## Sisällys



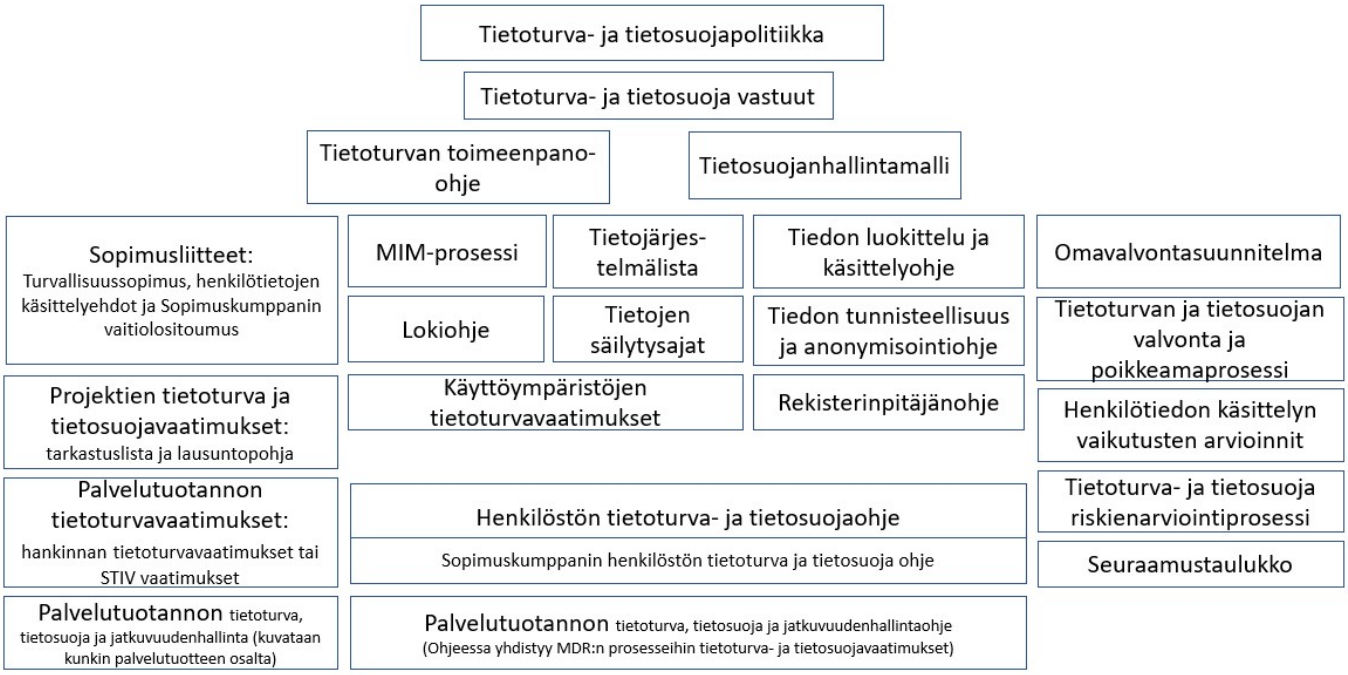
**VERSIOHISTORIA**

| Päivämäärä | Versio | Muutos | Tekijä |
|---|---|---|---|
| 16.3.2020 | 1.0 | Hyväksytty | Jenni Siermala |

# 1. JOHDANTO

SoteDigi Oy:n toiminta ja palvelut ovat riippuvaisia tietojärjestelmäpalveluiden keskeytyksettömästä saatavuudesta ja niiden turvallisesta toiminnasta. Tietojärjestelmäpalveluiden hyödyntäminen ja tietoturvallisuuteen panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan toimintakykyyn. Myös lainsäädäntö, standardit ja sopimukset asettavat velvoitteita tietoturvallisuudesta ja tietosuojasta huolehtimiselle.

Tietoturva- ja tietosuojapolitiikka on johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot. Tietoturva- ja tietosuojapolitiikka annetaan tiedoksi henkilöstölle ja heidän tulee toimia sen mukaisesti. Tietoturva- ja tietosuojapolitiikkaa tarkennetaan erillisissä ohjeissa.




