Vieremän kunnan tietoturva- ja tietosuojapolitiikka

Hyväksytty: Vieremän kunnanhallitus 16.4.2018 § 91

Sisällysluettelo

1 Vieremän kunnan tietoturva- ja tietosuojapolitiikka

Tietoturva- ja tietosuojapolitiikka on kunnan ylimmän johdon hyväksymä strateginen asiakirja, jolla otetaan kantaa tietosuojan ja tietoturvan kehittämiseen. Politiikan tavoitteena on luoda yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietosuoja- ja tietoturvatason toteuttamiseksi. Politiikassa määritellään kunnan tietosuoja- ja tietoturvatyön tavoitteet, vastuut, toimintatavat, valvonta ja seurantajärjestelmä. Politiikalla luodaan edellytykset toiminnan pitkäjänteiseen kehittämiseen. Työssä onnistuminen edellyttää kunnan johdon sitoutumista tietosuoja- ja tietoturvatyön tukemiseen.

Tietoturva- ja tietosuojapolitiikkaa ja sen perusteella annettuja ohjeita ja määräyksiä noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia Vieremän kunnan palveluksessa olevia viranhaltijoita, työntekijöitä ja luottamushenkilöitä sekä erikseen toimeksiantosopimuksin sovittuja ulkopuolisia palvelun toteuttajia.

1.1 Tietoturva ja tietosuoja

- ***Tietoturvalla*** tarkoitetaan eri muodoissa olevien tietojen (mm. sähköisesti tallennettu, välitetty tai rekisteröity tieto, suullinen puhuttu, postin kuljettama tai paperilla oleva tieto) suojaamista erilaisilta uhkatekijöiltä varmistaen palvelutoiminnan jatkuvuus sekä minimoiden toimintaan tai asiakkaiden tietoihin liittyvät riskitekijät.

- ***Tietosuojalla*** tarkoitetaan ihmisten yksityisyyden kunnioittamista ja suojelemista oikeudellisia säännöksiä ja organisaation ohjeita noudattaen.

Tietosuojaa säätelee Suomessa useita lakeja eri toimialoilla, mutta keskeinen tietosuojaan liittyvä lainsäädäntö on EU:n yleinen tietosuoja-asetus ja sen kansallinen tietosuojalaki. Kaikki viranomaiset sekä yritykset, jotka käsittelevät asiakkaiden henkilötietoja, ovat velvollisia noudattamaan tietosuojaan liittyvää lainsäädäntöä. Lainmukaisuutta ja tietosuojakäytäntöjä Suomessa valvoo kansallinen tietosuojaviranomainen.

1.2 Kunnan tietoturvallisuuden kehittämisvisio

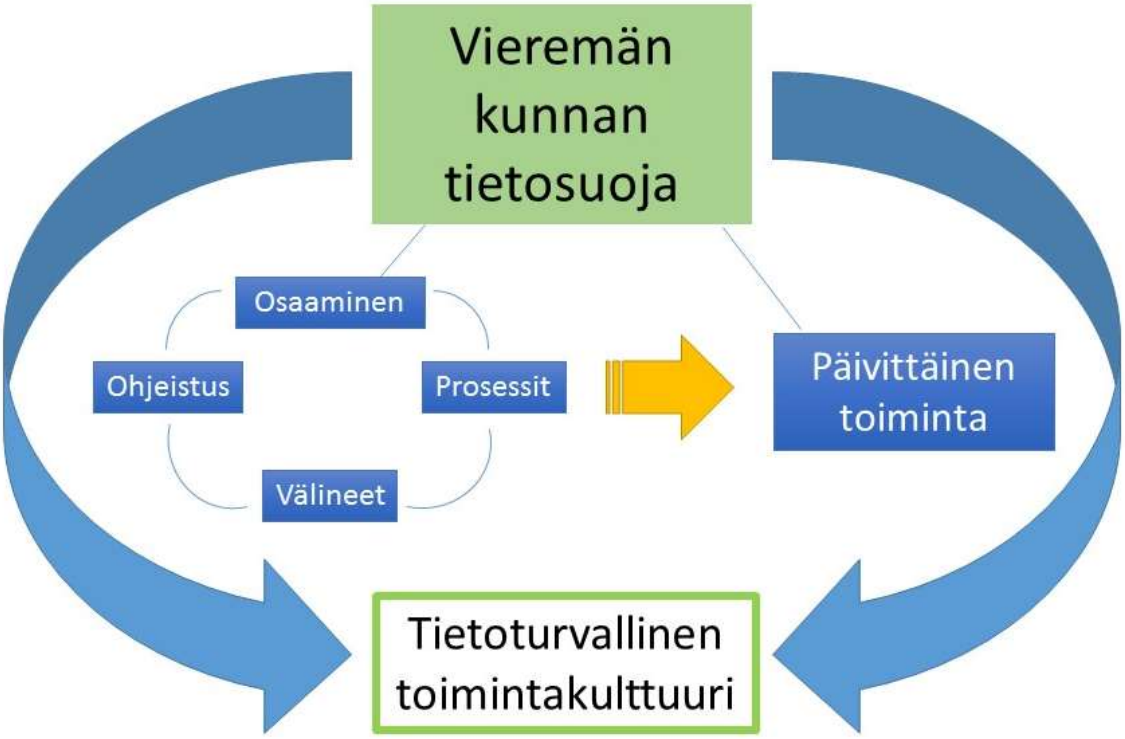
Vieremän kuntastrategian 2017–2021 vision mukaan Vieremä on Pohjois-Savon maakunnan metalli- ja teknologiateollisuuden keskus, jossa on erinomaiset mahdollisuudet hyvinvointiin, asumiseen ja yrittämiseen. Vieremä on maatalouden ja siihen liittyvän biotalouden sekä maatalousrobotiikan innovatiivinen edelläkävijä. Vieremä on aktiivinen toimija ja vaikuttaja Ylä-Savon seutukunnalla ja Pohjois-Savon maakunnassa.

