää tekoälyä: 19
28. EU:n tekoälyasetus ja muu lainsäädäntö 20
29. Vastuut ja osaaminen 21

30. Voimaantulo, seuranta ja päivittäminen 22
OSA IV: Kameravalvonta 22
31. Valvonnan suunnittelu ja käyttöönotto 22
32. Tietosuojaseloste ja merkinnät 23
33. Kameroiden sijoittaminen 23
34. Katseluoikeudet, katselu ja lokitus 23
35. Säilytys, poisto ja tekniset vaatimukset 24
36. Tallenteiden luovuttaminen 24
37. Kielletyt menettelyt 25
Liite 1: Tekoälyn muistilista henkilöstölle 26
Liite 2: Toimintaohje tietosuoja- ja tietoturvapoikkeamissa 27
Liite 3: Pikaohje poikkeamatilanteeseen (huoneentaulu) 29
Liite 4: Kameravalvonnan pikaohje katselijalle (huoneentaulu) 30

Rantasalmen kunnan tietosuoja- ja tietoturvapolitiikka

ICT-käyttöperiaatteet, tekoälylinjaus ja kameravalvonta

Kansitiedot

Kunnanhallitus hyväksyy asiakirjan kokonaisuudessaan.

Osa I sisältää politiikan, Osa II käyttöperiaatteet, Osa III tekoälylinjauksen ja Osa IV kameravalvonnan säännöt.

Versio	Käsittely	Päivämäärä ja pykälä
2.0	Kunnanhallitus	[täydennetään]
2.0	Yhteistyötoimikunta	[täydennetään]
1.0	Kunnanhallitus	2.10.2023 § 247
1.0	Yhteistyötoimikunta	18.9.2023 § 22

OSA I: Tietosuoja- ja tietoturvapolitiikka

1. Yleistä

Rantasalmen kunnan toiminta ja palvelut perustuvat hyvään hallintoon ja luotettavaan tietoon, joka on osin julkista ja osin salassa pidettävää. Tiedon on oltava luotettavaa, suojattua ja käytettävissä kaikissa tilanteissa, myös häiriöissä ja poikkeusoloissa. Tämä edellyttää johdon sitoutumista, selkeitä vastuita ja osaavaa henkilöstöä.
Politiikka ja sen nojalla annetut ohjeet koskevat kaikkia kunnan viranhaltijoita, työntekijöitä, luottamushenkilöitä, työryhmiä ja toimielimiä sekä sidosryhmien edustajia, kuten palveluntuottajia, jotka tehtäviensä tai toimeksiantonsa puitteissa käsittelevät kunnan omistamaa tai hallinnoimaa tietoa. Politiikkaa noudatetaan käyttöpaikasta, laitteesta ja yhteydestä riippumatta.
Politiikka on kunnan ylin tietosuojaa ja tietoturvaa ohjaava asiakirja. Sitä tarkentavat Osan II käyttöperiaatteet ja erilliset ohjeet. Politiikka ja ohjeet julkaistaan intranetissä, ja politiikka myös kunnan verkkosivuilla.

Viitekehys

Kunnan tietosuoja- ja tietoturvatyötä ohjaavat soveltuvin osin:

- EU:n yleinen tietosuoja-asetus (EU) 2016/679 ja tietosuojalaki (1050/2018)
- laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki)
- laki viranomaisten toiminnan julkisuudesta (621/1999) ja arkistointilaki (529/2026)
- laki yksityisyyden suojasta työelämässä (759/2004) ja laki työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnassa ja hyvinvointialueella (449/2007)
- kyberturvallisuuslaki (124/2025) ja tiedonhallintalain 4 a luku soveltuvin osin hyvänä käytäntönä (soveltuvuusarvio luettelon jälkeen)
- EU:n tekoälyasetus (EU) 2024/1689
- julkisen hallinnon tietoturvallisuuden arviointikriteeristö Julkri (tiedonhallintalautakunnan suositus voimassa olevana versiona) ja sitä korvaavat valtiovarainministeriön kansallisen kriteeristöpankin kriteerit sekä Digi- ja väestötietoviraston VAHTI-suositukset
- kunnan strategia, hallintosääntö, konserniohje ja valmiussuunnitelma

Kyberturvallisuuslain ja tiedonhallintalain 4 a luvun velvoitteet eivät koske kuntaa viranomaisena (valtiovarainministeriön kirje VN/784/2025, 8.10.2025).
Kyberturvallisuuslakia voidaan kuitenkin soveltaa kunnan vesi-, jäte- tai energiahuoltoon, jos toiminnon tai kuntaomisteisen yhteisön koko ylittää lain rajat. Kunta tarkistaa arvion katselmoinnin yhteydessä ja käyttää lain riskienhallintavaatimuksia hyvänä käytäntönä ja ICT-hankintojen vaatimuksissa.

Hyväksyminen ja katselmointi

Kunnanhallitus hyväksyy politiikan, käyttöperiaatteet, tekoälylinjauksen ja kameravalvonnan säännöt kokonaisuudessaan yhteistoimintamenettelyn jälkeen.

Hallintojohtaja antaa niitä täydentävät ohjeet. Lisäksi hän voi perustellusta syystä antaa tietosuojan ja tietoturvan varmistamiseksi tarpeelliset määräykset, esimerkiksi uuden uhan, teknisen muutoksen tai viranomaisohjeen vuoksi. Annetut määräykset sisällytetään politiikkaan seuraavassa katselmoinnissa.
Politiikka katselmoidaan vuosittain sekä aina, kun lainsäädäntö, viranomaisohjeistus, kunnan organisaatio tai ICT-palveluntuottaja muuttuu merkittävästi. Katselmoinnista vastaa tietosuojavastaava yhdessä tietosuoja- ja tietoturvatyöryhmän kanssa.

2. Keskeiset käsitteet

Käsite	Määritelmä
Tietosuoja	Perusoikeus, joka turvaa jokaisen oikeudet ja vapaudet henkilötietojen käsittelyssä. Määrittää, milloin, millä edellytyksillä ja miten henkilötietoja saa käsitellä.
Tietoturva	Toimet, joilla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys. Kattaa tiedot, laitteet, ohjelmistot, tietoliikenteen, tilat ja toiminnan.
Kyberturvallisuus	Tietoturvan osa-alue, joka kattaa tietoverkkojen ja digitaalisten palvelujen suojaamisen tahallisia hyökkäyksiä ja häiriöitä vastaan.
Luottamuksellisuus	Tiedot ovat vain niihin oikeutettujen saatavilla. Käyttöoikeus perustuu työtehtävän tarpeeseen ja vähimpien oikeuksien periaatteeseen. Käyttäjät tunnistetaan luotettavasti.
Eheys	Tietoja voivat muuttaa vain siihen oikeutetut. Tieto suojataan luvattomalta tai vahingossa tapahtuvalta muuttamiselta ja poistamiselta.
Käytettävyys	Tiedot ja palvelut ovat oikeutettujen käytettävissä silloin, kun niitä tarvitaan.
Henkilötieto	Kaikki tieto, jonka avulla luonnollinen henkilö voidaan tunnistaa suoraan tai välillisesti.
Henkilötietojen käsittely	Kaikki henkilötietoihin kohdistuvat toimet, kuten kerääminen, tallentaminen, säilyttäminen, muuttaminen, luovuttaminen ja poistaminen.
Rekisterinpitäjä	Taho, joka määrittelee käsittelyn tarkoitukset ja keinot tai jolle käsittely on laissa säädetty. Kunta on rekisterinpitäjä omien tehtäviensä henkilötietojen osalta.
Rekisteröity	Henkilö, jonka tietoja käsitellään.
Henkilötietojen käsittelijä	Ulkopuolinen taho, joka käsittelee henkilötietoja kunnan lukuun, esimerkiksi järjestelmä- tai palveluntoimittaja. Kunnan omat työntekijät eivät ole käsittelijöitä.
Erityiset henkilötietoryhmät	Tietosuoja-asetuksen 9 artiklan tiedot, jotka paljastavat rotu- tai etnisen alkuperän, poliittiset mielipiteet, uskonnollisen tai filosofisen vakaumuksen tai ammattiliiton jäsenyyden, sekä geneettiset tiedot, tunnistamiseen

Käsite	Määritelmä
	käytettävät biometriset tiedot, terveystiedot ja seksuaalista käyttäytymistä tai suuntautumista koskevat tiedot.
Rikostuomioita ja rikoksia koskevat tiedot	Tietosuoja-asetuksen 10 artiklan tiedot, joiden käsittelystä säädetään erikseen.
Salassa pidettävä tieto	Julkisuuslain 24 §:n tai muun lain nojalla salassa pidettävä tieto, esimerkiksi oppilashuoltoa, varhaiskasvatuksen tuen tarvetta tai henkilöstön terveydentilaa koskevat tiedot sekä henkilön taloudellista asemaa kuvaavat tiedot, kuten maksujen perusteena olevat tulotiedot.
Tekniset ja organisatoriset toimet	Keinot, joilla luottamuksellisuus, eheys ja käytettävyys varmistetaan, kuten koulutus, ohjeet, salassapitositoumukset, käyttöoikeuksien hallinta, salaus, pseudonymisointi, lokit ja auditoinnit.
Henkilötietojen tietoturvaloukkaus	Tapahtuma, jonka seurauksena henkilötietoja käytetään, tuhoutuu, häviää, muuttuu tai paljastuu luvatta tai vahingossa.
Tietoturvapoikkeama	Tietojärjestelmiin, verkkoon tai laitteisiin kohdistuva häiriö tai hyökkäys, kuten tietomurto, palvelunestohyökkäys tai haittaohjelma. Poikkeama ei aina koske henkilötietoja.
Tietosuojan vaikutustenarviointi	Ennen käsittelyn aloittamista tehtävä arvio, joka on pakollinen, kun käsittely todennäköisesti aiheuttaa korkean riskin rekisteröidyille.
Tiedonhallintamalli	Tiedonhallintalain 5 §:n mukainen kuvaus kunnan tietoaineistoista, tietojärjestelmistä, käsittelyvastuista ja suojaustoimista.
Päätelaite	Laite, joka voidaan kytkeä tietoverkkoon, kuten tietokone, tabletti tai matkapuhelin.

Tietoluokat

Kunnan tieto luokitellaan suojaustarpeen mukaan viiteen luokkaan. Luokka ratkaisee, miten tietoa säilytetään, jaetaan ja hävitetään sekä missä palveluissa sitä saa käsitellä. Henkilön nimi, yhteystieto, kiinteistötunnus tai muu henkilötieto ei sellaisenaan tee asiakirjasta ei-julkista tai salassa pidettävää. Asiakirjan julkisuus ratkaistaan julkisuuslain perusteella, ja salassa pidettävät osat erotetaan tarvittaessa muusta asiakirjasta. Julkisuus ei kuitenkaan tarkoita, että asiakirjan henkilötiedot saa julkaista verkossa, vaan julkaisemisessa noudatetaan tietosuojalainsäädäntöä. Jos luokka on epäselvä, valitaan tiukempi luokka.