Tiedon turvaaminen ja tietosuoja ovat osa toiminnan ja palveluiden laatua, kokonaisturvallisuutta sekä päivittäistä tietojen käsittelyä. Tietoturvan ja tietosuojan hyvä hallinta edellyttävät kaiken toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua, varautumista uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö niin henkilöstön kuin sen sidosryhmienkin tietojen käsittelyn osalta.

# 2. TAVOITTEET

### 2.1 Tietoturvan tavoitteet

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen. Tietojen turvallisuudesta on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä eli tiedon kaikissa muodoissa sen koko sen elinkaaren ajan. Tietojen turvaamisesta on huolehdittava kaikissa SoteDigi Oy:n toiminnoissa.

Tietoturvallisuustyö on tietojen turvaamiseksi tehtävää jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seurantaa. Sillä pyritään ennalta ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne riskienhallinnan avulla hyväksyttävälle tasolle. Tietoturvallisuudesta huolehditaan asiakkaiden vaatimusten sekä kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti noudattaen tietoturvallisuuden parhaita käytäntöjä ja suosituksia.

### 2.2 Tietosuojan tavoitteet

Tietosuojan tavoitteena on säilyttää henkilötietojen luottamuksellisuus sekä suojata tiedot luvattomalta tai henkilöä vahingoittavalta käytöltä. Toisin sanoen henkilötietoja saavat käsitellä vain ne henkilöt, joiden työtehtäviin henkilötietojen käsittely kuuluu.

Rekisterinpitäjänä ja henkilörekisterin käsittelijänä SoteDigi Oy huolehtii, että tietosuoja-asetuksessa ja kansallisessa tietosuojalaissa määriteltyjä tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa.

Tietosuojaperiaatteiden mukaan henkilötietoja käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Käsittelyn tulee rajoittua vain niihin tarkoituksiin, joita varten tiedot on kerätty tai jotka ovat yhteensopivia alkuperäisen käyttötarkoituksen kanssa. Tietosuojasta on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä eli tiedon kaikissa muodoissa sen koko sen elinkaaren ajan.

## 3. TIETOTURVAN ORGANISOINTI JA VASTUUT

Kokonaisuutena SoteDigi Oy:n toiminnasta ja sen turvallisuudesta vastaa toimitusjohtaja.

Kunkin palvelun ja prosessin vastuuhenkilö on vastuussa myös tietoturvasta. Tarvittaessa palveluille ja prosesseille voidaan nimetä erilliset tietoturvan vastuuhenkilöt. Jokaisen prosessiin ja toimintoon kuuluvan ja muuten palvelun tuottamiseen osallistuvan henkilön edellytetään toimivan vastuullisesti sekä huolehtivan omalta osaltaan vastuu- ja tehtäväalueensa turvallisuudesta.

Jokainen SoteDigi Oy:lle työskentelevä on velvollinen noudattamaan sääntöjä ja ohjeita. Jokaisen velvollisuutena on ilmoittaa havaitsemistaan turvallisuuspuutteista ja -heikkouksista sekä tapahtuneista häiriöistä ja vahingoista tai niiden epäilyistä sekä läheltä piti -tilanteista joko esimiehelleen tai tietoturvapäällikölle.

Keskeisimmät tietoturvallisuuteen ja tietosuojaan liittyvät toimijat, roolit, vastuut ja velvollisuudet on kuvattu *Tietoturva- ja tietosuojavastuut* -dokumentissa.

## 4. TOTEUTUSKEINOT

Tietoturvan ja tietosuojan ylläpito ja kehittäminen on jatkuva prosessi, jota johdetaan suunnitelmallisesti. Turvallisuuden kehittämisen toimenpiteet suunnitellaan, resursoidaan ja aikataulutetaan. Lisäksi varaudutaan kykyyn reagoida muutoksiin ja suunnata toimenpiteitä kulloinkin tärkeimpiin kohteisiin. Tietoturvallisuuteen kohdistuvat riskit arvioidaan ja käsitellään systemaattisesti.