Vieremän kunta tuottaa monikanavaiset palvelut luotettavalla ja tietoturvallisella ICT-infrastruktuurilla. Tietosuoja ja tietoturva ovat kiinteä osa johtamista, riskienhallintaa, palvelutoimintaa ja esimiestyötä. Tietosuojan ja tietoturvan hallinta on kustannustehokasta ja keskitetysti koordinoitua jokapäiväistä toimintaa palveluiden jatkuvuuden turvaamiseksi. Tietoturvan hallinta on hyvällä tasolla ja toimintaan vaikuttavia tietoturvan häiriötilanteita esiintyy mahdollisimman vähän. Vieremän kunnan tietosuoja- ja tietoturvatyöllä taataan sekä oman henkilöstön että asiakkaiden luottamuksellinen tietojen käsittely kaikissa eri toiminnoissa ja palveluissa.

2 Tietoturva- ja tietosuojatyön tavoitteet

Tavoitteena on luoda ja ylläpitää tietoturvallisia toiminta- ja palveluympäristöjä sekä luotettavien ratkaisuiden avulla mahdollistaa tuki tehokkaalle työskentelylle ja moderneille työtavoille ajasta, paikasta tai työvälineistä riippumatta. Tietosuoja ja tietoturva ovat kiinteä osa kunnan kokonaisarkkitehtuurityötä ja tietojärjestelmien kehitystyötä. Tietoturvaa ja tietosuojaa arvioidaan jo suunniteltaessa tietojärjestelmähankintoja ja ulkoistettaessa henkilötietoja sisältäviä palveluja.

Tietoturvan tärkeyttä on lisännyt kansalaisille suunnattujen sähköisten palvelujen laajentuminen, tietojärjestelmien etä- ja mobiilikäyttö, pilvipalvelut, organisaatioiden kuten esimerkiksi Ylä-Savon kuntien yhteistyö palvelujen järjestämisessä sekä laaja palveluntuottajien verkosto. Tietosuoja- ja tietoturvatyössä huomioidaan myös seudullinen sekä kansallinen palveluarkkitehtuuri. Lähtökohtana on soveltaa kansallisia tietoturvaohjeistuksia ja kansainvälisten tietoturvastandardien mukaisia parhaita käytäntöjä ja suojata tiedot niin normaali- kuin häiriötilanteissa riittävin hallinnollisin ja teknisin toimenpitein.



Kuva: Tietosuojan tavoitetila

Työllä pyritään varmistamaan:

- Tietojen luottamuksellisuus: tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeudet.
- Tietojen eheys: tiedon oikeellisuus ja suojaus on järjestetty niin, että tietoa ei voi tahallisesti tai tahattomasti muuttaa vaarantaen toiminnan luotettavuutta.
- Palveluiden ja tietojen saatavuus: tieto on saatavissa ja käytettävissä silloin, kun sitä palvelutoiminnassa tarvitaan.

Vieremän kunnan tietosuoja- ja tietoturvatoiminnan tavoitteena on luoda ja kehittää tietoturvan ja tietosuojan hallintajärjestelmää, jolla:
1. varmistetaan lainmukaisuuden, kansainvälisten sekä kansallisten velvoitteiden toteutuminen
2. tunnistetaan kunnan toiminnan kannalta merkittävät tietosuojaan ja tietoturvaan kohdistuvat uhkatekijät, joita hallinnoidaan hyväksytyllä tasolla.

3. turvataan tietojärjestelmien, tietoverkkojen ja tietojenkäsittelylaitteiden keskeytymätön toiminta, havaitaan ja estetään tietojen luvaton käyttö, tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen ja minimoidaan niistä aiheutuvat vahingot.
4. varmistetaan henkilöstön ja luottamushenkilöiden riittävä tietosuoja- ja tietoturvaosaaminen ja sitoutetaan heidät hyvän tietoturvatyön toteuttamiseen.
5. määritellään tietosuojaorganisaation säännölliset ja määrämuotoiset tehtävät (vuosikello), jotta voidaan taata niiden hoitamiseen tarvittava aika ja seurata niiden toteutumista.
6. varmistetaan kyky toimia häiriö- ja poikkeamatilanteissa.
7. toteutetaan seurantaa ja valvontaa sekä teknisin keinoin, että henkilöiden, palveluntoimittajien ja sidosryhmien toimesta.
8. voidaan seurata ja mitata tietoturvatasoa, ja osoittaa tehdyt toimenpiteet velvoitteiden täyttymiseksi.

3 Tietoturva- ja tietosuojatyön hallinnointi, roolit sekä vastuut

3.1 Kunnanhallituksen ja johdon vastuut

Kuntalain ja Vieremän kunnan hallintosäännön mukaisesti kokonaisvaltainen riskienhallinta ja sitä kautta tietoturvan toteuttamisen kokonaisvastuu on kunnanhallituksella ja kunnanjohtajalla. Kunnanhallitus johtaa ja valvoo tietoturva- ja tietosuojatyötä sekä päättää Vieremän kunnan tietoturvallisuuden kehittämisen tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista hyväksymällä tietoturva- ja tietosuojapolitiikan sekä nimeämällä tietosuoja- ja tietoturvavastaavan. Kunnan johdon ja esimiesten vastuulla on sitoutua tietoturvatyön jatkuvaan kehittämiseen, huolehtia alaistensa riittävästä perehdytyksestä ja tietoturva- ja tietosuojatyön jatkuvuudesta.

3.2 Tietohallinnon ohjausryhmä

Vieremän kunnan tietohallinto-ohjelman 2018–2021 mukaan (valtuusto 18.9.2017 § 86) kunnan tietohallinnon ohjausryhmä vastaa kunnan tietoturvan ja tietosuojan lainsäädännön mukaisesta järjestämisestä. Tietohallinnon ohjausryhmä muodostuu kunnan johtoryhmästä sekä tietohallinto-, tietoturva- ja tietosuojavastaavasta. Kunnan johtoryhmään kuuluvat hallintosäännön mukaisesti kunnanjohtaja, hallintojohtaja, sivistysjohtaja ja tekninen johtaja. Kunnanhallitus voi asettaa johtoryhmään myös luottamushenkilön. Hallintosäännön mukaan palvelusihteeri toimii kunnan tietohallinto-, tietoturva- ja tietosuojavastaavana. Tietohallintovastaava valmistelee ja panee täytäntöön ohjausryhmän päätökset. Ohjausryhmä kokoontuu tarvittaessa. Kunnan tietohallinnon ohjausryhmä toimii yhteistyössä YSITin asiakasvastaavan kanssa.

