THL määräys 3/2021 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

Vuoden 2022 Kanta-palvelujen käyttöönottojen ohjaustunti (1/3)
11.2.2022

Sote-tiedonhallinta - sotetiedonhallinta@thl.fi

Erityisasiantuntija Antti-Olli Taipale

Terveyden ja hyvinvoinnin laitos

Mikä tietoturvasuunnitelma 1/2?

Määräys 3/2021 on osa laajempaa määräysten kokonaisuutta, jolla toimeenpannaan uutta asiakastietolakia 784/2021

- Uudessa **asiakastietolaissa** aiemman lain tietosuojan ja tietoturvallisuuden sekä tietojärjestelmien käytön omavalvontasuunnitelma **on korvautunut tietoturvasuunnitelmalla**

- Sosiaali- ja terveydenhuollon toimijat **velvoitetaan laatimaan** tietoturvasuunnitelma
  - aiempi tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelma on pohja uuden lain mukaiselle tietoturvasuunnitelmalle: sisältö pääosin vastaava kuin aiemman asiakastietolain edellyttämässä omavalvontasuunnitelmassa

- Tietoturvasuunnitelma **edistää asiakas- ja potilastietojen turvallista käsittelyä sekä sote-toimijoiden tietosuojaa ja tietoturvaa** – vahvistaa tietoturvallisuuden ja tietosuojan suunnittelun ja toteuttamisen käytäntöjä

- Määräys **tarkentaa tietoturvasuunnitelmaan tarvittavien** selvitysten **sisältöä** ja tietoturvallisuudelle sosiaali- ja terveyspalveluissa asetettavia **vaatimuksia**.

Mikä tietoturvasuunnitelma 2/2?

- Uuden asiakastietolain ja määräysten kautta täsmennetään myös **tietojärjestelmiin** kohdistuvien **olennaisten vaatimusten** toteutumista **sote-palveluiden järjestäjien ja tuottajien näkökulmasta**

  - tietoturvasuunnitelma on myös palvelunantajan väline olennaisten vaatimusten täyttämisen varmistamisessa
  - sitoo yhteen sekä palvelunantajan omat käytännöt että kaikki käytössä olevat tietojärjestelmät ja ICT-palvelut

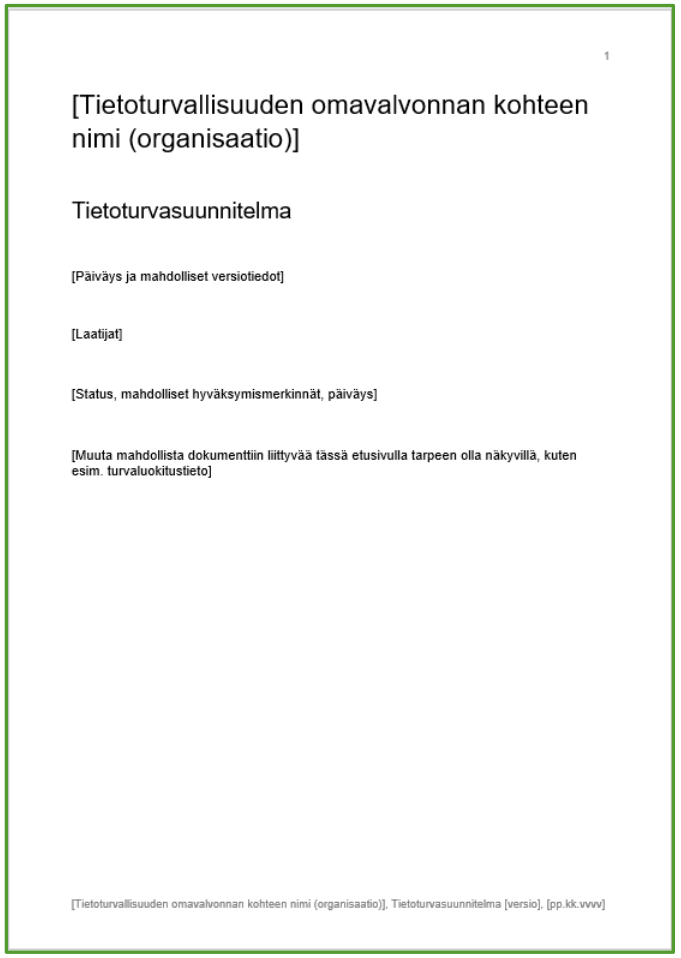
- **Tietoturvasuunnitelma ei ole julkinen** asiakirja

