### SAATE

*Tämä tietotilinpäätösmalli pohja pohjautuu alun perin Kati Suojasen ja Minna Järvisen Kuntaliitolle tekemään raporttiin osana Tampereen yliopiston hallintotieteiden kurssia. Konsultoiva asiantuntijatyö organisaatiossa keväällä 2018. Pohjaa on edelleen muokattu yhteistyössä Kuntaliiton (Tuula Seppo), Turun kaupungin (Jaana Halin, Sari Järvinen, Arvi Leino, Janne Mutanen, Antti Saarinen, Jouni Satopää) ja Suonenjoen kaupungin (Lauri Anakkala, Hanna Heikkilä) yhteistyönä.*

*Tietotilinpäätösmalli on rakennelma tai kehikko, joka on syntynyt tietosuojavaltuutetun ohjeeseen pohjautuen sekä tietotilinpäätösdokumentteja ja haastatteluja hyödyntäen (Suojanen, Järvinen 2018). Kuitenkin niin, että kyseessä on prosessinkuvauksen tuloksena syntynyt dokumentti, jonka sisältö muotoutuu vasta organisaation käytännössä. Sellaisenaan se ei esitä yhtä totuutta, vaan kuten jo tietosuojavaltuutetun ohjeistuksessa mainitaan, niin tietotilinpäätös on aina toimiala sekä organisaatio kohtainen. Tietotilinpäätökselle organisaatiossa annettu merkitys vaikuttaa dokumentin rakenteeseen sekä sisältöön - epäilemättä myös prosessiin ja toimijoihin.*

***Tietotilinpäätöksen tarkoitus****: Osoitusvelvollisuuden toteennäyttäminen, luottamuksen osoittamista sidosryhmiin nähden, johdon työväline ja sisäisen valvonnan työkalu.*

***Prosessi:*** *Yleensä tietosuojavastaava kerää tiedot osastoittain, mutta muitakin ratkaisuja voi olla. Kyseessä on yhden tietyn hetken tilanne. Tieto tuotetaan yleensä prosessin kautta, joka kehittyy kokemuksen myötä.*

***Painotukset****: Organisaatio ja toimialakohtaiset merkitykset.*

***Ohje:*** *Malli koostuu 7 luvusta. Jokainen luku sisältää yleisen tekstin ko. luvun sisällöstä. Yleisen tekstin jälkeen on laadittu kysymyksiä. Kysymyksiin vastaamalla saadaan tehdyksi oma tietotilinpäätös. Ei ole tarkoitus, että kaikkiin kysymyksiin vastataan, vaan kysymykset on laitettu avuksi siihen, minkälaisia asioita ko. luku käsittele. Mallia saa muokata ja käyttää omien tarpeiden mukaan. Malli on vain viitteellinen. Lopussa on kuvitteellisen Tyrskylän kunnan tietotilinpäätös.*

[Mallipohja – Tietotilinpäätös on organisaatiokohtainen dokumentti, joka muotoutuu kunkin organisaation omien tarpeiden ja merkitysten mukaan. Tässä rakenne ja sisältö ovat vain viitteellisiä.]

[Organisaatio] TIETOTILINPÄÄTÖS vuosi [xxxx]

***Pituus****:*

***Aikataulutus****: kerran vuodessa vuosikellon mukaan, muulloin pyydettäessä.*

***Tarkoitus****: Osoitusvelvollisuuden toteennäyttäminen, luottamuksen osoittamista sidosryhmiin nähden, johdon työväline tai sisäisen valvonnan työkalu.*

***Rajaukset****:*

**Päiväys ja laatija:**

**Allekirjoitukset tai muu hyväksyntä:**

SISÄLLYSLUETTELO

[SAATE 1](#_Toc15542062)

[JULKINEN TIIVISTELMÄ 4](#_Toc15542063)

[TIIVISTELMÄ JOHDOLLE 5](#_Toc15542064)

[1. JOHDANTO 6](#_Toc15542065)