Tietoluokka	Kuvaus	Esimerkkejä
Julkinen	Julkaistu tai julkisuuslain mukaan julkinen tieto	Pöytäkirjat, tiedotteet, kunnan verkkosivut, lait
Sisäinen	Tieto, joka ei ole salassa pidettävää, mutta jota ei ole tarkoitettu julkaistavaksi tai joka ei ole vielä tullut julkiseksi	Valmisteluluonnokset, muistiot, sisäiset ohjeet

Tietoluokka	Kuvaus	Esimerkkejä
Henkilötiedot	Tieto, josta henkilö on tunnistettavissa ja joka ei ole julkista	Nimet yhdessä asian kanssa, yhteystiedot, kuvat ihmisistä, hakemukset
Salassa pidettävä tai arkaluonteinen	Julkisuuslain tai muun lain nojalla salassa pidettävä tieto sekä erityisiin henkilötietoryhmiin kuuluvat tiedot	Oppilashuolto, terveystiedot, henkilön taloudellinen asema, liikesalaisuudet, keskeneräisten hankintojen ja neuvottelujen tiedot, tietoturvatiedot
Käyttäjätunnukset ja salasanat	Tunnistautumiseen käytettävät tiedot	Tunnukset, salasanat, avaimet

Sisäinen on kunnan oma käytännön luokka valmisteluvaiheen aineistolle, ei julkisuuslain käsite. Sisäinen tieto voi tulla julkiseksi asian valmistuttua, ja tietopyynnöt ratkaistaan aina julkisuuslain perusteella.

3. Politiikan tavoitteet

Politiikan tavoitteena on tukea kunnan strategisten tavoitteiden toteutumista, kokonaisturvallisuutta ja turvallisuuskulttuuria. Tietosuojan osalta politiikka määrittää keinot, joilla kunta osoittaa noudattavansa tietosuojalainsäädäntöä. Tietoturvan osalta se määrittää periaatteet, vastuut ja valvonnan, joilla tiedonhallintalain ja muun lainsäädännön vaatimukset täytetään.
Politiikkaa sovelletaan tiedon muodosta ja käsittelytavasta riippumatta tiedon koko elinkaaren ajan, keruusta hävittämiseen tai arkistointiin.

4. Roolit ja vastuut

Roolit ja vastuut jakautuvat alla olevan taulukon mukaisesti. Tehtävänimikkeet ja vastuut vastaavat kunnan hallintosääntöä. Jos vastuuta ei ole määritelty hallintosäännössä tai muussa säännössä, hallintojohtaja nimeää rooliin tehtävän osaamisvaatimukset parhaiten täyttävän henkilön.
Kunnan henkilötietojen käsittelytoimien tietosuojaselosteet julkaistaan kunnan verkkosivuilla. Sisäinen tietosuoja- ja tietoturvadokumentaatio julkaistaan intranetissä. Tässä asiakirjassa tietohallinnolla tarkoitetaan hallinnon toimialan tietohallintotehtäviä, joita johtaa hallintojohtaja.

Rooli	Vastuu
Kunnanhallitus	Vastaa tiedonhallintalain 4 §:n mukaisesti tiedonhallinnan, tietosuojan ja tietoturvan johtamisesta, resursoinnista ja valvonnasta. Hyväksyy tämän politiikan ja tiedonhallintamallin.
Kunnanjohtaja	Tietosuojan ja tietoturvan omistaja. Luo edellytykset politiikan toimeenpanolle ja raportoi kunnanhallitukselle.
Hallintojohtaja	Vastaa politiikan toimeenpanon koordinoinnista, antaa täydentävät ohjeet ja perustellusta syystä tarpeelliset määräykset sekä päättää henkilöstön vuosittaisen tietosuoja- ja tietoturvakoulutuksen tai testin toteutuksesta. Johtaa kunnan

Rooli	Vastuu
	tietohallintoa yhdessä hallinnon kanssa, mukaan lukien tiedonhallintamallin ylläpito, tietojärjestelmähankintojen yhteensovittaminen ja ICT-palvelusopimusten seuranta.
Tietosuoja- ja tietoturvatyöryhmä	Jäseninä ovat nimetyt toimialojen edustajat ja ainakin hallintojohtaja, tietosuoja-asioiden asiantuntija ja ICT-asiantuntija. Ryhmä seuraa tietosuojan ja tietoturvan toteutumista, laatii vuosisuunnitelman, valmistelee ohjeet ja tekee kehitysehdotuksia. Koordinoi tietoturvariskien ja poikkeamien hallintaa ja kytkee tietoturvan muuhun kokonaisturvallisuuteen ja varautumiseen. Hallintojohtaja toimii tietosuoja- ja tietoturvatyöryhmän puheenjohtajana.
Tietosuojavastaava	Hoitaa tietosuoja-asetuksen 39 artiklan tehtävät: neuvoo, valvoo säännösten noudattamista, antaa lausuntoja vaikutustenarvioinneista ja toimii yhteyspisteenä tietosuojavaltuutetun toimistoon. Tehtävä voidaan hoitaa palvelusopimuksella toisen organisaation kautta, jolloin toiminnallista yhteistyötä tietosuojavastaavan kanssa tekee hallintojohtajan määräämä henkilö. Toimii tehtävässään riippumattomasti, eikä hänelle anneta tehtäviä, jotka johtavat eturistiriitaan.
Toimialan johto	Vastaa tietosuojan ja tietoturvan toteutumisesta johtamassaan toiminnassa sekä siitä, että tietojärjestelmien omistajat ja pääkäyttäjät on nimetty.
Esihenkilöt	Valvovat ohjeiden noudattamista, huolehtivat alaistensa perehdytyksestä ja koulutuksesta sekä käyttöoikeuksien hakemisesta ja poistamisesta. Ilmoittavat havainnoista toimialajohdolle ja tietosuoja- ja tietoturvatyöryhmälle.
Viranhaltijat, työntekijät ja luottamushenkilöt	Noudattavat politiikkaa ja ohjeita omassa työssään ja ilmoittavat havaitsemistaan uhista, poikkeamista ja rikkomuksista viipymättä kunnan poikkeamailmoituskanavaan ja tiedottavat esihenkilöä. Teknisistä uhista ja häiriöistä ilmoitetaan lisäksi ICT-palveluntuottajan tukeen.
Tiedon, tietojärjestelmän tai palvelun omistaja	Määrittelee ja hyväksyy käyttäjät ja käyttöoikeudet, toteuttaa riskienhallinnan, vastaa tietojen luokittelusta, säilytysajoista ja hävittämisestä, laatii tietosuojaselosteen ja nimeää yhteyshenkilön. Varmistaa ennen käyttöönottoa tai merkittävää muutosta tietoturvan arvioinnin ja tarvittaessa vaikutustenarvioinnin.
Tietojärjestelmän pääkäyttäjä	Valvoo tietoturvan ja käyttöoikeuksien toteutumista järjestelmässä, katselmoi käyttöoikeudet riskiperusteisesti, toimii yhteyshenkilönä toimittajaan ja tiedottaa häiriöistä ja katkoista.
Henkilöstöhallinto	Ohjaa henkilöstöturvallisuutta ja henkilötietojen käsittelyä palvelussuhteen kaikissa vaiheissa, mukaan lukien

Rooli	Vastuu
	tietoturvasitoumukset ja käyttöoikeuksien poisto palvelussuhteen päättyessä.
Asiakirjahallintoa johtava viranhaltija	Ohjaa asiakirjahallintoa ja arkistonmuodostusta sekä vastaa arkistoon siirretyistä asiakirjoista.
Hankintoja ja sopimuksia tekevät	Varmistavat, että hankittavien tuotteiden ja palvelujen tietosuoja- ja tietoturvataso vastaa kunnan vaatimuksia ja että tarvittavat tietojenkäsittelysopimukset tehdään.
Viestinnästä vastaava	Tukee tietosuojaan ja tietoturvaan liittyvää viestintää, myös häiriötilanteissa.
ICT-palveluntuottaja ja järjestelmätoimittajat	Vastaavat tietoturvan ja teknisen valvonnan toteutuksesta sopimusten ja sääntelyn mukaisesti, raportoivat poikkeamista viipymättä ja tekevät kehitysehdotuksia.
Tytäryhteisöjen hallitukset ja toimitusjohtajat	Vastaavat tietosuojan ja tietoturvan toteutumisesta omissa organisaatioissaan konserniohjeen mukaisesti.

5. Suunnittelu ja raportointi

Tietosuoja- ja tietoturvatyötä suunnitellaan vuosisuunnitelmalla, jossa tehtävät on jaettu kuukausitasolle ja vastuutettu. Vuosisuunnitelma voidaan laatia tietosuojalle ja tietoturvalle erikseen.
Tietosuoja- ja tietoturvatyön tulokset kootaan vuosittain tietotilinpäätökseen, jonka laatii hallintojohtaja ja joka käsitellään kunnanhallituksessa ja liitetään tilinpäätökseen valtuuston hyväksyttäväksi. Tietosuojavastaavan havainnot voidaan käsitellä tietotilinpäätöksen yhteydessä.
Kunta ylläpitää tiedonhallintalain mukaisesti tiedonhallintamallia ja asiakirjajulkisuuskuvausta sekä arvioi tiedonhallintansa ja tietoturvansa tilaa säännöllisesti. Arvioinnissa käytetään riskiperusteisesti Julkri-kriteeristöä tai sitä korvaavia kriteerejä.

6. Henkilötietojen käsittelyn periaatteet

Kunta noudattaa asiakkaiden, kuntalaisten, henkilöstön, luottamushenkilöiden ja sidosryhmien henkilötietojen käsittelyssä voimassa olevaa lainsäädäntöä ja tietosuoja-asetuksen 5 artiklan periaatteita.

Periaate	Toteutus kunnassa
Lainmukaisuus, asianmukaisuus ja läpinäkyvyys	Jokaisella käsittelyllä on dokumentoitu oikeusperuste. Rekisteröidyille kerrotaan käsittelystä selkeästi tietosuojaselosteilla.
Käyttötarkoitussidonnaisuus	Käsittely perustuu ennalta määriteltyyn ja lailliseen tarkoitukseen. Tietoja ei käytetä tarkoitukseen, joka on yhteensopimaton alkuperäisen kanssa.
Tietojen minimointi	Tietoja kerätään ja käsitellään vain siinä määrin kuin tarkoitus edellyttää.
Täsmällisyys	Virheelliset tiedot oikaistaan tai poistetaan viipymättä.