Tietohallinnon ohjausryhmän tehtävät ovat:

- Käsittelee, kommentoi, antaa lausuntoja sekä hyväksyy tietoturvaan, kyberturvallisuuteen ja tietosuojaan liittyviä kunnan ohjeita, linjauksia ja asioita
- Käsittelee merkittävät tietoturvaan ja tietosuojaan liittyvät poikkeamat
- Käsittelee ja hyväksyy osaltaan projektit/hankkeet sovituissa pisteissä
- Kehittää ja edistää kunnan tietoturvan ja tietosuojan toteutumista

3.3 Tietosuojavastaava ja tietoturvavastaava

Tietoturvavastaavana toimii palvelusihteeri, joka vastaa ja valmistelee:

- Menetelmien kehittämisestä tietoturvan arvioimiseen, parantamiseen ja ylläpitämiseen
- Tietoturvallisten toimintaperiaatteiden toteutuksesta
- Säännöllisistä auditoinneista, tietoturvavastaavalla on johdon antama valtuutus tietoturvallisuuskartoitusten tekemiseen ja havaittujen heikkouksien parantamiseen.
- Tietoturvatietoisuuden lisäämisestä ja ylläpidosta.
- Tietoturvaohjeiden noudattamisen valvomisesta ja tietoturvatason arvioinnista koko organisaatiossa.

Tietosuojavastaavana toimii palvelusihteeri, jonka tehtäviin tietosuoja-asetuksen mukaisesti kuuluu:

- Asetuksen vaatimusten täytäntöönpano ja soveltaminen organisaatiossa
- Organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä
- Dokumentaation laatimisen, saatavuuden ja säilyttämisen valvonta
- Ilmoitusvelvollisuuden toteutumisen seuranta
- Vaikutusten arviointien tekemisen tukeminen ja valvonta
- Yhteistyö valvontaviranomaisen kanssa
- Tietosuojan tietoisuusohjelman rakentaminen ja kouluttaminen henkilöstölle
- Rekisteröityjen oikeuksien toteuttamisen tukeminen
- Käsittelytoimiin liittyvän riskin asianmukainen huomiointi tehtävien suorittamisessa

Poikkeusolojen johtoryhmän tiedotusvastaavaksi on nimetty hallintojohtaja, jolla on tiedotusvastuu ulkopuolelle häiriö- ja poikkeamatilanteissa. Hallintojohtaja myös toimii palvelusihteerin sijaisena tietosuoja- ja tietoturvavastaavan tehtävien osalta.

Seuraavassa on listattu tärkeimpiä tietosuoja-asetuksen määrittämiä tietosuojavastaavan asemaan ja tehtävänkuvaan liittyviä seikkoja:

- Riippumaton asema organisaatiossa
- Raportoi suoraan rekisterinpitäjän tai käsittelijän ylimmälle johdolle
- Otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkiin tietosuojaan liittyviin kysymyksiin
- Pätevyysvaatimus tietosuojan alalta: tietosuojalainsäädäntötuntemus, lain vaatimusten soveltamisosaaminen ja alan käytäntöjen tuntemus
- Voi olla rekisterinpitäjän tai käsittelijän palkkalistoilla, tai ulkoistettu palveluntuottajalle
- Taattava tarvittavat resurssit sekä asianmukainen pääsy henkilötietoihin ja niiden käsittelytoimiin tietosuojavastaavan tehtävien hoitamiseksi
- Tehtävä yhteistyötä useiden organisaation yksiköiden kanssa
- Julkinen yhteyspiste valvontaviranomaisen ja rekisteröityjen suuntaan
- Salassapitovelvollisuus
- Ei saa erottaa tai rangaista tietosuojavastaavan tehtävien hoitamisen vuoksi
- Voi suorittaa muitakin tehtäviä tietosuojavastaavan tehtävien ohella kuitenkin niin, ettei niistä aiheudu eturistiriitoja.

3.4 Toimialojen ja tytäryhtiöiden vastuut

Toimialojen ja tytäryhtiöiden johtajat vastaavat tietoturvapolitiikan ja -ohjeiden noudattamisesta toiminnassaan. Määritelty tietoturvataso on myös vaadittava ICT-ostopalveluiden toimittajilta läpi koko alihankintaketjun. Johtajien ja nimettyjen vastuuhenkilöiden tulee tuntea toimialansa erityispiirteet, lainsäädäntö ja selventää tietoturvavastuut sekä ICT-varautuminen osaksi kokonaisvaltaista johtamista. Tietojärjestelmien ja tietovarastojen omistajat sekä pääkäyttäjät vastaavat järjestelmien tietoturvasta ja sen jatkuvasta kehittämisestä.

3.5 Esimiesten ja pääkäyttäjien vastuut

Esimiesten vastuulla on huolehtia työnantajaa koskevien lakisääteisten tietoturva- ja tietosuojavelvoitteiden toteutumisesta. Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa.

Esimiehet huolehtivat loppukäyttäjän riittävästä perehdytyksestä Vieremän kunnan tietoturvakäytänteisiin ja varmistavat, että jokainen ymmärtää niiden merkityksen työtehtävissään.

Esimiesten ja pääkäyttäjien vastuulla on myös huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa ja että työsuhteen päättyessä käyttöoikeudet tietojärjestelmistä poistetaan ja työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden. Esimiehiltä odotetaan esimerkillistä sekä vastuullista tietoturvakäyttäytymistä. Esimiehillä ja pääkäyttäjillä on raportointivelvollisuus tietoturvapoikkeamista tietoturva- ja tietosuojavastaavalle.

Etätyössä esimies määrittelee työtehtävät, joita alainen voi tehdä. Etätyön tekeminen pyritään rajaamaan sähköiseen tietoaineistoon, jonka paljastuminen ei vaaranna tietoturvaa ja tietosuojaa. Esimiehellä on velvollisuus tarkistaa, että työntekijällä on etätyön suorittamiseksi riittävät taidot ja tietämys päätelaitteiden ja niillä käsiteltävien tietojen tietoturvallisuudesta. Etätyössä korostuu työntekijän henkilökohtainen vastuu siitä, että luottamukselliset tiedot ovat vain niiden käyttöön oikeutettujen saatavissa ja vain työtehtävien edellyttämässä laajuudessa. Etätyössä on noudatettava hyvän tiedonhallinnan käytänteitä ja erityistä huolellisuusvelvoitetta tietosuojan turvaamiseksi.