[2. TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN 7](#_Toc15542066)

[3. TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT 8](#_Toc15542067)

[4. LAINSÄÄDÄNTÖ JA MUU OHJEISTUS 10](#_Toc15542068)

[5. REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN 11](#_Toc15542069)

[6. ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN 12](#_Toc15542070)

[7. SEURANTA JA MITTARIT 13](#_Toc15542071)

### JULKINEN TIIVISTELMÄ

*Tee tiivistelmä lopuksi keskeisistä tietosuojaan, tietoturvaan, riskienhallintaan ja yleiseen tiedonhallintaan liittyvistä havainnoista ja vuoden aikana tapahtuneista tärkeimmistä tapahtumista esimerkiksi tietojärjestelmähankinnoista ja kehittämisprojekteista. Kerro myös tarvittaessa, miten tekoälyä hyödynnetään esimerkiksi asiakassegmenttien teossa, liikenneväylien suunnittelussa ja infrastruktuurissa sekä esimerkiksi suunniteltaessa henkilöstön koulutustarpeita. Hyödynnetäänkö tietoa, onko olemassa avointa dataa, mitä julkaistaan ja mistä löytyy, onko tehty tiedolla johtamisen määrityksiä. Tiivistä myös kehittämistarpeet tulevalla vuodelle.*

### TIIVISTELMÄ JOHDOLLE

*Tee myös oma, erillinen tiivistelmä johdolle keskeisistä havainnoista ja mittareista ja ehdotuksia toimenpiteistä. Johdon tulee saada tästä tiivistelmästä kokonaiskuva henkilötietojen käsittelyn nykytilasta ja kehittämistarpeista. Mikäli organisaatiossa on tiedolla johtamista, kuvaa miten kunta hyödyntää tietopääomaansa ja miten tiedolla johtaminen toteutuu. Huomioi, että johdon tiivistelmä saattaa sisältää salassapidettävää tietoa.*

### JOHDANTO

Tietotilinpäätös tarjoaa ajantasaisen **tilannekuvan** organisaation henkilötietojen käsittelyn nykytilasta sekä arvion tietosuojan toteutumisesta. Tietotilinpäätöksessä kartoitetaan henkilötietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä. Tavoitteena on tukea tietosuojatyön tekemistä ja lisätä tekemisen vaikuttavuutta. Tietotilinpäätös toimii myös yhtenä **osoitusvelvollisuuden** osoittamisen välineenä **ja sisäisen ja ulkoisen valvonnan raporttina**. Osoitusvelvollisuuteen kuuluu mm. se, että organisaation **sopimuksissa ja alihankinnoissa** on huomioitu tietosuojan ja -turvan vaatimukset. Lisäksi rekisterinpitäjä tulee huomioida rekisteröidyn henkilötietojen käsittelyyn kohdistuvat **riskit.** Rekisterinpitäjän tulee huolehtia siitä, että henkilöstöllä ja ulkopuolisilla henkilötietojen käsittelijöillä on tarvittava **ohjeistus ja osaaminen**.

Rekisterinpitäjän tulee myös **seurata, raportoida ja valvoa** tietosuojaan ja -turvaan liittyviä asioita ja huolehtia siitä, että tietosuojaan koskeva sääntely toteutuu organisaatiolla. Osoitusvelvollisuuteen kuuluu myös **sisäänrakennetun tietosuojan** vaatimus, millä tarkoitetaan sitä, että tietosuojaperiaatteet toteutuvat kaikissa käsittelyn vaiheissa. Tietosuojaperiaatteet (5 art.) ovat 1. lainmukaisuuden, kohtuullisen ja läpinäkyvyyden periaate, 2. käyttötarkoitussidonnaisuuden periaate, 3. tietojen minimoinnin periaate 4. täsmällisyyden periaate, 5. säilytyksen rajoittamisen periaate ja 6. eheyden ja luottamuksellisuuden periaate.