Henkilöstön turvallista toimintaa johdetaan käyttösäännöillä ja toimintaohjeilla sekä tietojen turvallisen käsittelyn perehdytyksillä, koulutuksilla, viestinnällä ja hyvällä esimiestyöllä. Henkilöstön turvallisuusosaaminen ja toiminnan turvallisuus varmistetaan koulutuksien ja seurannan avulla. Tietoturvapäällikkö tukee esimiestä tässä työssä.

Järjestelmien, teknisten toimintaympäristöjen, käsittelyprosessien ja ulkoisten palveluiden tietoturvallisuus varmistetaan yhteistyössä tietoturvapäällikön kanssa. Tietoturvallisuus varmistetaan määrittelemällä turvallisuusvaatimukset, varmistamalla asetettujen vaatimusten täyttyminen, huolehtimalla käyttöönottojen turvallisuudesta, ottamalla turvallisuusvaatimukset huomioon sopimuksissa sekä ylläpitämällä turvallisuusominaisuuksia koko elinkaaren ajan.

Tietoturvahäiriöt käsitellään häiriöhallintaprosessin mukaisesti. Palveluiden jatkuvuuden varmistamiseksi ylläpidetään jatkuvuussuunnitelmia, joiden mukaisesti toimitaan poikkeustilanteissa. Suunnitelmien toimivuus varmistetaan riittävällä testaamisella ja poikkeustilanteiden harjoittelulla.

Tietoturvallisuus osoitetaan dokumentoiduilla tietoturvallisuuden hallinnan prosesseilla sekä prosessien toteuttamisen ja seurannan yhteydessä syntyvällä dokumentaatiolla.

Henkilötietojenkäsittelyn tietosuoja varmistetaan lisäksi noudattamalla tietosuojaperiaatteita kuten lainmukaisuus, läpinäkyvyys ja käyttötarkoitussidonnaisuus. Nimetty tietosuojavastaava seuraa ja antaa neuvoja tietosuojan huomioon ottamisesta henkilötietojen käsittelyprosesseissa.

## 5. SALASSAPITO JA VAITIOLOVELVOLLISUUS

Terveydenhuollon potilasrekistereihin ja sosiaalihuollon asiakasrekistereihin sisältyvät tiedot ovat salassa pidettäviä suoraan lainsäädännön perusteella. Liike- ja ammattisalaisuudet sekä tiedot toimintamalleista, prosesseista ja teknisistä toteutuksista ovat salassa pidettäviä tietoja julkisuuslain perusteella, jos kyseinen tieto on määritelty salassa pidettäväksi. Lisäksi vaitiolovelvollisuus koskee muita ei julkisia tietoja.

Salassapitovelvollisuus jatkuu myös työ- tai sopimussuhteen päätyttyä asiaan liittyvän lainsäädännön tai erikseen sovitun salassapidon mukaisesti. Työsuhteen päättyessä on työntekijä luovuttaa hallussaan olevat dokumentit, ohjelmistot, työkalut yms. SoteDigi Oy:lle.

## 6. TIETOTURVAN JA TIETOSUOJAN SEURANTA JA ONGELMATILANTEIDEN KÄSITTELY

Tietoturvapäällikön tehtävänä on tehdä tietojenkäsittelyn turvallisuuteen liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi. Erikseen nimetyillä henkilöillä on häiriötilanteissa oikeus ryhtyä välittömiin toimenpiteisiin organisaatioon tai sen tietoihin kohdistuvan riskin minimoimiseksi.

Tietoturvallisuuden ylläpito edellyttää jatkuvaa seurantaa ja raportointia. Tietoturvapäällikkö koordinoi tietoturvallisuuden seurantaa ja raportoi säännöllisesti tietoturvallisuudesta johtoryhmälle.

Henkilöstön tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista tietoturvapäällikölle tai esimiehelle. Kaikki tietoturva- ja tietosuojapoikkeamatilanteet raportoidaan ja jokaiseen tilanteeseen reagoidaan asian vaatimalla tavalla.

23.3.2020 Helsingissä

Harri Hyvönen
Toimitusjohtaja