3.6 Työntekijöiden vastuut

Kunnan työntekijän velvollisuus on allekirjoittaa salassapito- ja vaitiolositoumus sekä suorittaa hyväksytysti kulloinkin voimassa oleva tietoturva- tai tietosuojakoulutus säännöllisin väliajoin.

Työntekijällä on vastuu noudattaa hyväksyttyjä tietoturvaohjeita ja huolehtia päivittäisissä työtehtävissä hyvän tiedonhallintatavan käytänteistä. Työntekijän vastuulla on myös huolehtia käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokittelusta sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä. Tietojen säilytys- tai arkistointiajan päätyttyä ne on hävitettävä ohjeiden mukaisesti. Työntekijällä on velvollisuus raportoida tietoturvaongelmista oman organisaation tietoturva- tai tietosuojavastaavalle.

Työntekijä, joka luo tai tuottaa tietoa, määrittelee tiedon julkisuuden ja sen, kenellä on oikeus käsitellä tietoa. Tiedon tuottajat vastaavat tiedon luotettavuudesta ja siitä, että tieto on niiden käytettävissä, jotka tietoa tarvitsevat.

3.7 Palveluostoihin liittyvät vastuut

Ostopalveluna hankitun ICT–palvelun operatiivisesta ja teknisestä tietoturvasta ja sen ohjeistamisesta vastaavat palveluntuottajat, joille palvelun toteutus on sopimuspohjaisesti luovutettu. ICT-palveluiden tuottajien tehtävänä on laatia ja ylläpitää kunnan tietohallinnon hyväksymien palvelukonseptien mukaisia käytännön tietoturvaohjeita.

Tilaajan tulee huolehtia, että kaikkiin tarjouspyyntöihin ja palvelusopimuksiin sisällytetään tietohallinnon ylläpitämät yleiset tietoturvavaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla sekä häiriötilanteiden toimintamallit ja selkeä vastuunjako läpi koko palveluketjun. Tilaajan tehtävä on vaatia palveluntuottajaa raportoimaan ja tiedottamaan merkittävistä tietoturvaan kohdistuvista poikkeustilanteista, riskitekijöistä sekä uhkatilanteista välittömästi palvelusopimuksessa määritellyille yhteyshenkilöille. Tilaajan on huolehdittava, että palveluntuottaja toimii vaatimusten mukaisesti.

3.8 Luottamushenkilöiden vastuut

Luottamushenkilö hoitaa tointaan virkavastuulla. Luottamushenkilöt ovat tehtävässään velvollisia käsittelemään ja säilyttämään huolellisesti käsiteltävänään olevia paperisia ja sähköisiä asiakirjoja.

Luottamushenkilöitä koskevat samat salassapitosäännöt kuin viranhaltijoita ja työntekijöitä. Luottamushenkilöille laaditaan oma ohje tietoturva- ja tietosuojaperiaatteiden noudattamisesta.

3.9 Seudullinen tietosuoja- ja tietoturvatyöryhmä

Ylä-Savon tasolla (Iisalmi, Kiuruvesi, Sonkajärvi, Vieremä ja näiden omistamat yhtiöt ja säätiöt) tietohallintovastaavien/tietosuojavastaavien/tietoturvavastaavien yhteinen tietohallintotyöryhmä koordinoi tietoturvanäkemyksiä seudullisesti.

4 Tietoturva- ja tietosuojaperiaatteet (hallintamalli)

Vieremän kunnan tulee pystyä osoittamaan, että se toteuttaa EU:n yleisen tietosuoja-asetuksen ja lain velvoitteet sekä tietoturva- ja tietosuojatyölle asettamansa tavoitteet tietojen käsittelyssä. Seuraavassa osioissa on kuvattu sekä tietoturvallisuuden että tietosuojan hallinnan eri osa-alueet, jotka kunnan tulee ottaa huomioon tietoturva- ja tietosuojatyössä.

4.1 Tietoturva- ja tietosuojaorganisaatio

Tietoturva- ja tietosuojaorganisaatio on määritetty rooleineen ja vastuineen. Myös henkilöstölle on määritelty tietoturvavastuut. Tietoturvan hallintatehtävät määritellään vuosikelloon. Tietoturvaa mitataan, todennetaan ja kehitetään säännöllisesti. Tietoturvaa voidaan todentaa esimerkiksi teknisellä testauksella ja hallinnollisten prosessien auditoimisella.

4.2 Henkilötietojen inventaario / luettelo rekistereistä ja käsittelijöistä

Vieremän kunta määrittelee keskitetyn, ajantasaisen ja kattavan luettelon henkilötietojen käsittelyn ja rekisterien kokonaisuudesta.

Henkilötietojen käsittelyyn liittyvät liiketoimintaprosessit, järjestelmät ja kumppanit kartoitetaan ja dokumentoidaan luetteloon, jota katselmoidaan määräajoin tapahtuneiden muutosten tunnistamiseksi. Näiden muutosten mukaisten vaikutusten päivittäminen luetteloon on esimiesten vastuulla. Prosessia koordinoi tietosuojavastaava.

4.3 Riskienarviointi ja -hallinta

Tietosuoja-asetus velvoittaa rekisterinpitäjää ottamaan huomioon uusimman tekniikan ja toteuttamiskustannukset sekä toisaalta arvioimaan tietoturvakeinojen kohtuullisuutta verrattuna arvioituun riskiin. Riskianalyysi toimii tietoturvan mitoittamisen apuvälineenä, tähän voidaan käyttää VAHTI 22/2017 Riskienhallinnan ohjetta ja työkalua.

Vieremän kunta rekisterinpitäjänä ja ulkopuolinen henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja valitsemaan arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta liitetään osaksi kunnan riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Tietosuojavastaava tukee eri yksiköitä, jotta tietosuojariskejä tunnistettaisiin paremmin, ja on mukana määrittelemässä tunnistetuille, hallintaan otettaville riskeille tarvittavia hallintakeinoja.

4.4 Tietosuojaprosessit

Tietosuojaprosesseja ovat pakollinen tietosuojan vaikutusten arviointi silloin, kun henkilötietoihin sisältyy korkea riski, sekä rekisteröityjen oikeuksien toteuttaminen.