Tietotilinpäätöksellä voidaan lisätä luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita ja käsitellään henkilötietoja sen mukaisesti. Hyvin hoidetulla tietosuojatyöllä vaikutetaan organisaation tehokkuuteen ja kilpailukykyyn. Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista.

Avainsanat: kokonaiskuva, osoitusvelvollisuus, sisäinen ja ulkoinen raportointi, sopimus, alihankinta, riskit, ohjeistus, osaaminen, valvonta, sisäänrakennettu tietosuoja

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin tarvittavilta osin]*

 *[Kerro keskeisistä tietosuojaan, tietoturvaan, riskienhallintaan ja yleiseen tiedonhallintaan liittyvistä vuoden aikana tapahtuneista tärkeimmistä tapahtumista, esimerkiksi tietojärjestelmähankinnoista ja kehittämisprojekteista. Kerro lisäksi, miten tietotilinpäätöksen tiedot on koottu? Onko osa strategiatyötä ja kehittämistyötä, sisältääkö tiedolla johtamista ja tiedon hyödyntämistä laajemmin, vai keskittyykö pelkästään tietosuoja ja -turvakysymyksiin? Sisältääkö tietotilinpäätös rajoituksia, onko erikseen julkinen ja salassapidettävä osio? Suositus on, että olisi pääosin julkinen, mutta esimerkiksi tietoturvallisuuteen liittyvät asiat voivat olla salassapidettäviä. Kerro myös, miten ja milloin tietotilinpäätös julkaistaan ja kuka työstä vastaa.]*

### TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

###

Tietosuoja-asetuksen (artikla 24) mukaan rekisterinpitäjä on vastuussa siitä, että se toteuttaatarvittavat **tekniset ja organisatoriset toimenpiteet**, joilla osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän on huomioitava henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudelta vaihtelevat riskit ja suhteuttava toimenpiteet näiden mukaisesti. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tila- ja käytönvalvontaa, pääsynhallinta, päivitysten ja muutosten hallintaa, fyysistä turvallisuutta, henkilöstöturvallisuutta, toimittajien ja sopimusten hallintaa, tietoturvallisuuden hallintaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, käytännesääntöjen sekä sertifikaattien käyttöä. Tässä kappaleessa annetaan kuva siitä, miten tiedon eheys, saatavuus ja luottamuksellisuus taataan sekä myös tiedon läpinäkyvyys (5 art.).

Avainsanat: tekniset ja organisatoriset toimenpiteet

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin tarvittavilta osin]*

 *[Kuvaus toimintaympäristöstä, miten tietoturva ja -tietosuoja on organisoitu ja millainen on tietosuojan ja -turvan hallintamalli ja/tai kehittämismalli, esim. kuka vastaa mistäkin asiasta, miten tietohallinto on järjestetty, hoidetaanko omana työnä, onko ulkoistettu. Onko seloste käsittelytoimista (30 art.) tehty ja tarvittaessa saatavilla. Huomioi myös tietosuojavastaavan rooli ja käytetäänkö esim. vuosikelloa. Kerro miten henkilökunnan koulutukset ja perehdytykset hoidetaan sekä laaditut toimintapolitiikat ja muut ohjeistukset sekä omalle että ulkopuolisille henkilötietojen käsittelijöille ja kuka näiden ajantasaisuudesta vastaa. Kuvaa myös, miten on toteutettu muut tekniset ja organisatoriset toimenpiteet (riskianalyysit, vaikutustenarvioinnit, ennakkokuulemiset, omavalvontasuunnitelma, jatkuvuuden hallinta, päivitysten ja muutosten hallinta, henkilötietojen tietoturvapoikkeamiin varautuminen, työntekijöiden turvallisuusselvitykset, salassapitosopimukset, tila- ja käytönvalvonta, etäyhteydet, kryptaus, pseudonymisointi. IT-sopimuskumppanit, miten sovellusten ja tietokoneiden ym. hankinta, käyttöönotto, kehittäminen ja ylläpito on toteutettu? Miten on hoidettu valvonta ja sisäinen tarkastus? Onko olemassa laatustandardeja, käytännesääntöjä, auditointeja tai sertifiointeja. Vastaa kysymykseen siitä, miten huolehditaan tietojen laadusta ja saatavuudesta. Ota huomioon myös erilaiset tutkimusluvat, niiden käsittely ja huomioi rekisteröidyn oikeudet tutkimuksissa.]*