Periaate	Toteutus kunnassa
Säilytyksen rajoittaminen	Säilytysajat määritetään tiedonohjaussuunnitelmassa, ja tiedot hävitetään tai arkistoidaan niiden mukaisesti.
Eheys ja luottamuksellisuus	Tiedot suojataan riskeihin suhteutetuin teknisin ja organisatorisin toimin.
Osoitusvelvollisuus	Kunta pystyy osoittamaan noudattavansa periaatteita dokumentaatiolla, jota kuvataan tämän luvun lopussa.

Riskiperusteisuus ja sisäänrakennettu tietosuoja

Kunta arvioi henkilötietojen käsittelyn riskit ennen uuden järjestelmän, palvelun tai toimittajan käyttöönottoa sekä olemassa olevien käsittelyjen muuttuessa. Kun käsittely todennäköisesti aiheuttaa korkean riskin, tehdään tietosuojan vaikutustenarviointi ennen käsittelyn aloittamista, ja tietosuojavastaava antaa siitä lausunnon.
Tietosuoja huomioidaan suunnittelussa alusta lähtien. Oletusarvoisesti:

- kerätään vain tarkoituksen kannalta välttämättömät tiedot
- tietoja ei säilytetä kauemmin kuin on tarpeen
- tietoja ei saateta rajoittamattoman henkilöjoukon saataville
- käyttöoikeudet rajataan työtehtävien mukaisiksi

Rekisteröityjen oikeudet

Kunta toteuttaa rekisteröityjen oikeudet käsittelyn oikeusperusteen mukaisesti. Rekisteröidyllä on oikeus saada tietoa käsittelystä, tarkastaa omat tietonsa, vaatia niiden oikaisemista tai poistamista, rajoittaa ja vastustaa käsittelyä, siirtää tietonsa järjestelmästä toiseen sekä olla joutumatta pelkästään automaattiseen päätöksentekoon perustuvan päätöksen kohteeksi. Pyynnöt käsitellään ohjeistetun prosessin mukaisesti kuukauden kuluessa tai lain sallimissa rajoissa pidennettynä.

Henkilötietojen tietoturvaloukkaukset

Jokaisen on ilmoitettava havaitsemastaan loukkauksesta tai sen epäilystä viipymättä kunnan poikkeamailmoituskanavaan ja tiedotettava esihenkilöä. Teknisistä uhista ja häiriöistä ilmoitetaan lisäksi ICT-palveluntuottajan tukeen. Loukkaukset käsitellään liitteen 2 toimintaohjeen mukaisesti:

1. Kaikki loukkaukset kirjataan loukkausrekisteriin, myös ne, joista ei tehdä ilmoitusta viranomaiselle.
2. Loukkauksesta ilmoitetaan tietosuojavaltuutetun toimistolle 72 tunnin kuluessa havaitsemisesta, ellei ole epätodennäköistä, että siitä aiheutuu riskiä rekisteröidyille.
3. Jos riski on korkea, myös rekisteröidyille ilmoitetaan ilman aiheetonta viivytystä.
4. Jos loukkaus liittyy tietoturvapoikkeamaan, menetellään lisäksi luvun 11 mukaisesti.

Kolmannet osapuolet ja tietojen siirrot

Kunta tekee kirjallisen tietojenkäsittelysopimuksen kaikkien henkilötietojen käsittelijöiden kanssa ja arvioi toimittajan riskit ennen yhteistyön alkua. Henkilötietoja ei lähtökohtaisesti siirretä EU:n tai ETA:n ulkopuolelle. Jos siirto on välttämätön, sille on oltava tietosuoja-

asetuksen mukainen siirtoperuste, ja siirto arvioidaan etukäteen. Sama koskee pilvipalveluja, joissa tietoja tai tukipalveluja voidaan käsitellä EU:n ulkopuolelta.

Keskeiset dokumentit

Dokumentti	Sisältö
Tietosuoja- ja tietoturvapolitiikka	Tämä asiakirja
Tiedonhallintamalli	Tietoaineistot, tietojärjestelmät, vastuut ja suojaustoimet
Seloste käsittelytoimista	Sisäinen kuvaus henkilötietojen käsittelystä
Tietosuojaselosteet	Rekisteröityjen informointi
Tiedonohjaussuunnitelma ja asiakirjajulkisuuskuvaus	Säilytysajat, julkisuus ja arkistointi
Riskiarviot ja vaikutustenarvioinnit	Esiarvioinnit, vaikutustenarvioinnit ja tasapainotestit
Vuosisuunnitelma ja tietotilinpäätös	Suunnitellut tehtävät ja niiden toteutuminen
Koulutussuunnitelma	Henkilöstön ja luottamushenkilöiden koulutukset
Tietojenkäsittelysopimuspohja	Käsittelijöihin sovellettavat ehdot
Rekisteröityjen pyyntöjen ohjeet ja lomakkeet	Oikeuksien toteuttaminen
Loukkaus- ja poikkeamaohje sekä loukkausrekisteri	Loukkausten käsittely ja dokumentointi

7. Tietoturvaperiaatteet

Tietoturvaperiaatteita noudatetaan tiedon koko elinkaaren ajan ja kaikissa tiedon olomuodoissa. Niillä varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys ja sitä kautta palvelujen luotettavuus ja jatkuvuus. Tietoturvan perusta on osaava ja sitoutunut henkilöstö.

Osa-alue	Keskeinen sisältö
Hallinnollinen tietoturva	Johdon hyväksymät periaatteet, vastuunjako, ohjeet, resurssit, riskienarviointi ja valvonta.
Henkilöstöturvallisuus	Tietoturvasitoumus, perehdytys, vuosittainen koulutus tai testi, tehtävien eriyttäminen sekä käyttöoikeuksien hallinta palvelussuhteen alusta loppuun.
Fyysinen turvallisuus	Tilojen kulunvalvonta sekä suojautuminen palo-, vesi-, sähkö- ja murtovahingoilta.
Tietoaineistoturvallisuus	Tietojen luokittelu, suojaaminen, säilytys ja hävittäminen, myös analogisten aineistojen ja tallennusvälineiden osalta.
Käyttöturvallisuus	Turvalliset käyttötavat, monivaiheinen tunnistautuminen, käyttöoikeuksien hallinta, päivitykset, varmuuskopiointi ja ajantasaiset prosessikuvaukset.

Osa-alue	Keskeinen sisältö
Laitteistoturvallisuus	Laitteiden keskitetty hallinta, kokoonpanojen määrittely, elinkaaren hallinta ja turvallinen poistaminen käytöstä.
Ohjelmistoturvallisuus	Ohjelmistojen hyväksyntä, haavoittuvuuksien hallinta, päivitykset, lokitus ja valvonta.
Tietoliikenneturvallisuus	Tietoliikenteen salaus, verkon segmentointi ja suojaus sekä viestien alkuperän ja eheyden varmistaminen.

8. Riskienhallinta

Kunta arvioi tiedonhallinnan ja tietojärjestelmien tietoturvariskit tiedonhallintalain 13 §:n mukaisesti ja valitsee suojaustoimet riskitason perusteella. Tietojärjestelmät luokitellaan kriittisyyden mukaan. Kriittisten järjestelmien suojaukset tarkistetaan ja toipuminen testataan riskiperusteisesti. Kunta edellyttää tarkistukset ja testaukset ICT-palveluntuottajalta ja saa niistä raportin.
Tietojärjestelmän tietoturvallisuus arvioidaan ennen käyttöönottoa ja merkittäviä muutoksia. Kriittisistä järjestelmistä kerätään tiedonhallintalain 17 §:n mukaiset lokitiedot. Henkilötietojen käsittelyn riskit arvioidaan luvun 6 mukaisesti.
Riskienhallintaa kehitetään riskiarvioiden, poikkeamista saatujen kokemusten ja toimintaympäristön muutosten perusteella.

9. Toimittajahallinta

Tietosuojan ja tietoturvan vaatimukset sisällytetään kaikkiin ICT-hankintoihin ja sopimuksiin riskiarvion perusteella. Hankintoja ja sopimuksia tekevät vastaavat siitä, että vaatimukset täyttyvät sekä sopimusta tehdessä että sopimuskauden aikana. Vaatimukset huomioidaan uusissa sopimuksissa sekä voimassa olevia sopimuksia uusittaessa tai muutettaessa.
Sopimuksissa sovitaan vähintään:

- tietojenkäsittelysopimuksesta ja tietojen sijainnista
- poikkeamien ilmoittamisesta kunnalle ilman viivytystä
- kunnan oikeudesta auditoida toimittaja
- jatkuvuus- ja toipumisvaatimuksista
- alihankkijoiden käytöstä ja niiden hyväksymisestä
- sopimuksen päättymisestä: tietojen palauttamisesta kunnalle käytettävässä muodossa, tietojen hävittämisestä ja sen todentamisesta, hallintatunnusten ja käyttöoikeuksien siirrosta sekä lokitietojen säilymisestä

Toimittajan kanssa pidetään säännöllisesti seurantapalavereita, joissa käsitellään myös tietoturva. Toimittajan vaihtuessa laaditaan siirtymäsuunnitelma, jossa tietoturvan ja tietosuojan riskit arvioidaan erikseen.

10. Toiminnan jatkuvuus ja varautuminen

Kunta tunnistaa toiminnan jatkuvuutta uhkaavat riskit ja varautuu niihin jatkuvuus- ja toipumissuunnitelmilla, jotka ovat osa kunnan valmiussuunnitelmaa. Varautumiseen kuuluvat:

- kriittisten palvelujen ja järjestelmien tunnistaminen sekä niiden suurin sallittu katkoaika
- varmuuskopiointi, joka on suojattu kiristyshaittaohjelmia vastaan, ja palautuksen säännöllinen testaus
- toimintaohjeet tietojärjestelmien ja tietoliikenteen häiriöiden varalle
- kyberhäiriöharjoitus kerran vuodessa tarkoituksenmukaisella tavalla, esimerkiksi pöytäharjoituksena yhdessä ICT-palveluntuottajan kanssa tai osallistumalla valtakunnalliseen harjoitukseen

Sopimuskumppaneilta edellytetään ajantasaisia jatkuvuus- ja toipumissuunnitelmia.

11. Tietoturvapoikkeamat ja rikkomukset

Tietoturvajärjestelyt toteutetaan niin, että poikkeamat ja rikkomukset voidaan selvittää jälkikäteen. Jokaisen on ilmoitettava havaitsemastaan uhasta, poikkeamasta tai rikkomuksesta viipymättä kunnan poikkeamailmoituskanavaan ja tiedotettava esihenkilöä. Teknisistä uhista ja häiriöistä ilmoitetaan lisäksi ICT-palveluntuottajan tukeen.
Poikkeamat käsitellään liitteen 2 toimintaohjeen mukaisesti. Tietosuoja- ja tietoturvatyöryhmä huolehtii, että poikkeamat kirjataan, selvitetään viipymättä ja havaitut riskit saatetaan hallintaan. Merkittävistä poikkeamista ilmoitetaan Kyberturvallisuuskeskukselle ja tarvittaessa poliisille. Henkilötietoja koskevat loukkaukset käsitellään lisäksi luvun 6 mukaisesti.
Politiikan ja ohjeiden rikkomiseen puututaan välittömästi. Rikkomisesta voi seurata käyttöoikeuksien rajoittaminen, työoikeudellisia toimenpiteitä työsopimuslain tai viranhaltijalain mukaisesti sekä rikos- tai vahingonkorvausoikeudellisia seuraamuksia.