1. Tietosuojan vaikutustenarviointiprosessi on osa kokonaisriskienhallintaa**.** Sen käynnistävät tekijät määritellään ja sitä sovelletaan yhdenmukaisesti läpi organisaation.

Tietosuojan vaikutustenarviointiin liittyvät mallipohjat vakinaistetaan ja niiden tueksi laaditaan ohjeet varmistamaan yhdenmukainen ja täsmällinen mallipohjan täydentäminen. Tietosuojavastaava osallistuu vaikutustenarviointien tekemiseen arvioiden analyysin tuloksia ja konsultoi riskienhallintakeinojen suunnittelussa. Laaditaan tarvittavat prosessit seuraamaan ja varmistamaan, että tietosuojan vaikutustenarviointia koskevaa prosessia noudatetaan. Valvontaviranomainen on julkaissut tarkemman ohjeen, milloin ja miten vaikutustenarviointi tehdään. Ohjeessa käsitellään keinoja selvittää, liittykö henkilötietojen käsittelyyn korkea riski. Ohje löytyy kohdasta 8 Linkit.

2. Rekisteröityjen oikeudet ja tietopyynnöt
Vieremän kunta määrittelee Asiakastietojen tarkastus, korjaus ja poistaminen -prosessin rekisteröityjen oikeuksiin liittyvien pyyntöjen käsittelemiseksi (ml. oikeuksien laajuuksien ja sovellettavuuden määrittely, yhteyspisteen määrittäminen organisaatiossa, pyyntöä esittävän rekisteröidyn identiteetin varmistaminen, pyynnön reitittäminen, tietojen koostaminen, pyynnön sisällön toteuttaminen). Rekisteröityjen esittämät pyynnöt käsitellään ilman aiheetonta viivytystä ja rekisteröidylle ilmoitetaan kuukauden kuluessa ne toimenpiteet, joihin organisaatio aikoo pyynnön johdosta ryhtyä. Esitetyt ja toteutetut pyynnöt osoitetaan kirjaamoon, jossa ne kirjataan asianhallintajärjestelmään.

4.5 Henkilötietojen käsittelyn periaatteet

Vieremän kunnalle on laadittu tietoturva- ja tietosuojapolitiikka, joka määrittää ylätason linjaukset, periaatteet ja vastuut tietosuojan hallinnoinnissa ja henkilötietojen käsittelyssä. Tietoturva- ja tietosuojapolitiikka on johdon hyväksymä, julkaistu ja viestitty läpi organisaation.

Tietohallinnon ohjausryhmä hyväksyy politiikan linjausten, periaatteiden ja vastuiden mukaisesti laadittavat henkilötietojen käsittelyn ohjeistukset, jotka hyväksynnän jälkeen jalkautetaan huolellisesti. Vieremän kunnan henkilötietojen käsittelijöihin kohdistuvat velvoitteet kuvataan ohjeessa henkilötietojen käsittelijöille.

Henkilöstön tietoturvatietoisuus ja osaaminen varmistetaan koulutuksilla ja ohjeiden jalkauttamisella. Vaitiolo- ja salassapitosopimukset allekirjoitetaan henkilöstön sekä alihankkijoiden kanssa. Tarvittaessa ja lain mahdollistaessa tehdään henkilöiden turvallisuusselvitykset.

Kunnan eri rekistereistä vastaavat henkilöt huolehtivat ulkoisesta tiedoksiannosta rekisteröidyille, mm. julkaisemalla tietosuojaselosteen kunnan verkkosivulle sekä linkittämällä sen rekisterin yhteyteen. Aiemmista tietosuojaselosteen versioista pidetään lokia.

4.6 Tietosuoja hankinnoissa sekä järjestelmä- ja sovelluskehityksessä

Vieremän kunnan hankkiessa järjestelmiä, sovelluksia ja palveluja, jotka tulevat käsittelemään henkilötietoja, tietosuoja tulee huomioida jo hankintaprosessissa. Näin valitaan sellaisia toimittajia,

joiden toimittamien tuotteiden tietosuojataso vastaa tietosuoja-asetuksen vaatimuksia. On myös huomioitava henkilötietoja käsittelevien järjestelmien ylläpitohenkilöstön sijainti, jotta tietoja ei luovuteta kolmansiin maihin. Tietosuojavaatimukset tulee asettaa jo tarjouspyyntöön ja liittää ne osaksi tarjouspyynnön perusteella tehtäviä sopimuksia. Sopimuksissa on suositeltavaa vaatia salassapitoa ja tarvittaessa tulee lisäksi laatia erillinen vaitiolositoumus.

Kun uusia järjestelmiä, sovelluksia tai palveluja otetaan käyttöön, tulee ennen käyttöönottoa arvioida tarvittavat toimenpiteet tietosuojan säilymisen kannalta. Tällaisia toimenpiteitä voivat olla esimerkiksi rekisteriselosteen laadinta tai päivittäminen, ja aloitettavan käsittelyn liittäminen osaksi rekisteröidylle tarjottavia kanavia heidän oikeuksiensa toteuttamiseen.

Vieremän kunta ei voi rekisterinpitäjänä ulkoistaa tätä velvollisuutta. Käsittelyn periaatteet ja sisäänrakennettu tietosuoja on suunniteltava tapauskohtaisesti ja ennakoiden, eli tietosuoja tulee huomioida jo osana hankinnan vaatimusmäärittelyä.

Mikäli Vieremän kunta rekisterinpitäjänä ulkoistaa sovelluskehityksen kolmannelle osapuolelle, tulee ulkoistussopimuksessa vaatia sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen kehitysprosessissa. Vaatimukset tulisi pystyä yksilöimään mahdollisimman tarkasti eikä viittaamaan yleisesti ”riittävän tietosuojan toteuttamiseen”. Kunnan tulee hallita sovelluskehityksen ulkoistussopimuksissa olevia vaatimuksia.

Tietojärjestelmien testauksessa tulee huolehtia henkilötietojen käytön rajoittamisesta. Tietoturvatestaus suoritetaan järjestelmien hyväksyntätestauksen yhteydessä.

Vaatimukset henkilötiedon elinkaaren ajan
Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta koko käsiteltävien henkilötietojen elinkaaren ajan. Elinkaarella tarkoitetaan ajanjaksoa henkilötietojen keräämisestä niiden anonymisointiin tai poistoon, ks.kuva.