### **TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT**

Organisaation tulee suunnitella ja kuvata tiedonhallinnan, tietovarantojen ja tietovirtojen kokonaistilanteensa. Tämä tapahtuu esimerkiksi **kokonaisarkkitehtuurin, tietojärjestelmäarkkitehtuurin, tietovarantokuvausten, tiedonohjaussuunnitelmien ja erilaisten prosessikuvausten** avulla. Tarkoituksena on selventää sitä, miten tietoa hallintaa sen koko **elinkaaren** ajan, tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Lisäksi kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineitä. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi sitä, että tietojen säilytysajat on määritelty asianmukaisesti ja että niiden hävittäminen on suunnitelmallista. Tietovarantoja ja tietojenkäsittelyä saatetaan hoitaa myös organisaation ulkopuolella, esim. palkanlaskenta. Organisaatiolla on olemassa ohjeistus ja sopimukset näihin ulkoisiin tietojenkäsittelytilanteisiin. Organisaatio voi myös käsitellä tietoja käyttäen omia palvelinsalejaan tai ulkoisista pilvipalveluista.

Organisaatio voi johtaa tiedolla ja hyödyntää omaa tietopääomaansa vain, jos johdolla on tarpeeksi tietoa muun muassa omasta toiminnasta, toimintaympäristöstään, prosessien toimivuudesta, henkilökunnan osaamisesta, tietovirroista ja tietovarannoista. Tässä luvussa kuvataan muun muassa sitä, miten organisaatio toteuttaa tietosuojaperiaatteina tietojen minimointia, käyttötarkoitussidonnaisuutta ja säilytyksen rajoittamista ja tiedon läpinäkyvyyttä.

Avainsanat: kuvaukset, kokonaisarkkitehtuuri, tietovarannot, tiedonohjaussuunnitelmat, prosessikuvaukset, tiedon elinkaari

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin tarvittavilta osin]*

 *[Onko tiedossa ja kuvattu se, miten tieto kulkee ja sitä käsitellään organisaatiossa? Kerro mitä* ***keskeisiä*** *tietovarantoja ja tietojärjestelmiä on olemassa? Onko henkilötiedoille/rekistereille merkitty käyttötarkoitukset. Miten on huolehdittu tiedon elinkaaren hallinnasta mukaan lukien säilytysajat, hävittäminen ja arkistointi. Kerro tilanne koskien kokonaisarkkitehtuurikuvauksia, tiedonohjaussuunnitelmia, arkistonmuodostussuunnitelmia, prosessikuvauksia, tietovirtakuvauksia, tietojärjestelmäkuvauksia ym. Onko ulkopuolisia henkilötietojen käsittelijöitä ja tietovarantoja, käytetäänkö pilvipalveluita. Onko tehty tarvittavat sopimukset ja ohjeistukset henkilötietojen käsittelijöiden kanssa. Miten organisaatiossa on huolehdittu tiedonsaannista ja tietojen luovuttamista, onko olemassa sähköisen asioinnin kanavia, rajapintoja, katseluyhteyksiä. Hyödynnetäänkö tietoa, onko olemassa avointa dataa, mitä julkaistaan ja mistä löytyy, onko tehty tiedolla johtamisen määrityksiä]*