  - *”Tämän määräyksen mukaista tietoturvasuunnitelmaa **ei tule sisällyttää tai yhdistää** julkaistaviin tai julkisesti saatavilla oleviin omavalvontasuunnitelmiin.”*

  - *”Tietoturvasuunnitelmaa ja siinä viitattuja liitedokumentteja **tulee käsitellä ja säilyttää ottaen huomioon tarvittava suojaaminen sivullisilta** ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto.”*

- Tietoturvasuunnitelma on hyvä **käytännön työväline** – kokoava dokumentti, ”**kokonaisturvallisuuden** toimeenpanon ja seurannan suunnitelma”

Mikä tietoturvasuunnitelman mallipohja?



1

[Tietoturvallisuuden omavalvonnan kohteen nimi (organisaatio)]

Tietoturvasuunnitelma

[Päiväys ja mahdolliset versiotiedot]

[Laatijat]

[Status, mahdolliset hyväksymismerkinnät, päiväys]

[Muuta mahdollista dokumenttiin liittyvää tässä etusivulla tarpeen olla näkyvillä, kuten esim. turvaluokitustieto]

[Tietoturvallisuuden omavalvonnan kohteen nimi (organisaatio)], Tietoturvasuunnitelma [versio], [pp.kk.vvvv]

- Määräyksen 3/2021 liitteenä on **tietoturvasuunnitelman mallipohja**
  - uudistettu ja selkeytetty verrattuna aiemman määräyksen mukaisiin mallipohjiin
- Mallipohja on tarkoitettu vapaaehtoisesti hyödynnettäväksi
  - **tietoturvasuunnitelman voi laatia tarkoituksenmukaiseksi katsomallaan tavalla**, kunhan suunnitelmasta tai sen liitteistä käyvät määräyksessä 3/2021 esitetyt seikat selkeästi ilmi
  - tietoturvasuunnitelma voi koostua myös useammasta dokumentista, joista osa voi olla suunnattu henkilöstölle, osa tietohallinnolle tai tietosuojan vastuuhenkilöille
- Mallipohjasta on määräyksen liitteeksi laadittu **vain yksi versio**
  - kooltaan ja toiminnaltaan hyvinkin erilaiset sote-palvelunantajat voivat soveltaa, tiivistää tai täydentää mallipohjaa omaan toimintaansa peilaten
- Aiempi tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelma **on päivitettävä** voimassa olevan asiakastietolain mukaiseksi **tietoturvasuunnitelmaksi**
  - päivittämisessä on suositeltavaa lähteä liikkeelle kriittisimmistä kohteista omassa toiminnassa tunnistettujen riskien ja tietoturvallisuuden tilan tarkastelun kannalta

Määräys 3/2021 vs. tietoturvasuunnitelman mallipohja

Sisällys

Sisällys

Asiakastietolaki 27 1 § ja 2 § avattuina sekä 28 §

(Tietoturvallisuuden) omavalvonnan kohde laatii Tietoturvasuunnitelman

Tietoturvasuunnitelmassa on oltava **selvitykset** siitä, **miten** seuraavat asiakas- ja potilastietojen ja järjestelmien käsittelyyn liittyvät **vaatimukset (= ”velvoitteet”)** varmistetaan:

Selvitykset voidaan **kuvata suoraan** tietoturvasuunnitelmaan tai **niihin voidaan viitata** tietoturvasuunnitelmassa liitedokumenteilla, linkeillä, …

"Tietoturvasuunnitelman kohteena olevista tahoista käytetään tässä määräyksessä ja määräyksen liitteessä yleisnimeä tietoturvallisuuden omavalvonnan kohde tai omavalvonnan kohde."

Asiakastietolaki 28 §
Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu
Sosiaali- ja terveydenhuollon palvelunantajan vastaavan johtajan on huolehdittava, että 27 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan ja sitä noudatetaan. Vastaavan johtajan on annettava kirjalliset ohjeet asiakastietojen käsittelystä ja noudatettavista menettelytavoista sekä huolehdittava henkilökunnan riittävästä asiantuntemuksesta ja osaamisesta asiakastietojen käsittelyssä.

Velvoitteet Määräyksessä 3/2021 = Asiakastietolaki 784/2021 27 § 1 momentti

1) henkilöillä, jotka käyttävät tietojärjestelmiä, on niiden käytön vaatima koulutus;

2) tietojärjestelmien yhteydessä on saatavilla niiden asianmukaisen käytön kannalta tarpeelliset käyttöohjeet;

3) tietojärjestelmiä käytetään tietojärjestelmäpalvelun tuottajan antaman ohjeistuksen mukaisesti;

4) tietojärjestelmiä ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti;

5) tietojärjestelmän käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön;

6) tietojärjestelmiin liitetyt muut tietojärjestelmät tai muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia;

7) tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus;

8) 29 §:ssä tarkoitetut tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset 34 §:ssä säädetyt olennaiset vaatimukset; sekä

9) **palvelunantajalla, välittäjällä ja Kansaneläkelaitoksella** on suunnitelma siitä, miten omavalvonta järjestetään ja toteutetaan sen toiminnassa.

Asiakastietolaki 784/2021 27 § 2 momentti

Ennen liittymistään valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi on palvelunantajan tietoturvasuunnitelmassa **selvitettävä**, **miten** tietosuoja ja valtakunnallisten palvelujen tietoturvallisen käytön edellyttämät **vaatimukset** on varmistettu.

Yhteenveto tietoturvasuunnitelmasta

- **Tietoturvasuunnitelma** on keskeinen käytännön työväline palvelunantajalle sosiaali- ja terveydenhuollon tietosuojan ja tietoturvallisuuden suunnitteluun, toteuttamiseen ja seurantaan
- Tietoturvasuunnitelma auttaa riskienhallinnassa, tietoturvallisuustyössä, tietojärjestelmien hallinnoinnissa ja varautumisessa
- Asiakastietolain toimeenpano ja määräykset luovat pohjaa esim. hyvinvointialueiden tarvitsemalle tiedonhallinnalle – tietoturva- ja tietosuojakäytäntöjen yhdenmukaistaminen ja parantaminen on keskeinen osa suunnittelua myös sote-uudistuksessa
- Tietoturvasuunnitelma on sovitettava organisaation omaan toimintaan ja kokoon – otettava huomioon erityisesti tähän yhteyteen liittyvät sopimukset ja kumppanuudet
- Tietoturvan ja tietosuojan omavalvonta ja sen dokumentointi tietoturvasuunnitelmaan auttaa myös mm. EU:n yleisen tietosuoja-asetuksen mukaisen osoitusvelvollisuuden täyttämisessä
- Vastuu tietoturvasuunnitelman laatimisesta ja noudattamisesta on sote-organisaation vastaavalla johtajalla (Asiakastietolaki 28 §)

Tietoturvasuunnitelma verkossa

- THL Määräys 3/2021 - Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset on julkaistu Finlexissä 20.12.2021: FINLEX ® - Viranomaisten määräyskokoelmat – Terveyden ja hyvinvoinnin laitos: https://www.finlex.fi/fi/viranomaiset/normi/561001/47658

- Määräys ja mallipohja ovat saatavilla THL:n sivuilla: https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset

Koulutusta tietoturvasuunnitelmasta

- **Tietoturvasuunnitelmasta järjestetään koulutustilaisuus 31.3.2022**
  https://thl.fi/fi/ajankohtaista/tapahtumat/tapahtumakalenteri/-/event/8473157

- 31.3.2022 pidettävä koulutus uusitaan noin puolen vuoden kuluttua syksyllä 2022

Tietoturvasuunnitelman koulutustilaisuus sote-palvelunantajille

Tiedonhallinta sosiaali- ja terveysalalla

Torstai 31.03.2022 - Torstai 31.03.2022

09:00 - 11:30

Teams-tapahtuma

Lataa omaan kalenteriisi

Koulutuksessa paneudutaan uuden asiakastietolain 784/2021 mukaisen tietoturvasuunnitelman laadintaan THL:n määräyksen 3/2021 ja tietoturvasuunnitelman mallipohjan kautta.

Koulutuksessa käsitellään myös aiemman lain mukaisten omavalvontasuunnitelmien päivittämistä.

Koulutuksessa esiintyvät Terveyden ja hyvinvoinnin laitoksen asiantuntijat **Juha Mykkänen** ja **Antti-Olli Taipale**.

Tämä tietoturvasuunnitelman koulutus uusitaan noin puolen vuoden kuluttua syksyllä 2022.

Kiitos!