Kuva: Henkilötietojen elinkaari

Seuraavat tarvittavat **tekniset ja organisatoriset toimenpiteet ja menettelyt** tulee toteuttaa, jotta mm.
1) voidaan hallita suostumuksia sekä kieltoja ja myöhemmin tarvittaessa osoittaa rekisteröidyn antama suostumus käsittelytoimiin, lisäksi alle 16-vuotiaat käyttäjät tulee tunnistaa riittävän luotettavasti.
2) oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta (käsittelyllä on oikeudellinen peruste)
3) pääsy henkilötietoihin on rajattu käyttäjätasolla. Pääsy perustuu aina työtehtäviin liittyvään tarpeeseen ja pääsyoikeuksissa noudatetaan vähimpien oikeuksien periaatetta (principle of least privilege).

4) taataan rekisteröityjen oikeuksien toteutuminen varmistamalla, että käsiteltävät henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä sekä käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.
5) tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
6) taataan henkilötietojen suoja tarvittavin tietoturvakeinoin.

Rekisterinpitäjän on ennen käsittelyn aloittamista määriteltävä henkilötietojen tarpeellinen säilytysaika, eli kuinka kauan henkilötietoja tarvitaan niiden käsittelytarkoitukseen. Vähintäänkin on määriteltävä ne kriteerit, joiden pohjalta säilytysaika määräytyy. Säilytysaikamääritykset tulee tehdä lisäksi henkilötietoja käsitteleviin sovelluksiin ja järjestelmiin hallintakeinojen toteutusvaiheessa.

Säilytysaika on huomioitava myös varmistuksissa, ettei vanhentunutta ja käsittelystä poistunutta tietoa pääse palautumaan esimerkiksi epäsuotuisista tilanteista järjestelmän toipumisen yhteydessä. Mikäli henkilötietoja ei enää tarvita niiden käsittelytarkoituksen toteuttamiseen, mutta niitä ei voida poistaa muun sääntelyn takia, tulee tiedot arkistoida ja niiden käsittelyä rajoittaa. Tällaisia tietoja voivat olla esimerkiksi kirjanpitoa varten säilytettävät tiedot. Kun määritelty säilytysaika tuotantojärjestelmissä ja arkistossa on umpeutunut, tiedot tulee joko poistaa tietoturvallisesti tai anonymisoida siten, että rekisteröidyt eivät enää ole tunnistettavissa. Säilytysaika tulee ilmoittaa myös rekisteröidyille suunnattavassa viestinnässä esim. tietosuojaselosteessa.

4.7 Viranomaisyhteistyö

Rekisterinpitäjällä on velvollisuus tehdä yhteistyötä valvontaviranomaisen kanssa valvontaviranomaisen niin pyytäessä. Vieremän kunnassa yhteistyö valvontaviranomaisen kanssa kuuluu tietosuojavastaavan vastuulle. Mikäli Vieremän kunnalla rekisterinpitäjänä on toimintaa useassa EU:n jäsenvaltiossa, voi se asioida päätoimipaikkansa valvontaviranomaisen kanssa.

Valvontaviranomaisen pyynnön ohella kunnan on tehtävä yhteistyötä valvontaviranomaisen kanssa ennakkokuulemisen muodossa, jos suunniteltuun henkilötietojen käsittelyyn liittyy tietosuojan vaikutustenarvioinnin perusteella suuria riskejä, eikä rekisterinpitäjällä ole keinoja riskitason pienentämiseksi.

Vieremän kunnalla on myös ilmoitusvelvollisuus valvontaviranomaiselle henkilötietojen tietoturvaloukkaustilanteissa luvussa 5 kuvatulla tavalla. Valvontaviranomainen voi vaatia yhteistyötä tilanteen selvityksen yhteydessä arvioidakseen, miten kunta noudattaa tietosuoja-asetuksen velvollisuuksia. Henkilötietojen tietomurtotapauksissa kunnan on hyvä tehdä yhteistyötä myös Viestintäviraston kanssa tekemällä ilmoitus tietoturvaloukkauksesta Kyberturvallisuuskeskukselle. Tällöin voi olla aiheellista tehdä myös tutkintapyyntö poliisille.

4.8 Tietoturvallisuustoiminta

Turva-arkkitehtuuri
Vieremän kunnalla on turvallinen verkko- ja järjestelmäarkkitehtuuri, joka sisältää asianmukaiset palomuurit, verkkojen eriyttämisen, palvelinten kovennukset sekä henkilötietojen ja tietojen siirtoväylien salaamisen. Vieremän kunnan käytössä on mm. salattu sähköposti arkaluonteisten ja salassa pidettävien tietojen siirtoon.

Käyttäjä- ja pääsynhallinta
Käyttäjät ja admin-käyttäjät on dokumentoitu. Kaikilla järjestelmien ja rekisterien käyttäjillä on henkilökohtaiset käyttäjätunnukset. Järjestelmän käyttäjän luomis-, muutos- ja poistoprosessi voidaan dokumentoida ja toteuttaa määräysten mukaisesti. Järjestelmien ja rekisterien käyttäjät katselmoidaan

säännöllisesti vastuuhenkilön toimesta. Autentikointi on tietoturvallinen ja salasanavaatimukset ovat riittävällä tasolla. Pääsynhallinnassa tulee ottaa huomioon myös etäyhteydet EU:n tai Euroopan talousalueen ulkopuolelta, sillä etäyhteyden ottaminen rinnastetaan henkilötietojen siirtoon, mikäli toimenpiteessä käsitellään henkilötietoja.

Käsittelyn valvonta ja seuranta, lokitus
Rekisterinpitäjän tulee voida jälkikäteen todentaa lokitiedostoista, kuka on suorittanut henkilötietojen haun järjestelmästä, mitä henkilötietoja on katsottu, muutettu, lisätty tai poistettu sekä milloin toimenpide on suoritettu (aikaleima). Myös admin-käyttöä tulee seurata. On tärkeää, että menettelyt, joilla lokitiedostoja seurataan ja miten epäillyt väärinkäytökset käsitellään, on suunniteltu etukäteen.

Mahdolliset seuraamukset henkilötietojen väärinkäytöksistä on kartoitettu ja ne sisällytetään henkilötietojen käsittelijöille sekä luottamushenkilöille suunnattuihin ohjeisiin. Seurantaa on mahdollisuuksien mukaan hyvä suorittaa automatisoidusti, sillä lokia muodostuu tyypillisesti hyvin paljon. Poikkeamien hallintaa käsitellään tarkemmin kappaleessa 5.

Omaisuuden ja tiedon hallinta
Vieremän kunta ohjeistaa henkilöstöä tietovälineiden käsittelystä sekä tiedon luokittelusta ja luokitellun tiedon käsittelystä. Henkilöstölle tulee olla selvää, miten henkilötietoja on sallittua käsitellä esimerkiksi pilvipalveluun tallentamisessa, sähköpostilla siirtämisessä ja siirrettäville tietovälineille tallentamisessa.

Päivitysten ja muutosten hallinta
Ohjelmistokomponenttien haavoittuvuuksien saatavilla olevia päivityksiä seurataan ja hallitaan (CERT-ryhmät). Järjestelmien tietoturvallisuudesta huolehditaan päivitysten ja muutosten yhteydessä. Muutosten hallinnasta ja jäljitettävyydestä huolehditaan myös.

Fyysinen turvallisuus, toimitilat
Tilaturvallisuudesta huolehditaan tarvittavin pääsykontrollein ja -rajauksin. Tietovälineet, joilla henkilötietoja käsitellään, huolletaan ja hävitetään tietoturvallisesti, jotta henkilötietoja ei päädy luvattomasti kolmansille osapuolille. Henkilöstön tulee käyttää kulunvalvontaa varten annettuja tunnistusvälineitä.

Toimittajien ja sopimusten hallinta
Tietoturva- ja tietosuojavaatimukset määritellään sopimuksen/hankinnan kohteelle ja alihankkijoille. Tietoturvan ja tietosuojan hallinnan menettelytavat on sovittava, mukaan lukien henkilötietojen käsittelyn seuranta ja valvonta sekä tietoturvaraportointi ja tietoturvapoikkeamien hallinta.

Toiminnan jatkuvuuden hallinta
Henkilötietojen varmuuskopioinnista huolehditaan ja niitä käsittelevien järjestelmien kapasiteettia hallitaan. Laaditaan tarvittavat suunnitelmat epäsuotuisiin tilanteisiin ja niistä toipumiseen, jotta voidaan taata henkilötietojen saatavuus esimerkiksi teknisen vian sattuessa.

5 Poikkeamien hallinta ja ilmoitusvelvollisuus

Vieremän kunnassa tietoturvapoikkeamien käsittelystä ja kehittämisestä vastaa tietohallinnon ohjausryhmä.

5.1 Tietoturvapoikkeamien hallintaprosessi

- ***Vaihe 1. Tietoturvapoikkeamien käsittelykyvyn muodostaminen*** käsittää erilaiset varautumistoimet, joiden avulla poikkeamatilanteessa voidaan toimia. Varautumistoimissa huomioidaan mm. järjestelmien ja prosessien riittävä dokumentaatio, päätöksenteko, riippuvuuksien tunnistaminen, omat ja yhteistyötahojen henkilöstöresurssit, tilannekuvan muodostaminen ja tiedon jakaminen, haittaohjelmien ja poikkeavan toiminnan havainnointikyvyn kehittäminen, sopimusmenettelyt ja harjoittelu.

- ***Vaihe 2. Tietoturvapoikkeaman havaitseminen ja analysointi*** käsittää normaalista poikkeavan toiminnan havaitsemisen ja analysoinnin, minkä tavoitteena on selvittää, mitä on tapahtunut ja miksi. Poikkeamatiedon lähteitä voi olla esim. järjestelmälokit, hyökkäyksen havainnointi- ja estojärjestelmät, tietoverkon aktiivilaitteet, haittaohjelmien ja roskapostin suodatusjärjestelmät, päätelaitteet, ulkoistetun palveluntoimittajan tai tietoliikenneoperaattorin järjestelmät, kulunvalvonta- ja kameravalvontajärjestelmät, käyttäjien ja asiakkaiden yhteydenotot sekä palvelutoimittajien ja sidosryhmien yhteydenotot. On hyvä, että koko henkilöstö koulutetaan siten, että kaikilla on valmiudet havaita mahdollinen tietoturvapoikkeama tai sen uhka. Analysoinnin tuloksena voidaan todeta, onko kyseessä tietoturvapoikkeama tai esim. ICT-häiriötilanne. Valvontaa voidaan suorittaa myös esim. tietoturva-tapahtumien havainnointiohjelmistolla, jolla voidaan keskitetysti kerätä ja analysoida mm. palomuurien, hakemistopalvelun ja tietoturvaohjelmistojen tapahtumia sekä työasema- ja palvelinlokeja.

- ***Vaihe 3. Tietoturvapoikkeaman reagointiin*** liittyvät toimenpiteet vastuutetaan ja aikataulutetaan, jotta voidaan minimoida mahdolliset vahingot. Poikkeamasta informoidaan muita viranomaisia ja sidosryhmiä sekä käynnistetään toimenpiteet poikkeaman korjaamiseksi. Tietosuojavastaava tekee ilmoituksen sekä valvontaviranomaiselle että niille rekisteröidyille, joiden yksityisyyden suoja on vaarantunut, mikäli katsotaan, että on aiheellista tehdä tietosuoja-asetuksen mukainen ilmoitus. Tarvittaessa tulee tehdä tutkintapyyntö myös poliisille.

- ***Vaihe 4. Toipumisvaiheessa*** organisaation ja palveluiden toiminta palautetaan normaalitilaan. Poikkeamasta laaditaan raportti, jonka havaintojen perusteella kehitetään käsittelykykyä ja varautumista, jotta poikkeaman toistuminen voitaisiin jatkossa estää.

Kunnan tulee varmistaa ulkopuolisen avun saaminen tarvittaessa, erityisesti laajavaikutteisissa poikkeamissa. Henkilötietoihin liittyvistä poikkeamatilanteista tulee myös dokumentoida tutkintaan ja toipumiseen tehdyt toimenpiteet sekä huolehtia tarvittavien todistusaineistojen säilyttämisestä. Valvontaviranomainen voi pyytää dokumentaatiota auditoitavaksi.

5.2 Ilmoituksen tekeminen

Vieremän kunnan tulee tehdä ilmoitus valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta 72 tunnin kuluessa siitä, kun loukkaus on havaittu.

Valvontaviranomaiselle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavassa kappaleessa listatut kohdat. Ilmoitukselle laaditaan mallipohja. Ilmoitusvelvollisuus huomioidaan myös kriisi- ja

häiriötilanneviestinnässä niin prosessin kuin ohjeistuksen osalta.

- Kuvaus mitä on tapahtunut.
- Mikäli mahdollista, niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskettaa.
- Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta valvontaviranomainen voi kysyä lisätietoja.
- Millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidyille.
- Kuvaus niistä toimenpiteistä, joita kunta aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi.
- Jos tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä. Jos ilmoitusta ei tehdä 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys viivästyksen syistä.

Edellä mainittujen tehtävien suorittamiseksi tehdään prosessimäärittely Tietosuojapoikkeamista ilmoittaminen, johon kuuluvat selkeät roolit ja vastuut. Tyypillisesti prosessi integroidaan osaksi tapahtumien hallintaa. Mikäli Vieremän kunta ei hallinnoi itse työasema- ja järjestelmäympäristöä, tulee poikkeamien hallinta ja ilmoitusvelvollisuus sisällyttää toimittajasopimuksiin. Myös tällöin tarvitaan prosessimäärittely, jossa kuvataan millaisista tilanteista ilmoitetaan rekisterinpitäjälle, mitä kanavia käyttäen ja miten tilanteen selvittämiseen ja ilmoitusvelvollisuuden täyttämiseen liittyvät vastuut jakautuvat.

Henkilöstöä, luottamushenkilöitä ja sidosryhmiä varten Vieremän kunnan poikkeamailmoittamiseen tehdään keskitetty ilmoituslomake osoitteeseen: www.vierema.fi/tietoturva. Kaikista ilmoituksista tulee tulla tieto kunnan tietosuoja- ja tietoturvavastaavalle.

6 Hallinnolliset sakot ja seuraamukset

Tietosuoja-asetus tuo valvontaviranomaisille uutena oikeuden määrätä rekisterinpitäjälle ja / tai henkilötietojen käsittelijälle sakkoja tai hallinnollisia seuraamuksia tietosuoja-asetuksen velvoitteiden laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella kolmeen luokkaan. Sakon enimmäismäärä on 20 miljoonaa euroa tai 4 % organisaation edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Niiden tietosuoja-asetuksen vaatimusten laiminlyöntien osalta, joihin ei sovelleta hallinnollisia sakkoja, voi valvontaviranomainen määrä muita varoittavia seuraamuksia. Näitä voivat olla esimerkiksi käsittelyn kieltäminen, kunnes tarvittavat velvollisuudet on täytetty. Valvontaviranomaisella on oikeus auditoida rekisterinpitäjän tietosuojan toteutusta. Suomessa julkishallinnon osalta käytettävä menettely tarkentuu osana lainsäädäntötyön etenemistä.

7 Seuranta ja valvonta

7.1 Tietotilinpäätös

Seurannan keskiössä on vuosittain tietosuojavastaavan kokoama tietotilinpäätös.
Se on raportti, joka syntyy Vieremän kunnan sisäisen tarkastelun ja arvioinnin tuloksena. Se on myös työkalu EU:n tietosuoja-asetuksen rekisterinpitäjän velvollisuuksien osoitusvelvollisuuden todentamiseen sekä osa kunnan sisäänrakennettua tietosuojaa eli riskien jatkuvaa seurantaa.

Tietotilinpäätös voidaan jakaa julkiseen osaan ja ei-julkiseen. Julkaisemalla tietotilinpäätöksen kunta osoittaa, että se noudattaa lainsäädäntöä ja käsittelee tietoja asianmukaisesti ja luottamuksellisesti.

Samalla minimoidaan valvontaviranomaisten ja asiakkaiden tiedustelut ja kyselytarve, kun kunta raportoi ja tiedottaa oma-aloitteisesti ja ennakoiden.

Tietotilinpäätös on lisäksi johdon työväline sisäiseen ja ulkoiseen valvontaan. Se nostaa esille tietojen käsittelyyn liittyviä kehittämiskohteita ja antaa kokonaiskuvan kunnan tietojen käsittelyn ja tiedonhallinnan nykytilasta. Se toimii ennen kaikkea luottamuksen rakentajana Vieremän kunnan menettelytapoihin.

Tietotilinpäätökseen voidaan sisällyttää mm. seuraavia mittareita

- keskeiset tietovarantojen tunnusluvut
- tietoturva- ja tietosuojapoikkeamat
- tietojärjestelmien käyttökatkot ja niiden vaikutukset
- käytönvalvontasuunnitelman toteutuminen
- tietoturvan ja tietosuojan omavalvontasuunnitelman toteutuminen
- tietosuoja- ja tietoturvarikkomukset
- rekisteröityjen informoinnin ajantasaisuus ja tulleet pyynnöt
- mahdolliset viranomaisten selvityspyynnöt
- lakimuutokset ja niiden jalkautukset
- tietosuoja- tietoturvakoulutukset
- uudet ohjeistukset

8 Linkit

Tietoturva- ja tietosuojatyötä ohjaavat keskeiset VAHTI-ohjeet:
25/2017 Sähköisen asioinnin tietoturvaohje
22/2017 Ohje riskienhallintaan

- Riskienhallintatyökalu - Excel - perusversio
- Riskienhallintatyökalu - Excel - laajempi versio
- Ohje riskienhallintatyökaluun

8/2017 Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2016 Toiminnan jatkuvuuden hallinta -ohje
VAHTI 2/2015 Ohje salauskäytännöistä

Tietosuojan valvontaviranomaisen julkaisut:
Ohje tietosuojaa koskevasta vaikutusten arvioinnista

9 Voimaantulo

Tietoturva- ja tietosuojapolitiikka tulee hyväksymisen jälkeen voimaan välittömästi ja korvaa kunnanhallituksen 4.11.2013 § 260 hyväksymän Ylä-Savon ICT -palvelut Oy:n (YSIT) omistajakuntien yhteisen tietoturvaohjeiston ja – koulutusympäristön.