### **LAINSÄÄDÄNTÖ JA MUU OHJEISTUS**

Julkishallinnon organisaatiot noudattavat **Suomen ja EU:n lainsäädäntöä**. Kuntia ohjaavat mm. kuntalaki, hallintolaki, julkisuuslaki, tietosuoja-asetus, tietosuojalaki, arkistolaki sekä lukuiset muut yleis- ja erityislait. Lisäksi sisäiset ja ulkoiset **rahoittajat** (projektit, hankkeet) on omat ohjeistukset henkilötietojen käsittelystä, säilyttämisestä ja arkistoinnista. Sen lisäksi organisaatioilla on omia **käytännesääntöjä ja ohjeistuksia** sekä **kansallisia tai kansainvälisiä sertifikaatteja**. Organisaatioissa on myös omavalvontaa sekä virallisempia auditointeja. Tässä luvussa tehtävänä on käydä läpi lainsäädännöllistä ja omien ohjeistuksiin ja politiikkoihin liittyviä taustoja tietojenkäsittelyn osalta. Toisaalta tiedon laatuun ja käytettävyyteen liittyvät tekijät tulisi myös huomioida tietotilinpäätöksessä. Sosiaali- ja terveyspalvelujen tuottajien on laadittava tietosuojan ja tietoturvan omavalvontasuunnitelma, jonka malli saattaa olla hyödynnettävissä tietototilinpäätöksessä. Tässä luvussa vastataan tietosuojaperiaatteiden kysymyksiin koskien tietojenkäsittelyn lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä.

Avainsanat: lainsäädäntö, kansallinen, EU, rahoittajat, käytännesäännöt, ohjeistukset, politiikat, sertifikaatit, omavalvontasuunnitelma

*[Käy läpi keskeinen lainsäädäntö, ohjeistukset, toimintapolitiikat, strategiat, sertifioinnit ja auditoinnit. Ota huomioon myös mahdolliset sisäisten ja ulkoisten rahoittajien ohjeistukset.]*

### **REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN**

Jokaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, jonka tarkoituksena on turvata **rekisteröidyn oikeuksien ja vapauksien** toteutuminen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Rekisterinpitäjän velvollisuus on huolehtia rekisteröidyn oikeuksien toteutumisesta. Näitä ovat muun muassa rekisteröidyn oikeus saada tietoa henkilötietojen käsittelystä, oikeus saada pääsy tietoihin ja oikeus oikaista virheellisiä tietoja. Lisäksi rekisteröidyillä on oikeus tietyillä rajauksilla saada tieto sosiaali- ja terveydenhuollon käyttö ja -luovutustiedoista. Rekisterinpitäjän tulee **informoida** rekisteröityjä henkilötietojen käytöstä avoimesti ja selkeästi. Rekisterinpitäjän tulee myös varautua mahdollisiin henkilötietojen tietoturvaloukkauksiin ja harjoitella niihin varautumista käytännössä. **Henkilötietojen tietoturvaloukkauksia** ovat mm., että tiedot lähetetty väärälle vastaanottajalle, suojaamaton tiedonsiirtoväline on hävinnyt esim. USB-tikku, haittaohjelmatartunta, kyberhyökkäys ja hakkerointi. Rekisterinpitäjän tulee tilastoida henkilötietojen tietoturvaloukkaukset ja ilmoittaa niistä tietosuojavaltuutetun toimistolle ja tietyn edellytyksin myös rekisteröidyille. Henkilötietojen käsittelijöillä on velvollisuus puolestaan ilmoittaa henkilötietojen tietoturvaloukkauksista rekisterinpitäjälle. Tässä luvussa kuvataan tietosuojaperiaatteina erityisesti läpinäkyvyyttä ja kohtuullisuutta.