12. Koulutus ja tietoisuus

Kunnan on pystyttävä osoittamaan, että henkilöstön tietosuoja- ja tietoturvaosaaminen on ajantasaista:

- jokainen hyväksyy tietoturvasitoumuksen palvelussuhteen alkaessa ja politiikka on osa perehdytystä
- koko henkilöstö suorittaa vuosittain tietosuoja- ja tietoturvakoulutuksen tai osaamista mittaavan testin, ja suorittamista seurataan ja tilastoidaan
- kunta järjestää luottamushenkilöille koulutuksen toimikauden alussa ja tarvittaessa sen aikana ja edellyttää sen suorittamista
- henkilötietoja paljon käsitteleville ja järjestelmien pääkäyttäjille järjestetään kohdennettua koulutusta
- vuosittainen koulutus tai testi voidaan toteuttaa myös tietojenkalasteluharjoituksena

Hallintojohtaja päättää vuosittaisen koulutuksen tai testin toteutustavasta, sisällöstä, suoritusajasta, hyväksytyn suorituksen rajasta ja seurannasta. Koulutus on osa kunnan henkilöstö- ja koulutussuunnitelmaa. Esihenkilöt huolehtivat, että heidän alaisensa suorittavat koulutuksen tai testin ja valvovat ohjeiden noudattamista.

13. Viestintä

Tietosuojasta ja tietoturvasta viestitään läpinäkyvästi. Henkilöstölle tiedotetaan politiikasta intranetin lisäksi esihenkilöiden kautta. Häiriötilanteiden viestinnästä vastaa kunnanjohtaja hallintosäännön mukaisesti ja viestinnän valmistelevat hallintojohtaja ja viestinnästä vastaava.

OSA II: ICT-päätelaitteiden ja tietojärjestelmien käyttöperiaatteet

Nämä käyttöperiaatteet tarkentavat Osaa I. Ne koskevat kaikkia kunnan laitteiden, tietojärjestelmien ja palvelujen käyttäjiä. Hallintojohtaja antaa niitä täydentävät ohjeet ja tarvittaessa luvun 1 mukaiset määräykset ja ICT-palveluntuottaja antaa tekniset ohjeet. Hyvinvointi- ja sivistyslautakunta tai sen valtuuttama viranhaltija voi antaa opetustoimen oppilaslaitteista ja opetuksen pilvipalveluista erillisen ohjeen, jossa näitä periaatteita sovelletaan opetusympäristöön.

14. Laitteet ja niiden hallinta

- Kunnan työntekijöillä ja tarvittaessa luottamushenkilöillä on tehtävien edellyttämät ajanmukaiset ja tietoturvalliset välineet.
- Päätelaitteet ja niille tallennetut työtiedot ovat kunnan omaisuutta ja tarkoitettu ensisijaisesti työkäyttöön.
- Laitteet hankitaan kunnan kilpailuttamien sopimusten kautta. Esihenkilö tilaa laitteen erillisen ohjeen mukaisesti.
- Kaikki laitteet kirjataan laiterekisteriin ja liitetään keskitettyyn laitehallintaan, jonka kautta laitteille asennetaan tietoturva-asetukset, päivitykset ja sovellukset.
- Laitehallinnalla voidaan asettaa sääntöjä ja estoja, kuten näytönlukitus ja sovellusten asennusrajoitukset. Laitteen sisältö salataan ja työtiedot eriytetään henkilökohtaisista tiedoista, kun se on teknisesti mahdollista.
- Ohjelmistojen asennuksia saa tehdä vain ICT-palveluntuottaja tai sen valtuuttama taho.
- Laite palautetaan palvelussuhteen tai luottamustoimen päättyessä. Käytöstä poistettavien laitteiden tiedot hävitetään todennetusti.
- ICT-yhdyshenkilönä toimii kunnan ICT-asiantuntija tai muu hallintojohtajan nimeämä henkilö. Hän toimii yhteyshenkilönä kunnan ja ICT-palveluntuottajan välillä, seuraa laiterekisteriä, koordinoi laitetilaukset ja vastaa laitemallien ja laitekannan säännöllisestä katselmoinnista.

15. Omat laitteet

Kunnan sähköpostia, Teamsia ja muita hyväksyttyjä pilvipalveluja saa käyttää omalla matkapuhelimella tai tabletilla vain kunnan hyväksymien sovellusten kautta, kun laitteessa on näytönlukitus ja ajantasainen käyttöjärjestelmä. Kunta ottaa myöhemmin käyttöön sovellushallinnan ja ehdollisen pääsyn, minkä jälkeen käyttö edellyttää niiden vaatimusten täyttymistä. Kunnan tietoja ei saa tallentaa oman laitteen paikalliseen muistiin tai henkilökohtaisiin pilvipalveluihin. Kokousaineistoja saa lukea kunnan kokousjärjestelmästä omalla laitteella. Muiden tietojärjestelmien käyttö omalla laitteella on kielletty, ellei hallintojohtaja ole erikseen sitä hyväksynyt. Luottamustoimen hoidossa käytetään kunnan tarjoamaa sähköpostia ja muita kunnan M365-palveluja. Kunnan sähköposteja tai

kalenterikutsuja ei saa ohjata henkilökohtaiseen sähköpostiin, eikä kunnan asioita hoideta henkilökohtaisella sähköpostilla.

16. Tietojärjestelmät ja käyttöoikeudet

- Kunta määrittelee työssä käytettävät tietojärjestelmät ja sovellukset. Jokaiselle järjestelmälle nimetään omistaja ja pääkäyttäjä ja se luokitellaan kriittisyyden mukaan.
- Käyttöoikeudet myönnetään työtehtävän tai luottamustoimen edellyttämässä laajuudessa. Järjestelmän omistaja tai hänen valtuuttamansa hyväksyy oikeudet esihenkilön pyynnöstä.
- Käyttöoikeudet muutetaan tehtävien muuttuessa ja poistetaan viimeistään palvelussuhteen päättymispäivänä. Pääkäyttäjä katselmoi oikeudet riskiperusteisesti: katselmoinnin tiheys määräytyy järjestelmän kriittisyyden ja siinä käsiteltävien tietojen mukaan.
- Kaikissa kunnan pilvipalveluissa ja etäyhteyksissä käytetään monivaiheista tunnistautumista. Windowsin tunnistautumismenetelmät, kuten kasvojentunnistus, sormenjälki ja PIN-koodi, ovat hyväksyttyjä. Vahvaa tunnistautumista vaativissa palveluissa suositellaan mobiilivarmennetta tai toimikorttia. Salasanat ovat vahvoja ja palvelukohtaisia ja ne säilytetään turvallisesti, esimerkiksi luotettavassa salasanojen hallintaohjelmassa. Salasanoja ei kirjoiteta näkyville eikä tallenneta suojaamattomaan tiedostoon. Kunta selvittää yhteisen salasanojen hallintaohjelmiston käyttöönoton.
- Tunnukset ovat henkilökohtaisia. Yhteiskäyttötunnuksia käytetään vain hallintojohtajan hyväksymässä tapauksessa ja niiden käyttäjät kirjataan.
- Tietoliikenne kunnan palveluihin on salattu, eikä salausta saa ohittaa.

17. Laitteiden ja tietojen käyttö

- Laite säilytetään turvallisesti, näyttö lukitaan poistuttaessa ja ulkopuolisten pääsy laitteeseen ja tietoihin estetään, myös paikasta riippumattomassa työssä ja julkisilla paikoilla.
- Laite liitetään vain riittävän turvallisiksi arvioituihin verkkoihin, kuten kunnan verkkoon tai salattuun kotiverkkoon. Julkisissa verkoissa käytetään vain kunnan palveluja, joiden yhteys on salattu, eikä verkon pyytämiä ohjelmia tai varmenteita asenneta. Salassa pidettävää tietoa käsitellään julkisessa verkossa vain, jos verkko on arvioitu riittävän turvalliseksi, muuten käytetään matkapuhelinyhteyttä.
- Työtiedot tallennetaan kunnan hyväksymiin tallennuspaikkoihin, ei laitteen paikalliseen muistiin tai muistitikulle. Tiedot vastaanotetaan ensisijaisesti sähköpostilla tai kunnan hyväksymän tiedostonjakopalvelun kautta. Ulkopuolisilta saatuja muistitikkuja tai muita ulkoisia tallennusvälineitä ei kytketä kunnan laitteisiin ilman ICT-tuen tarkistusta. Jos tietoja luovutetaan muistitikulla, käytetään kunnan hankkimaa tikkua ja salassa pidettävä tai henkilötietoja sisältävä aineisto salataan.

- Tiedostoja jaetaan kunnan ulkopuolelle vain kunnan hyväksymillä palveluilla ja nimetyille vastaanottajille. Salassa pidettävä tieto lähetetään suojatulla sähköpostilla. Suojattu sähköposti annetaan käyttöön niille, joiden tehtäviin salassa pidettävän tiedon lähettäminen kuuluu.
- Työsähköposteja tai kalenterikutsuja ei saa ohjata tai välittää yksityiseen sähköpostiin.
- Salassa pidettävät tulosteet haetaan tulostimelta heti ja paperiaineistot hävitetään luvun 18 mukaisesti.
- Laitteen katoamisesta, varkaudesta tai tietojen luvattomasta paljastumisesta ilmoitetaan viipymättä kunnan poikkeamailmoituskanavaan ja ICT-palveluntuottajan tukeen sekä tiedotetaan esihenkilöä.

18. Paperiset ja muut analogiset aineistot

Analogisella aineistolla tarkoitetaan paperiasiakirjoja sekä muuta ei-sähköistä aineistoa, kuten valokuvia, karttoja, piirustuksia, mikrofilmejä sekä ääni- ja videotallenteita. Niihin sovelletaan samoja periaatteita kuin sähköiseen tietoon. Salassa pidettävää ja henkilötietoja sisältävää analogista aineistoa käsitellään seuraavasti:

- **Säilytys:** aineisto säilytetään lukitussa kaapissa tai tilassa, eikä sitä jätetä työpöydälle työpäivän päätteeksi.
- **Hävittäminen:** aineisto hävitetään tietoturvasäiliöiden tai sopimuskumppanin hävityspalvelun kautta, ei tavallisen paperinkeräyksen mukana.
- **Postitus ja kuljetus:** aineisto lähetetään suljetussa kuoressa ja tarvittaessa kirjattuna. Salassapitomerkintä tehdään asiakirjaan tai sisäkuoreen, ei ulkokuoreen.
- **Paikasta riippumaton työ:** aineistoa viedään työpaikan ulkopuolelle vain, kun se on työtehtävän kannalta välttämätöntä ja sitä säilytetään ja hävitetään samoin periaattein kuin työpaikalla. Erityisiin henkilötietoryhmiin kuuluvaa tai muuten erityisen arkaluonteista aineistoa ei pääsääntöisesti viedä työpaikan ulkopuolelle.
- **Kokousaineistot:** luottamushenkilöiden paperiset salassa pidettävät liitteet palautetaan kokouksen jälkeen tai hävitetään tietoturvallisesti.
- **Arkistotilat:** kulunvalvonnasta ja kulkuoikeuksista määrätään kunnan asiakirjahallinnon ohjeessa.
- **Digitointi:** skannatun aineiston paperioriginaalit käsitellään tiedonohjaussuunnitelman mukaisesti.

Myös analogiseen aineistoon voi kohdistua henkilötietojen tietoturvaloukkaus, esimerkiksi kun kirje postitetaan väärään osoitteeseen tai aineisto katoaa. Tällaiset tapaukset ilmoitetaan ja käsitellään luvun 6 mukaisesti.

19. Kameravalvonta

Kameravalvontaa käytetään vain henkilöiden ja omaisuuden turvallisuuden varmistamiseen sekä rikosten ja vahinkojen ehkäisemiseen ja selvittämiseen. Valvonta suunnitellaan, dokumentoidaan ja arvioidaan ennen kameroiden asentamista. Kameroita ei sijoiteta valvomaan yksittäisen työntekijän työpistettä tai tiloja, joissa yksityisyyden suoja on

erityisen vahva. Tallenteita saavat katsella vain nimetyt henkilöt kirjatusta syystä ja ne poistetaan määritellyn ajan kuluttua. Tarkemmat säännöt ovat Osassa IV.

20. Tietoturvatyökalut ja tekninen valvonta

Kunnan ympäristö suojataan monitasoisesti. Käytössä ovat vähintään:

- päätelaitteiden haittaohjelmatorjunta ja käyttäytymistä analysoiva suojaus
- sähköpostin suodatus, joka analysoi viestien sisällön, liitteet ja linkit
- monivaiheinen tunnistautuminen ja kirjautumisten poikkeamien tunnistus
- haitallisten verkko-osoitteiden esto (DNS-suodatus)
- tietoturvavalvonta ICT-palvelusopimuksen mukaisesti

Työkalut keräävät lokitietoja laitteiden, käyttäjätunnusten ja järjestelmien toiminnasta, kuten kirjautumisista, verkkoyhteyksistä ja tietoturvahälytyksistä. Tietoja käytetään vain tietoturvan varmistamiseen, vianselvitykseen ja poikkeamien tutkintaan, ei työsuorituksen seurantaan. Tietoihin pääsevät vain ne henkilöt ja kumppanit, joiden tehtävä sitä edellyttää. Tekninen valvonta ja sähköpostin käsittely toteutetaan työelämän tietosuojalain mukaisesti, ja niiden periaatteet käsitellään yhteistoimintamenettelyssä tämän politiikan yhteydessä.

21. Kielletty käyttö

Kunnan laitteilla ja järjestelmissä on kiellettyä:

- asentaa tai käyttää muita kuin kunnan hyväksymiä ohjelmistoja ja palveluja
- käyttää kunnan tietoja tai tietojärjestelmien tietosisältöä, kuten henkilörekistereitä sekä asiakas- ja henkilöstötietoja, omiin tarkoituksiin tai muuhun kuin kunnan toiminnan tai päätöksenteon tarpeisiin
- luovuttaa omaa tunnusta tai salasanaa toiselle tai antaa toisen käyttää itselle luovutettua kunnan laitetta
- kirjautua järjestelmään, palvelimelle tai yhteiskäyttötilille ilman siihen myönnettyä oikeutta
- aiheuttaa tietoturvaloukkauksia tai häiriöitä tietoliikenteeseen
- monitoroida verkkoa tai tallentaa verkkoliikennettä, ellei se kuulu nimenomaisesti työtehtäviin
- kiertää tai muuttaa laitteen suojausmekanismeja

22. Käyttö yksityisiin tarkoituksiin

Tietojärjestelmien tietosisällön käyttö omiin tarkoituksiin on kielletty luvun 21 mukaisesti. Kunnan laitteen sovelluksia, kuten selainta ja toimisto-ohjelmia, saa käyttää kohtuullisessa määrin satunnaisten välttämättömien henkilökohtaisten asioiden hoitamiseen, kuten pankkiasiointiin, jos se ei häiritse työtä tai vaaranna tietoturvaa. Laitteelle ei saa asentaa henkilökohtaiseen käyttöön tarkoitettuja sovelluksia. Henkilökohtaiset tiedot pidetään erillään kunnan tiedoista, eikä kunnan tietoja saa siirtää henkilökohtaisiin palveluihin.

OSA III: Tekoälylinjaus

23. Tarkoitus ja soveltamisala

Rantasalmen kunta käyttää tekoälyä aktiivisesti työn tukena, turvallisesti ja lainmukaisesti. Tekoäly on avustava työväline. Se ei korvaa työntekijän, viranhaltijan tai luottamushenkilön harkintaa, vastuuta eikä asiantuntemusta.
Tekoälyä kannattaa käyttää erityisesti tehtävissä, joissa siitä on selvää hyötyä ja joissa mahdollinen virhe havaitaan ja korjataan ennen kuin siitä aiheutuu vahinkoa.
Linjausta sovelletaan:

- kunnan työntekijöihin ja viranhaltijoihin
- luottamushenkilöihin, kun he käsittelevät kunnan tehtäviin liittyviä tietoja
- kunnan lukuun työskenteleviin, kun he käsittelevät kunnan tietoja tai käyttävät kunnan järjestelmiä.

Linjaus koskee erillisiä tekoälypalveluja (esimerkiksi keskustelevia tekoälyjä), kunnan tietojärjestelmiin sisältyviä tekoälyominaisuuksia sekä tekoälyä hyödyntäviä lisäosia ja integraatioita.
Hyvinvointi- ja sivistyslautakunta voi antaa omaan palvelutoimintaansa, kuten kouluille ja oppilaiden tekoälyn käyttöön, tätä linjausta täydentäviä ohjeita.
Linjaus korvaa maaliskuussa 2024 julkaistun kunnan tekoälylinjauksen.

24. Periaatteet

Tekoälyn käyttö perustuu julkisen hallinnon arvoperustaan, virkavastuuseen ja viranomaistoimintaa säätelevään lainsäädäntöön. Kuusi periaatetta ohjaa kaikkea käyttöä.

1. **Ihminen vastaa.** Tekoäly ei tee viranomaispäätöksiä eikä käytä julkista valtaa. Vastuu valmistelusta, tiedon oikeellisuudesta ja lopullisesta sisällöstä on aina tehtävästä vastaavalla henkilöllä.
2. **Tarkista aina.** Tekoälyn tuotos voi olla virheellinen, puutteellinen tai vanhentunut. Tekoäly voi keksiä lähteitä, lakiviittauksia ja lukuja. Mitään tekoälyn tuottamaa ei käytetä sellaisenaan.
3. **Hyvä hallinto.** Käyttö ei saa heikentää asian selvittämistä, päätösten perustelemista, puolueettomuutta eikä julkisuusperiaatetta. Hallinnon oikeusperiaatteet (tarkoitussidonnaisuus, suhteellisuus, objektiivisuus, luottamuksensuoja) pätevät myös tekoälyä käytettäessä.
4. **Yhdenvertaisuus.** Tekoälyn tuotoksissa voi olla vinoumia. Tekoälyn luokittelua, suositusta tai arviota ei käytetä henkilöä koskevan ratkaisun perusteena ilman ihmisen itsenäistä arviointia.
5. **Tietosuoja ja tietoturva.** Palveluun syötetään vain tietoa, jonka käsittelyyn palvelu on hyväksytty (luku 25).
6. **Läpinäkyvyys.** Tekoälyn käytön on oltava perusteltavissa ja tarvittaessa jälkikäteen selvitettävissä. Kuntalaiselle kerrotaan, kun hän asioi tekoälyn kanssa.

25. Mitä tekoälyyn saa syöttää

Se, mitä tekoälyyn saa syöttää, riippuu kahdesta asiasta: tiedon luokasta (luku 2) ja siitä, onko palvelu hyväksytty luvun 26 mukaisesti. Muuhun kuin hyväksyttyyn palveluun saa syöttää vain julkista tietoa.

Tieto	Esimerkkejä	Muu palvelu tai henkilökohtainen tili	Hyväksytty palvelu kunnan tunnuksilla
Julkinen	Julkaistut pöytäkirjat, lait, kunnan verkkosivut, tiedotteet	Sallittu	Sallittu
Sisäinen	Valmisteluluonnokset, muistiot, sisäiset ohjeet	Ei sallittu	Sallittu
Henkilötiedot	Nimet yhdessä asian kanssa, yhteystiedot, kuvat ihmisistä, hakemukset	Ei sallittu	Vain jos palvelu on arvioitu ja hyväksytty henkilötietojen käsittelyyn
Salassa pidettävä tai arkaluonteinen	Sosiaali- ja terveystiedot, oppilashuolto, liikesalaisuudet, keskeneräisten hankintojen ja neuvottelujen tiedot, tietoturvatiedot	Ei sallittu	Ei sallittu, ellei palvelua ole erikseen hyväksytty juuri tähän käyttöön
Käyttäjätunnukset ja salasanat	Tunnukset, salasanat, avaimet	Ei koskaan	Ei koskaan

Jos tiedon luokka on epäselvä, tietoa käsitellään tiukemman luokan mukaan ja asiasta kysytään esihenkilöltä tai hallintojohtajalta.

Tekijänoikeudet: palveluun saa syöttää vain aineistoa, jota kunnalla tai käyttäjällä on oikeus käyttää tällä tavalla. Tekoälyn antama lähdeviite tai sitaatti tarkistetaan aina alkuperäisestä lähteestä.

Julkisuus: tekoälylle annettu aineisto ja sen tuotos voivat olla viranomaisen asiakirjoja. Asiaan liittyvä olennainen aineisto tallennetaan asianhallintaan kuten muukin valmisteluaineisto.

26. Hyväksytyt palvelut ja käyttötavat

Työssä käytetään ensisijaisesti kunnan hyväksymiä tekoälypalveluja kunnan omilla käyttäjätunnuksilla. Toimialakohtaisista palveluista päättää toimiala. Yleisistä, koko kuntaa koskevista palveluista ja järjestelmistä sekä luottamushenkilöiden käyttämistä palveluista päättää hallinnon toimiala. Päätöksessä määritellään, mihin tietoluokkiin palvelua saa käyttää. Tietohallinto arvioi palvelun tietoturvan ennen päätöstä ja ylläpitää kunnan yhteistä luetteloa hyväksytyistä ja kielletyistä palveluista. Luettelo julkaistaan intranetissä.

- Muissa kuin hyväksytyissä palveluissa saa käyttää vain julkista tietoa (luku 25).
- Tekoälypalvelua ei yhdistetä kunnan sähköpostiin, kalenteriin, tiedostoihin tai muihin järjestelmiin ilman tietohallinnon hyväksyntää.
- Kunnan tietojärjestelmiin (esimerkiksi talous-, asianhallinta-, henkilöstö- ja arkistointijärjestelmät) sisältyviä tekoälyominaisuuksia ei oteta käyttöön oma-aloitteisesti. Tietohallinto arvioi ne ennen käyttöönottoa yhdessä järjestelmän omistajan kanssa ja käyttöönotosta päättää järjestelmästä vastaava toimiala. Arvioinnissa määritellään käyttötarkoitus, tietoluokat, käyttäjäryhmät, lokitiedot, tietojen säilytys ja ihmisen tarkistusvelvollisuus. Arviointi tehdään osana tiedonhallintalain mukaista muutosvaikutusten arviointia.
- Tekoälyä hyödyntäviä palveluja hankittaessa tekoälyominaisuudet, tietojen käsittelypaikka ja palveluntarjoajan oikeus käyttää kunnan tietoja mallien kouluttamiseen selvitetään osana hankintaa.

Tekoälyä voi käyttää esimerkiksi:

- tekstien, muistioiden, tiedotteiden ja hankekuvausten luonnosteluun
- asiakirjojen jäsentelyyn, kielenhuoltoon ja selkokieliseksi muuttamiseen
- julkisten tai palvelussa käsiteltäväksi hyväksyttyjen asiakirjojen tiivistämiseen
- ideointiin ja vaihtoehtojen hahmottamiseen
- käännösten ensimmäisiin versioihin
- koulutus- ja perehdytysaineiston valmisteluun
- tiedonhakuun ja julkiseen tietoon perustuviin vertailuihin
- laskentaan, aineistojen analysointiin ja ohjelmointiin, kun tieto ja palvelu soveltuvat siihen.

Luettelo ei ole tyhjentävä. Sallittavuus ratkaistaan aina palvelun, tiedon ja käyttötarkoituksen perusteella.
Päätös palvelun käyttöönotosta tehdään kirjallisesti. Päätöksessä mainitaan palvelu, sallitut tietoluokat ja käyttäjäryhmät.

27. Tekoäly viranomaistoiminnassa ja päätöksenteossa

Tekoälyä saa käyttää päätösten valmistelun tukena, mutta valmistelija ja päättäjä tekevät harkinnan itse ja vastaavat lopputuloksesta.
Päätösasiakirjat. Pöytäkirjoissa ja viranhaltijapäätöksissä noudatetaan kunnan sovittua rakennetta ja ulkoasua. Tekoälyllä ei muuteta päätösasiakirjan rakennetta.
Viranhaltijapäätöksen otsikot ovat asian selostus, toimivalta ja päätös. Yhtenäinen rakenne turvaa pöytäkirjojen haettavuuden ja vertailtavuuden pitkällä aikavälillä.

Kiellettyä on käyttää tekoälyä:

- viranomaispäätösten tekemiseen tai päätösvallan siirtämiseen tekoälylle
- henkilöstövalintojen tai henkilöarviointien ratkaisemiseen
- kuntalaisten, asiakkaiden, henkilöstön tai oppilaiden profilointiin
- henkilön oikeuksiin tai asemaan vaikuttaviin ratkaisuihin ilman ihmisen tosiasiallista arviointia

- ainoana tietolähteenä päätöksen perusteena
- harhaanjohtavan, syrjivän tai epäasiallisen sisällön tuottamiseen tai julkaisemiseen
- todellisen henkilön kuvan tai äänen jäljittelyyn ilman tämän lupaa.

Erityistä ennakkoarviointia vaativat käyttötavat, joissa tekoäly käsittelee henkilötietoja laajasti, arvioi tai luokittelee ihmisiä, vaikuttaa palvelujen myöntämiseen, asioi kuntalaisen kanssa ilman ihmistä tai liitetään asiankäsittely- tai päätöksentekojärjestelmään. Näistä tehdään ennen käyttöä tietohallinnon ja toimialan yhteinen arviointi sekä tarvittaessa tietosuojan vaikutustenarviointi. Käyttöönotosta päätetään luvun 26 mukaisesti.

Asiakaspalvelu ja viestintä. Kun kuntalainen asioi tekoälyn kanssa, esimerkiksi verkkosivujen chatissa, siitä kerrotaan selvästi ja ihmisen tavoittaminen on mahdollista. Tekoälyllä tuotettu tai muokattu kuva, video tai ääni merkitään, jos se voisi muuten vaikuttaa aidolta.

Dokumentointi. Tekoälyn käyttö kirjataan, kun sillä on ollut olennainen merkitys päätösasian valmistelussa, oikeudellisessa tai taloudellisessa arviossa, henkilön asemaan vaikuttavassa asiassa tai merkittävän julkaistavan asiakirjan laatimisessa. Asian valmisteluaineistoon kirjataan käytetty palvelu, käyttötarkoitus, tarkistustapa ja vastuuhenkilö. Kielenhuoltoa, muotoilua tai vähäistä ideointia ei tarvitse kirjata.

28. EU:n tekoälyasetus ja muu lainsäädäntö

Kunta on EU:n tekoälyasetuksessa tekoälyjärjestelmän käyttäjä (deployer). Asetuksen velvoitteet tulevat voimaan vaiheittain, ja kesäkuussa 2026 hyväksytty niin sanottu digitaalinen omnibus siirsi korkean riskin velvoitteita myöhemmäksi.

Velvoite	Mitä se tarkoittaa kunnalle	Sovelletaan
Kielletyt käytännöt	Esimerkiksi sosiaalinen pisteytys ja tunteiden tunnistaminen työpaikalla ovat kiellettyjä	2.2.2025 alkaen
Tekoälylukutaito	Kunta tukee henkilöstön tekoälyosaamisen kehittymistä (luku 29)	2.2.2025 alkaen
Läpinäkyvyys	Tekoälyllä tuotetut aidolta näyttävät kuvat, videot ja äänet merkitään. Julkiseksi tiedoksi tarkoitettu tekoälyteksti merkitään, ellei ihminen ole tarkistanut sitä ja vastaa siitä	2.8.2026 alkaen
Korkean riskin järjestelmät (asetuksen liite III)	Esimerkiksi rekrytointiin, koulutukseen tai julkisten etuuksien ja palvelujen myöntämiseen käytettävät järjestelmät. Käyttäjällä on velvoitteita ihmisen valvonnasta, lokitiedoista ja vaikutustenarvioinnista	2.12.2027 alkaen

Kunta ei ota käyttöön korkean riskin tekoälyjärjestelmää ilman luvun 27 ennakkoarviointia, vaikka velvoitteet tulevat sovellettaviksi vasta myöhemmin.

Lisäksi noudatetaan erityisesti:

- hallintolakia, joka sallii asian automaattisen ratkaisemisen vain 8 b luvun tiukoin edellytyksin. Kunta ei vielä käytä tekoälyä asioiden automaattiseen ratkaisemiseen.
- tietosuoja-asetusta ja tietosuojalakia
- julkisuuslakia ja tiedonhallintalakia
- kuntalakia, kunnan hallintosääntöä ja tekijänoikeuslakia.

29. Vastuut ja osaaminen

Jokainen käyttäjä vastaa omalta osaltaan linjauksen noudattamisesta. Noudattaminen on henkilöstölle osa virka- ja työvelvollisuuksia ja luottamushenkilöille osa virkavastuuta. Henkilöstön osalta rikkominen voi johtaa työnantajan toimenpiteisiin.

Taho	Vastuu
Kunnanhallitus	Hyväksyy tekoälylinjauksen osana tätä asiakirjaa
Toimialan johto	Päättää toimialakohtaisista tekoälypalveluista ja vastaa linjauksen noudattamisesta ja osaamisesta toimialallaan
Hyvinvointi- ja sivistyslautakunta	Voi antaa täydentäviä ohjeita omaan palvelutoimintaansa, kuten kouluille
Hallinnon toimiala ja tietohallinto	Päättää yleisistä, koko kuntaa koskevista ja luottamushenkilöiden käyttämistä tekoälypalveluista, arvioi palvelujen tietoturvan, ylläpitää kunnan yhteistä palveluluetteloa, järjestää koulutuksen, antaa käyttöohjeet ja seuraa kehitystä
Tietosuojavastaava	Neuvoo ja valvoo henkilötietojen käsittelyä lakisääteisen tehtävänsä mukaisesti
Esihenkilöt	Varmistavat, että työntekijät suorittavat vuosittaisen koulutuksen tai testin ja noudattavat linjausta
Käyttäjä	Noudattaa linjausta, tarkistaa tuotokset ja kysyy epäselvissä tilanteissa ohjeistusta ennen käyttöä

Osaaminen:

- Jokainen tekoälyä työssään käyttävä suorittaa vuosittain tekoälykoulutuksen tai osaamistestin. Sen voi yhdistää luvun 12 mukaiseen vuosittaiseen tietosuoja- ja tietoturvakoulutukseen tai testiin. Tekoälyn käytön voi aloittaa ennen ensimmäistä suoritusta, kun noudattaa tätä linjausta.
- Koulutus ja testi kattavat vähintään tämän linjauksen, tietoluokat, tuotosten tarkistamisen ja tekoälyn rajoitukset. Perustiedoksi sopii lisäksi esimerkiksi Elements of AI.
- Suoritukset kirjataan. Sisältö päivitetään, kun linjaus tai käytössä olevat palvelut muuttuvat olennaisesti.
- Tekoälyä laajemmin hyödyntävät saavat syventävää koulutusta. Kokemuksia ja hyviä käytäntöjä jaetaan kollegoiden kesken.

Väärinkäytökset ja tietoturvapoikkeamat, kuten vahingossa tekoälyyn syötetyt henkilötiedot, ilmoitetaan heti kunnan poikkeamailmoituskanavaan ja tiedotetaan esihenkilöä. Nopea ilmoitus rajaa vahinkoa.

30. Voimaantulo, seuranta ja päivittäminen

Linjaus tulee voimaan, kun kunnanhallitus on hyväksynyt sen osana tätä asiakirjaa. Linjaus arvioidaan vähintään kerran vuodessa politiikan katselmoinnin yhteydessä sekä aina, kun lainsäädäntö, kunnan käyttämät palvelut tai tunnistetut riskit olennaisesti muuttuvat. Hyväksyttyjen palvelujen luetteloa, käyttöohjeita ja henkilöstön muistilistaa (liite 1) voidaan päivittää ilman kunnanhallituksen päätöstä, jos muutokset eivät muuta linjauksen periaatteita.

OSA IV: Kameravalvonta

Tämä osa koskee kunnan toimitiloissa, kiinteistöillä ja alueilla toteutettavaa kameravalvontaa. Kameravalvonta on henkilötietojen käsittelyä, ja siihen sovelletaan tietosuoja-asetusta, tietosuojalakia, lakia yksityisyyden suojasta työelämässä (16 ja 17 §) sekä julkisuuslakia.

31. Valvonnan suunnittelu ja käyttöönotto

Kameravalvonta suunnitellaan ja dokumentoidaan ennen kameroiden asentamista kohdekuvaukseen, joka on kohdekohtainen kuvaus valvonnan tarkoituksesta, toteutuksesta ja vastuista. Kameravalvonnan omistajana toimii kiinteistöpäällikkö, joka vastaa valvontajärjestelmästä, teknisistä vaatimuksista, merkinnöistä ja kohdekuvausten ylläpidosta. Kohdekuvauksessa nimetään kohteen vastuuhenkilö sekä katselijat ja tallenteiden luovuttamisesta vastaava henkilö. Käyttöönotosta päättää kohteesta vastaava toimialajohtaja. Ennen päätöstä:

- kohteen vastuuhenkilö laatii yhdessä kiinteistöpäällikön kanssa kohdekuvauksen, jossa määritellään valvonnan tarkoitus, kameroiden sijainti ja kuvausalueet, tallennus, säilytysaika, katseluoikeudet ja tekniset ratkaisut
- kohteen vastuuhenkilö arvioi valvonnan tarpeellisuuden ja riskit, ja kun valvonta kohdistuu laajasti yleisölle avoimiin alueisiin tai lapsiin, tehdään tietosuojan vaikutustenarviointi, josta tietosuojavastaava antaa lausunnon
- kohteen vastuuhenkilö vie valvonnan käsiteltäväksi yhteistoimintamenettelyssä, kun valvonta kohdistuu työpaikalle. Työpaikalla tarkoitetaan tiloja ja alueita, joissa kunnan henkilöstö työskentelee tai oleskelee säännöllisesti
- laaditaan tietosuojaseloste ja asennetaan merkinnät luvun 32 mukaisesti

Asennuksen jälkeen kiinteistöpäällikkö tarkistaa, että kuvausalueet vastaavat kohdekuvausta ja kirjaa tarkistuksen. Kohdekuvaus päivitetään aina, kun kameroita lisätään, siirretään tai poistetaan. Kohteen vastuuhenkilö arvioi valvonnan tarpeellisuuden vuosittain, ja tarpeettomaksi käynyt valvonta lopetetaan.
Ennen tämän osan voimaantuloa käyttöön otetusta kameravalvonnasta laaditaan kohdekuvaus ja tietosuojaseloste vuoden kuluessa voimaantulosta. Jos laitteisto ei täytä luvun 35 teknisiä vaatimuksia, puutteet kirjataan kohdekuvaukseen ja korjataan viimeistään laitteiston uusimisen yhteydessä.

32. Tietosuojaseloste ja merkinnät

Kohteen vastuuhenkilö vastaa kameravalvonnan tietosuojaselosteen laadinnasta ja ajantasaisuudesta. Samaan tarkoitukseen käytettävistä kohteista voidaan laatia yhteinen seloste. Selosteessa kerrotaan:

- rekisterinpitäjä ja sen yhteyshenkilö sekä tietosuojavastaavan yhteystiedot
- valvonnan tarkoitus ja käsittelyn oikeusperuste
- valvotut kohteet
- tallennettavat tiedot ja säilytysaika
- tietojen vastaanottajat, kuten poliisi
- tieto siitä, ettei tietoja siirretä EU:n tai ETA:n ulkopuolelle
- rekisteröidyn oikeudet ja oikeus tehdä valitus tietosuojavaltuutetulle

Seloste julkaistaan kunnan verkkosivuilla. Valvotun alueen sisäänkäynneille asennetaan merkintä, josta ilmenevät kameravalvonta, sen tarkoitus, rekisterinpitäjän yhteystiedot ja selosteen saatavuus.

33. Kameroiden sijoittaminen

Kamerat sijoitetaan niin, että ne kuvaavat vain valvonnan tarkoituksen kannalta välttämättömiä alueita.

Sallittua	Ei sallittua
Rakennusten sisäänkäynnit, aulat ja käytävät	Yksittäisen työntekijän työpiste
Kiinteistöjen piha- ja pysäköintialueet	Pukuhuoneet, wc-tilat ja peseytymistilat
Varastot, laite- ja kassatilat	Henkilöstön tauko- ja lepotilat
Ilkivallalle alttiit kohteet	Opetustilat oppituntien aikana
	Naapurikiinteistöt ja yleiset alueet laajemmin kuin valvonnan tarkoitus edellyttää

Äänen tallentaminen ja piilokameroiden käyttö on kielletty.
Jos kamera tallentaa tallenteet omaan tallennusvälineeseensä eikä keskitettyyn järjestelmään, tallenteita ei lähetetä henkilökohtaiseen puhelimeen tai sähköpostiin, vaan ne siirretään vain kunnan laitteelle tai järjestelmään. Tallennusväline suojataan luvattomalta käytöltä ja tallenteet siirretään ja poistetaan siitä säännöllisesti, vähintään säilytysajan välein. Tällaisiin kameroihin sovelletaan luvun 35 teknisiä vaatimuksia soveltuvin osin.

34. Katseluoikeudet, katselu ja lokitus

Katseluoikeudet määritellään kohteittain kohdekuvauksessa nimetyille rooleille ja katselijoita on mahdollisimman vähän. Tallenteita katsotaan vain kirjatusta syystä, kun selvitetään tapahtunutta vahinkoa, rikosta, turvallisuusuhkaa tai työtapaturmaa. Reaaliaikaista kuvaa katsotaan vain, jos se on kohdekuvauksessa määritelty. Katselijan pikaohje on liitteessä 4 ja se sijoitetaan katselupisteen yhteyteen.
Tallenteista ei tehdä hakuja yksityishenkilöiden tai muiden tahojen pyynnöstä, esimerkiksi henkilöiden, ajoneuvojen tai veneiden liikkumisen selvittämiseksi. Poikkeuksena ovat

poliisin pyyntö sekä kunnan omaisuuteen kohdistuneen vahingon tai rikoksen selvittäminen.
Tallenteita katsotaan vain kunnan järjestelmässä ja kunnan laitteella tilassa, jossa sivulliset eivät näe niitä. Järjestelmä tallentaa lokiin katselijan ja ajankohdan. Katselija kirjaa lisäksi tallenteen katselun syyn ja katsotun aikavälin järjestelmään tai jos se ei ole mahdollista, kohdekuvauksessa määriteltyyn katselulokiin. Reaaliaikaisen kuvan seuraamista ei kirjata erikseen. Kiinteistöpäällikkö tarkistaa katseluoikeudet ja lokit vähintään kerran vuodessa. Työelämän tietosuojalain 17 §:ssä tarkoitetuissa tilanteissa, kuten häirinnän tai työtapaturman selvittämisessä, tallenteen käytöstä päättää hallintojohtaja.

35. Säilytys, poisto ja tekniset vaatimukset

Säilytysaika määritellään kohteittain lyhimmäksi tarkoitukseen riittäväksi ajaksi, lähtökohtaisesti enintään 30 vuorokaudeksi ja säilytysaika perustellaan kohdekuvauksessa. Tallenteet poistetaan säilytysajan päätyttyä, ensisijaisesti automaattisesti. Selvitystä varten tarvittava tallenne tallennetaan erikseen, säilytetään asian käsittelyn ajan ja poistetaan sen jälkeen. Tallennus ja poisto kirjataan.

Teknisesti edellytetään, että:

- käytetään kunnan hyväksymää järjestelmää ja laitteet kirjataan laiterekisteriin
- tallennin on lukitussa tilassa ja tallenteet salataan
- järjestelmään kirjaudutaan henkilökohtaisilla tunnuksilla, oletussalasanat vaihdetaan ja ohjelmistot pidetään ajan tasalla
- etäkatselussa käytetään monivaiheista tunnistautumista eikä kameroihin avata suoria yhteyksiä internetistä
- pilvipalvelun tarjoajan sekä tallenteita katselevan tai järjestelmää huoltavan ulkopuolisen palveluntuottajan kanssa tehdään tietojenkäsittelysopimus, ja tiedot säilytetään EU:n tai ETA:n alueella

36. Tallenteiden luovuttaminen

Poliisille tallenne luovutetaan poliisin kirjallisesta pyynnöstä tai kunnan rikosilmoituksen liitteenä. Tallenteesta luovutetaan vain pyydetty aikaväli suojatulla tavalla ja luovutuksen tekee kohdekuvauksessa nimetty henkilö.
Rekisteröidylle annetaan pyynnöstä häntä itseään koskeva tallenne tietosuoja-asetuksen 15 artiklan mukaisesti. Pyytäjää pyydetään todistamaan henkilöllisyys, yksilöimään aika ja paikka ja pyyntö käsitellään kuukauden kuluessa. Muiden henkilöiden kuvat peitetään tai tallenne näytetään kunnan tiloissa.
Tallennetta tai kuvailutietoa tallenteesta ei luovuteta:

- muille kuin poliisille, rekisteröidylle tai taholle, jolla on laissa säädetty oikeus saada se
- vakuutusyhtiölle, medialle, toiselle kuntalaiselle tai huoltajalle toista henkilöä koskevana

- rekisteröidylle, jos luovutus paljastaisi muiden henkilöiden tietoja eikä niitä voida peittää
- jos tallenne on jo poistunut säilytysajan päätyttyä

Luovutukset kirjataan. Tietopyynnöt ratkaistaan julkisuuslain perusteella, ja kielteisestä ratkaisusta annetaan pyynnöstä valituskelpoinen päätös.

37. Kielletyt menettelyt

Kameravalvonnassa on kiellettyä:

- asentaa kamera ilman hyväksyttyä kohdekuvausta ja arvioita
- muuttaa kuvausalueita päivittämättä kohdekuvausta
- katsella tallenteita muusta kuin kirjatusta syystä
- kopioida tallenteita omalle laitteelle tai tallentaa kuvia näytöltä muilla laitteilla
- näyttää tallenteita ulkopuolisille, jakaa niitä sosiaalisessa mediassa tai tehdä niistä hakuja ulkopuolisten pyynnöstä
- käyttää tallenteita työsuorituksen seurantaan

Väärin perustein tehty katselu tai luovutus on henkilötietojen tietoturvaloukkaus, ja se ilmoitetaan liitteen 2 mukaisesti.

Liite 1: Tekoälyn muistilista henkilöstölle

Kokeile tekoälyä rohkeasti työssäsi, kun onnistuminen hyödyttää ja virhe ei aiheuta vahinkoa.

Ennen käyttöä kysy itseltäsi

1. Onko palvelu hyväksytty toimialallani ja käytänkö kunnan tunnuksia?
2. Mitä tietoja syötän? Onko joukossa henkilötietoja tai salassa pidettävää?
3. Voiko virheellinen tuotos vahingoittaa ihmistä, kuntaa tai kolmatta osapuolta?
4. Vaikuttaako käyttö jonkun oikeuksiin tai palvelujen saamiseen?
5. Pystynkö tarkistamaan tuotoksen luotettavasti?
6. Pitääkö käyttö kirjata?

Älä koskaan

- syötä avoimeen palveluun henkilötietoja, kuvia ihmisistä, salassa pidettävää tai luottamuksellista tietoa
- syötä käyttäjätunnuksia tai salasanoja mihinkään tekoälypalveluun
- käytä tekoälyn tuotosta tarkistamatta
- anna tekoälyn ratkaista asiaa puolestasi
- yhdistä tekoälypalvelua kunnan järjestelmiin tai ota uusia tekoälyominaisuuksia käyttöön ilman hyväksyntää.

Näin saat paremman tuloksen

- Kerro tarkasti, mitä haluat: tarkoitus, kohderyhmä, pituus ja sävy. Anna esimerkki halutusta lopputuloksesta.
- Anna tekoälylle lähdeteksti, josta vastaus haetaan. Se vähentää keksittyjä tietoja.
- Jaa iso tehtävä pienempiin osiin ja ohjaa jatkokysymyksillä.
- Tarkista luvut, nimet, päivämäärät, lakiviittaukset ja lähteet alkuperäisestä lähteestä.

Epäselvissä tilanteissa kysy esihenkilöltä tai hallintojohtajalta ennen käyttöä.

Liite 2: Toimintaohje tietosuoja- ja tietoturvapoikkeamissa

Ohje kertoo, miten toimitaan, kun havaitaan tai epäillään tietosuoja- tai tietoturvapoikkeamaa. Ohje koskee kaikkia, joihin tätä asiakirjaa sovelletaan. Nopea ilmoitus on tärkein yksittäinen keino rajata vahinkoa, joten ilmoitus tehdään jo epäilystä. Varmuutta ei tarvitse odottaa, eikä ilmoittajaa syyllistetä.

Mikä on poikkeama

Poikkeama on tilanne, jossa tieto on joutunut tai voi joutua vääriin käsiin, kadonnut, muuttunut tai ollut poissa käytöstä, tai jossa kunnan laitteisiin tai järjestelmiin on kohdistunut hyökkäys. Esimerkkejä:

- sähköposti tai liite on lähetetty väärälle vastaanottajalle
- kirje on postitettu väärään osoitteeseen tai paperiaineisto on kadonnut
- kunnan laite tai muistiväline on kadonnut tai varastettu
- tietojenkalasteluviestin linkkiä on klikattu tai tunnukset on annettu ulkopuoliselle
- laitteessa on haittaohjelma tai tiedostot ovat salautuneet
- tunnuksilla on kirjauduttu tuntemattomasta paikasta
- henkilötietoja tai salassa pidettävää tietoa on syötetty tekoälypalveluun, johon sitä ei saa syöttää
- käyttöoikeudet ovat liian laajat tai tietoja on katsottu ilman työtehtävän tarvetta

Havaitsijan toimet

1. **Ilmoita heti** kunnan poikkeamailmoituskanavaan. Jos kyse on teknisestä uhasta tai häiriöstä, kuten haittaohjelmasta, kalastelusta tai kadonneesta laitteesta, ilmoita myös ICT-palveluntuottajan tukeen. Kerro asiasta esihenkilöllesi.
2. **Rajoita vahinkoa**, jos voit tehdä sen turvallisesti:
    - irrota haittaohjelmaa epäiltäessä laite verkosta, mutta älä sammuta sitä
    - vaihda salasana ICT-tuen ohjeen mukaan, jos tunnukset ovat voineet vuotaa
    - pyydä väärää vastaanottajaa poistamaan viesti ja vahvistamaan poisto kirjallisesti
    - pyydä ICT-tukea lukitsemaan kadonnut laite
3. **Kirjaa** havaintosi heti: mitä tapahtui, milloin, mitä tietoja tai laitteita asia koskee, keitä tiedot koskevat ja mitä olet jo tehnyt.
4. **Älä** poista viestejä, lokeja tai tiedostoja, älä yritä itse poistaa haittaohjelmaa, maksaa lunnaita tai kertoa asiasta kunnan ulkopuolelle tai sosiaalisessa mediassa.

Käsittely ja vastuut

Vaihe	Vastuu	Aikaraja
Ilmoituksen vastaanotto ja kirjaus poikkeama- ja loukkausrekisteriin. Merkittävistä poikkeamista ilmoitetaan heti hallintojohtajalle.	Hallintojohtaja ja tietosuojavastaava	Heti

Vaihe	Vastuu	Aikaraja
Tekninen selvitys ja vahingon rajaaminen	ICT-palveluntuottaja	Heti
Riskin arviointi: koskeeko henkilötietoja, kuinka monta henkilöä, kuinka arkaluonteisia tietoja ja mitä haittaa voi aiheutua	Tietosuojavastaava, esihenkilö ja ICT-palveluntuottaja	Ensimmäisen vuorokauden aikana
Ilmoitus tietosuojavaltuutetun toimistolle, ellei ole epätodennäköistä, että loukkauksesta aiheutuu riskiä rekisteröidyille	Tietosuojavastaava valmistelee, hallintojohtaja tai hänen nimeämänsä tekee	72 tunnin kuluessa havaitsemisesta
Ilmoitus rekisteröidyille, jos riski on korkea	Asian omistava toimiala tietosuojavastaavan tuella	Ilman aiheetonta viivytystä
Ilmoitus Kyberturvallisuuskeskukselle merkittävissä tietoturvapoikkeamissa	Hallintojohtaja ICT-palveluntuottajan tuella	Mahdollisimman pian
Rikosilmoitus poliisille rikosta epäiltäessä	Hallintojohtaja	Mahdollisimman pian
Viestintä henkilöstölle, kuntalaisille ja medialle	Kunnanjohtaja, valmistelu hallintojohtaja ja viestinnästä vastaava	Tarpeen mukaan
Juurisyyn selvitys, korjaavat toimenpiteet ja raportointi tietosuoja- ja tietoturvatyöryhmälle	Tietosuoja- ja tietoturvatyöryhmä	Kuukauden kuluessa

Merkittävä poikkeama on poikkeama, josta todennäköisesti ilmoitetaan viranomaiselle tai rekisteröidyille, joka koskee salassa pidettävää tai laajaa henkilötietoaineistoa tai joka häiritsee palvelujen toimintaa. Aikaraja tietosuojavaltuutetulle alkaa siitä, kun kunta on havainnut loukkauksen. Siksi ilmoitus on tehtävä myös viikonloppuna tai lomakaudella. Jos kaikkia tietoja ei vielä ole, ilmoitus tehdään puutteellisena ja täydennetään myöhemmin. Kaikki poikkeamat raportoidaan vuosittain tietotilinpäätöksessä ilman henkilötietoja.

Yhteystiedot

Taho	Yhteystieto
Kunnan poikkeamailmoituskanava	[täydennetään]
ICT-palveluntuottajan tuki	[täydennetään]
Tietosuojavastaava	[täydennetään]
Hallintojohtaja	[täydennetään]
Tietosuojavaltuutetun toimisto	tietosuoja.fi, sähköinen ilmoituslomake
Kyberturvallisuuskeskus	kyberturvallisuuskeskus.fi, sähköinen ilmoituslomake

Liite 3: Pikaohje poikkeamatilanteeseen

Huomasitko tietoturva- tai tietosuojapoikkeaman? Ilmoita heti, jo epäilystä.
Esimerkiksi: viesti väärälle vastaanottajalle, kadonnut laite tai paperi, klikattu kalastelulinkki, outo kirjautuminen tai henkilötieto tekoälyssä.

1. **Ilmoita** poikkeamailmoituskanavaan. Teknisestä uhasta tai häiriöstä myös ICT-tukeen. Kerro esihenkilöllesi.
2. **Rajoita:** irrota saastunut laite verkosta, vaihda salasana, pyydä väärää vastaanottajaa poistamaan viesti.
3. **Kirjaa:** mitä, milloin, mitä tietoja ja mitä olet tehnyt.
4. **Älä** sammuta laitetta, poista todisteita, maksa lunnaita tai kerro asiasta ulkopuolisille.

Kunnalla on 72 tuntia aikaa ilmoittaa henkilötietojen loukkauksesta tietosuojavaltuutetun toimistolle. Jokainen tunti on tärkeä. Ilmoittajaa ei syyllistetä.

Kenelle	Yhteystieto
Poikkeamailmoituskanava	[osoite]
ICT-tuki	[puhelin ja sähköposti]
Tietosuojavastaava	[puhelin ja sähköposti]

Liite 4: Kameravalvonnan huoneentaulu

Katso tallenteita vain kirjatusta syystä ja vain, jos sinulla on katseluoikeus tähän kohteeseen.

Hyväksyttävä syy on tapahtuneen vahingon, rikoksen, turvallisuusuhan tai työtapaturman selvittäminen.

1. **Katsele** vain kunnan järjestelmässä ja kunnan laitteella, niin että sivulliset eivät näe tallenteita.
2. **Kirjaa** katselun syy ja katsottu aikaväli järjestelmään tai katselulokiin.
3. **Tallenna erikseen** vain selvitystä varten tarvittava tallenne, ja kirjaa tallennus.
4. **Luovuta** tallenne vain poliisille kirjallisesta pyynnöstä tai rekisteröidylle hänen omista tiedoistaan, ja vain, jos olet nimetty luovuttaja.

Älä

- tee hakuja yksityishenkilöiden pyynnöstä, esimerkiksi henkilöiden, ajoneuvojen tai veneiden liikkumisesta
    - ohjaa pyytäjä tekemään tarvittaessa rikosilmoitus!
- kopioi tallenteita omalle laitteelle tai kuvaa näyttöä
- näytä tallenteita ulkopuolisille tai jaa niitä eteenpäin
- käytä tallenteita työsuorituksen seurantaan.

Jos tallenteita on katsottu tai luovutettu väärin perustein, ilmoita asiasta heti poikkeamailmoituskanavaan.

Kenelle	Yhteystieto
Kohteen vastuuhenkilö	[täydennetään kohteittain]
Kiinteistöpäällikkö	[täydennetään]
Poikkeamailmoituskanava	[osoite]

RANTA SALMI

Eliel Saarisen tie 2 | 58900 Rantasalmi
rantasalmen.kunta@rantasalmi.fi

rantasalmi.fi