**Avainsanat: rekisteröityjen oikeudet, informointi, henkilötietojen tietoturvaloukkaukset**

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin]*

[*Kuvaa, miten organisaatiossa on hoidettu rekisteröityjen informointi, onko esim. tietosuojaselosteita muita informoinnin menetelmiä käytössä ja miten rekisteröidyn oikeudet toteutuvat organisaatiossa käytännössä. Kerro myös mistä tietosuojaselosteet ja muu informointimateriaali löytyvät. Kuvaa myös tietopyyntö-virheenkorjaus ja lokitietojen pyyntöön liittyvät prosessit sekä henkilötietojen tietoturvaloukkausprosessit ja mistä näihin liittyvät mahdolliset lomakkeet löytyvät. Ota huomioon myös tutkimuslupien käsittely ja rekisteröityjen oikeudet erilaisissa tutkimuksissa. Kerro myös henkilötietojen tietoturvaloukkausten harjoittelusta ja mahdollisista muista harjoituksista.]*

### **ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN**

Organisaation tulee arvioida tietosuojan ja -turvan tilanne toimintapolitiikan, mittareiden, kokonaisarkkitehtuuri ja muiden kuvausten avulla sekä mahdollisten asiakas- ja henkilöstön palautteiden näkökulmasta ja verrata kehitystä aiempiin vuosiin. Henkilöstön osaamisen, tietovirtojen ja toimintaprosessien arviointi ja kehittäminen ovat keskiössä. Organisaation johto voi johtaa tiedolla vain, jos sillä on riittävä ymmärrys omasta toiminnasta ja toimintaympäristöstään. Tavoitteena on päästä kohti tiedon hyödyntämistä. Tarkoituksena on tuoda esille myös keskeiset kehittämistavoitteet. Samalla on myös arvioitava asetettujen kehittämistavoitteiden toteutumista.

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin]*

[*Kuvaa organisaation nykytilanne, tehtyjen kehittämistavoitteiden toteutumista ja tee suositukset tarvittaviksi kehittämistoimiksi. Mieti henkilökunnan osaamistarpeet, millaista koulutusta, ohjeistusta, prosessien kehittämistä tarvitaan. Tarkoituksena on parantaa tietosuoja- ja -turvaosaamista koko organisaation tasolla sekä jos organisaatiossa tiedolla johtaminen ja tiedon hyödyntäminen ovat osa tietotilinpäätöstä, niin kuvaa myös niitä asioita. Miten tietoa hyödynnetään ja tarvittaessa myös, miten tekoälyä hyödynnetään esimerkiksi asiakassegmenttien teossa, liikenneväylien suunnittelussa ja infrastruktuurissa sekä esimerkiksi suunniteltaessa henkilöstön koulutustarpeita. Hyödynnetäänkö tietoa, onko olemassa avointa dataa, mitä julkaistaan ja mistä löytyy, onko tehty tiedolla johtamisen määrityksiä. Kuvaa kokonaisarvio mm. asiakastyytyväisyydestä, henkilökunnan tyytyväisyydestä ja erilaisten tiedonhallintaa liittyvien prosessin toimivuudesta.]*

### SEURANTA JA MITTARIT

Organisaatiolla on velvoitteita kuvata erilaisilla mittareilla toimintaansa. Osa mittaristosta palvelevat organisaation omaa tarvetta ja osa mittareita ovat sellaisia, joita joudutaan raportoimaan muulla. Ilman mittareita on vaikea tietää, miten organisaatio on kehittynyt ja mitä osa-alueita tulee vielä kehittää. Apuna tulosten kuvaamisessa voi käyttää väestörekisterikeskuksen (VRK) vuosittain tekemän digiturvakyselyn tuloksia. Alla on kuvattu yleisimpiä tietosuojaan, tietoturvaan ja riskienhallintaan liittyviä mittareita. Organisaatio valitsee omien tarpeidensa mukaan käytettävät mittarit ja voi myös seurata muita asioita, mitkä koetaan tarpeelliseksi ja omaa toimintaa kuvaavaksi. Mittarit on ryhmitelty viiteen eri osioon. Näitä ovat tietohallinto, riskien arviointi ja tarkastukset, tietovarannot, osaaminen ja ohjeistus sekä rekisteröidyn oikeudet.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tunnusluku** | **Mittari** | **Sote** | **Muut** | **Toteuma 2017** | **Toteuma 2018** |
| **Tietohallinto** |  |  |  |  |  |
| Työasemat | lkm |  |  |  |  |
| Käyttäjien (AD-tunnuksia) | lkm |  |  |  |  |
| Käyttötukipyynnöt  | lkm |  |  |  |  |
| Matkapuhelimia  | lkm |  |  |  |  |
| Kannettavat tietokoneet  | lkm |  |  |  |  |
| IT-palvelut, tietohallinto | htv |  |  |  |  |
| IT-ulkoiset sopimuskumppanit | lkm |  |  |  |  |
| Tietosuoja-tietoturva hlöstö | htv |  |  |  |  |
| Tietojärjestelmien kehittämisbudjetti | euroa |  |  |  |  |
| Käynnissä olevat projektit, joissa IT-osuus | lkm |  |  |  |  |
| **Riskien arviointi ja tarkastukset** |  |  |  |  |  |
| Tehdyt riskianalyysit, (sis. esim. HaiPro) | lkm |  |  |  |  |
| Tehdyt vaikutustenarvioinnit | lkm |  |  |  |  |
| Tehdyt ennakkokuulemiset | lkm |  |  |  |  |
| Tehdyt turvallisuusselvitykset | lkm |  |  |  |  |
| Tehdyt tarkastukset | lkm |  |  |  |  |
| Tehdyt auditoinnit, sisäiset | lkm |  |  |  |  |
| Tehdyt auditoinnit, ulkoiset | lkm |  |  |  |  |
| Sertifikaatit | lkm |  |  |  |  |
| Omavalvontasuunnitelma | lkm |  |  |  |  |
| **Tietovarannot** |  |  |  |  |  |
| Kokonaisarkkitehtuurikuvaus valmiusaste | % |  |  |  |  |
| Prosessikuvaukset valmiusaste | % |  |  |  |  |
| Tiedonohjaussuunnitelmat valmiusaste | % |  |  |  |  |
| Tietovirtojen kuvaukset valmiusaste | % |  |  |  |  |
| Tietovarannot | lkm |  |  |  |  |
| Tietojärjestelmät | lkm |  |  |  |  |
| Pilvipalvelut | lkm |  |  |  |  |
| Rajapinnat | lkm |  |  |  |  |
| Katseluyhteydet | lkm |  |  |  |  |
| Sähköisen asioinnin kanavat | lkm |  |  |  |  |
| Avattua dataa | lkm |  |  |  |  |
| **Osaaminen ja ohjeistus** |  |  |  |  |  |
| Henkilöstön koulutukset | % |  |  |  |  |
| Henkilöstön osaamiskartoitukset | % |  |  |  |  |
| Seloste käsittelytoimista (30 art.) valmiusaste | % |  |  |  |  |
| Ohjeiden ajantasaisuus | % |  |  |  |  |
| Ohjeiden päivittämissykli | lkm |  |  |  |  |
| **Rekisteröidyn oikeudet** |  |  |  |  |  |
| Tietosuojaselosteet ja muu informointi valmiusaste | % |  |  |  |  |
| Henkilötietojen tietoturvaloukkaukset | lkm |  |  |  |  |
| Henkilötietojen tietoturvaloukkaukset ilmoitukset TSV | lkm |  |  |  |  |
| Henkilötietojen tietoturvaloukkaukset ilmoitukset rekisteröidyille | lkm |  |  |  |  |
| Henkilötietojen tietoturvaloukkausharjoitukset | lkm |  |  |  |  |
| Tehdyt tarkastuspyynnöt | lkm |  |  |  |  |
| Tehdyt poistopyynnöt | lkm |  |  |  |  |
| Tehdyt korjauspyynnöt | lkm |  |  |  |  |
| Käyttö- ja luovutuslokipyynnöt | lkm |  |  |  |  |
| Esille tulleet tietosuojarikkomukset  | lkm |  |  |  |  |
| Epäillyt tietosuojarikkomukset | lkm |  |  |  |  |
| Palveluestohyökkäykset | lkm |  |  |  |  |
| Virushavainnot | lkm |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |