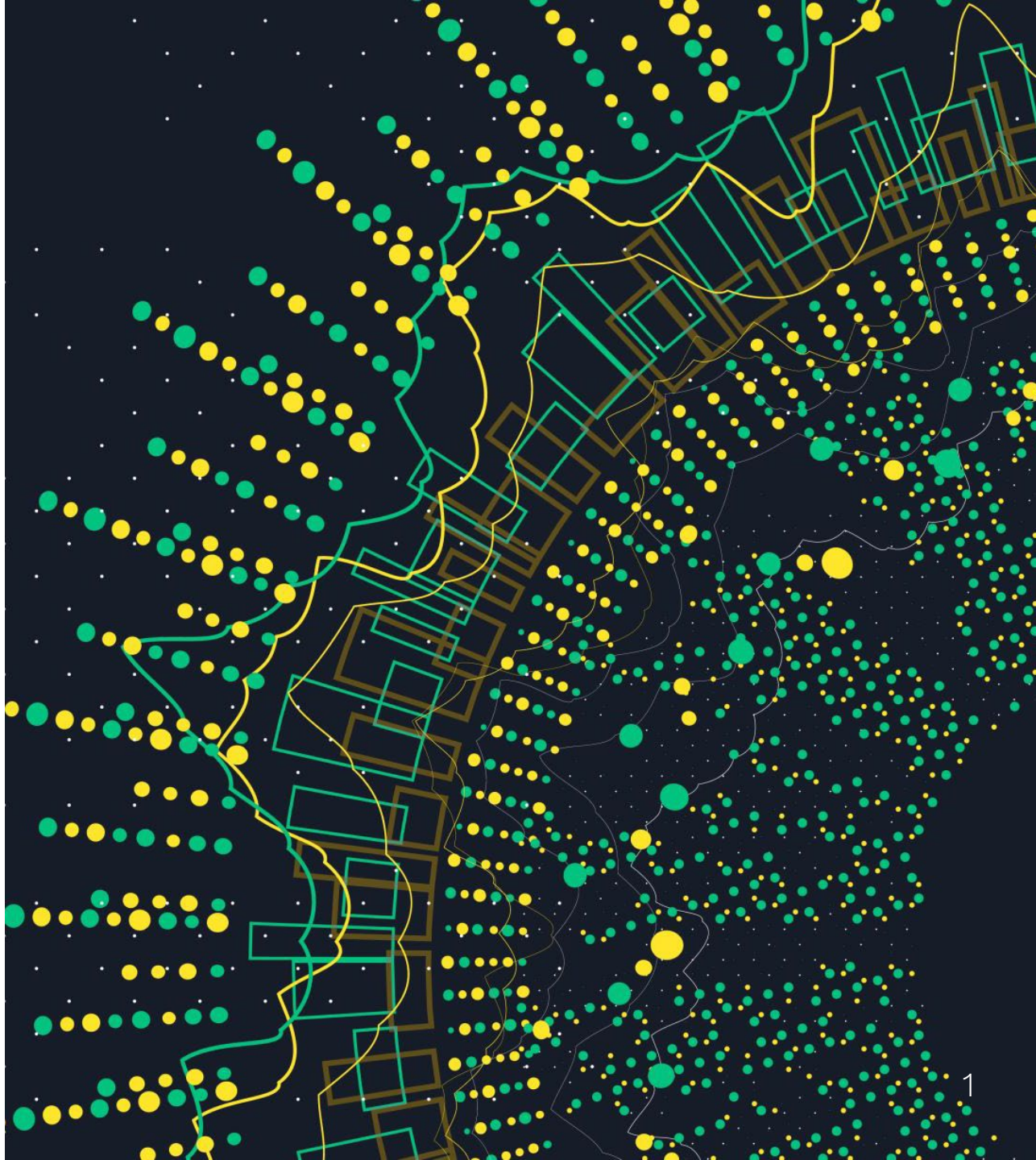
Uudistunut tietoturvasuunnitelma

THL:n määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista

Tiima-foorumi
11.4.2024



Alkuun vähän historiaa 1.7.2007 – nykypäivä 11.4.2024

Kumoutuneet

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007

X
  - Ollut voimassa 1.7.2007-31.10.2021
  - THL:n määräys 2/2015 Omavalvontasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista.

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021

X
  - Ollut voimassa 1.11.2021-31.12.2023
  - THL:n määräys 3/2021 **Tietoturvasuunnitelmaan** sisällytettävistä selvityksistä ja vaatimuksista.

Voimassa

- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023 – 1.1.2024 lähtien
  - THL:n määräys 3/2024 **Tietoturvasuunnitelmaan** sisällytettävistä selvityksistä ja vaatimuksista – 22.2.2024 lähtien

Kaiken perustana 1.1.2024 voimaan tullut asiakastietolaki

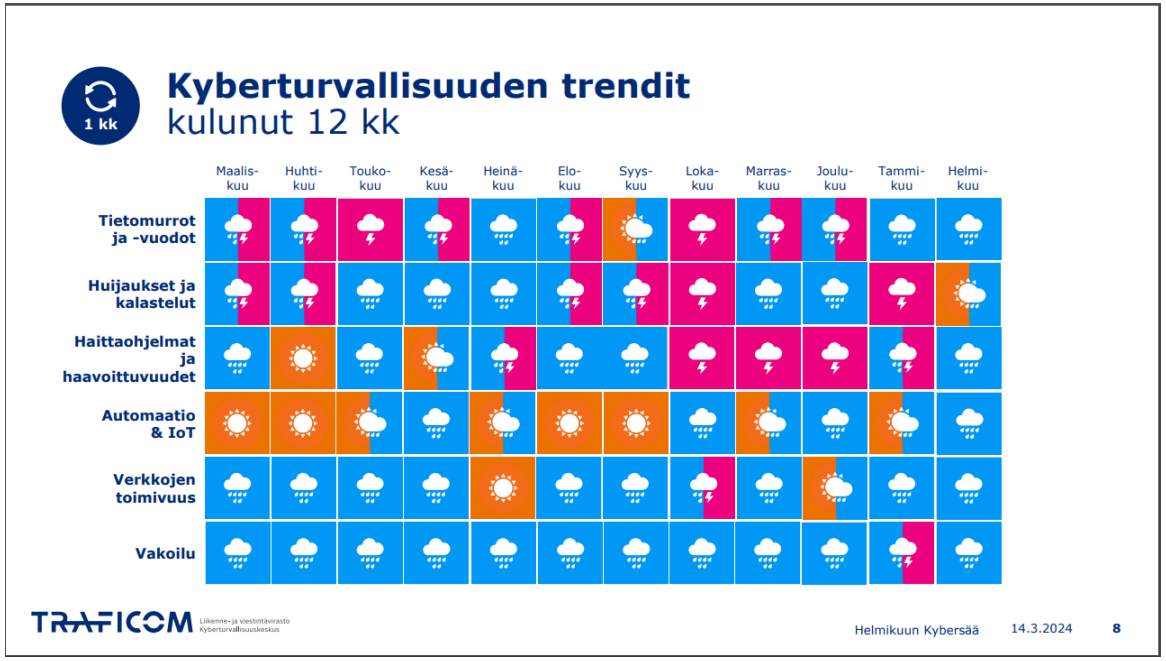
- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023 ja sieltä erityisesti **pykälät 77** ja **78**:

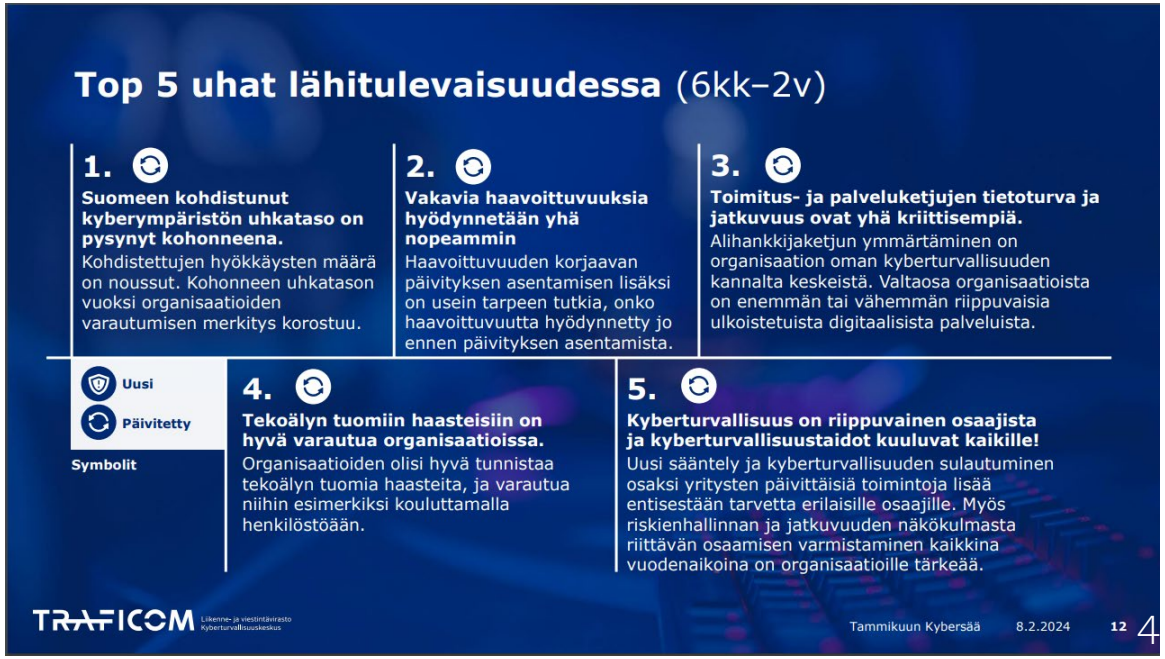
- 77 §: ”**Palvelunantajan, apteekin, välittäjän ja Kansaneläkelaitoksen on laadittava** tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma. Tietoturvasuunnitelmassa on selvitettävä, miten asiakas- ja potilastietojen käsittelyyn ja tietojärjestelmiin liittyvät vaatimukset varmistetaan:…”

- 78 §: ”Sosiaali- ja terveydenhuollon **palvelunantajan vastaavan johtajan ja apteekkarin on huolehdittava**, että 77 §:ssä tarkoitettu **tietoturvasuunnitelma laaditaan ja sitä noudatetaan**. Palvelunantajan, apteekin ja Kansaneläkelaitoksen tulee oma-aloitteisesti ryhtyä tarvittaviin toimenpiteisiin, jos joku on lainvastaisesti käsitellyt asiakastietoja. …”.

Minkälaisessa maailmassa elämme vs. digiturvallisuus 1/2?

- Traficomin Kyberturvallisuuskeskuksen kybersäät alkuvuodesta 2024 nostavat esille kuluneiden 12 kuukauden trendit ja Top 5 uhat lähitulevaisuudessa 2024-2026.





Minkälaisessa maailmassa elämme vs. digiturvallisuus 2/2?

14.8.2023

yle Etusivu | Vaalikone | Venäjän hyökkäys | UMK24

Teknologia

Tekoälyn tekemät monimutkaiset huijaukset lisääntyvät Suomessakin muutaman vuoden sisään, asiantuntija ennakoi

Tekoäly pystyy jo matkimaan ihmisääntä keräämänsä aineiston pohjalta. Hädissään soittava "lapsi" voi olla huijausta.

4.12.2023

yle Etusivu | Vaalikone | Venäjän hyökkäys | UMK24

Turvallisuus

Romanssihuijarit ovat jo valjastaneet tekoälyn käyttöönsä – videopuhelussa näkemääsi ihastusta ei ehkä ole olemassakaan

Järjestäytynyt rikollisuus kouluttaa jäseniään hyödyntämään uusinta teknologiaa. Jo verkon ilmaisohjelmat ja diginatiivius tarjoavat valmiudet huijauksiin.

11.9.2023

mtv UUTISET

Asiantuntija varoittaa yhä uskottavammista tekoälyn luomista huijauksista: "Minua on huijattu ja tullaan huijaamaan"

17.1.2024

mtv UUTISET

Tena-tuotteiden valmistajan toimet syynissä – taustalla jättimäinen tietomurto

LEHTIKUVA

JULKAISTU 17.01.2024 13:58

MTV UUTISET – STT

Tietosuojavaltuutetun toimisto selvittää parhaillaan Tenan inkontinenssisuojia valmistavan Essity-yhtiön ja lääkealan yhtiön Roche Diagnosticsin toimintaa Westlog-yhtiöön tehdyn tietomurron vuoksi.

24.1.2024

ILTA-SANOMAT

TIETOTURVA

OmaKanta-huijaus yrittää viedä rahasi – näin sen erottaa aidosta sivusta

Huijaussivu näyttää varsin aidolta.

JAA | TALLENNA | KOMMENTIT

21.3.2023

UUSI TEKNOLOGIA.fi

UUDET TEKNIIKAT · TUTKIMUS · TUOTEKEHITYS · INNOVAATIOT · PROTOT · PALVELUT

Tekoälyn ChatGPT-huijaukset rajussa kasvussa

Artikkelit/raportit - 21.4.2023

Uutta ChatGPT-palvelua ja yleisemmin tekoälyn suosiota käytetään Palo Alto Networksin mukaan syöttinä ihmisten huijaamisessa ja haittaohjelmien asentamisessa. Yhtiön turvayksikkö Unit 42 on julkaissut uuden selvityksen alueen huijausyrityksistä.

18.10.2023

Helsingin Uutiset

Vastaamon tietomurtaja sai syytteen tuhansista rikoksista

Tietoturvasuunnitelma

- edistää asiakas- ja potilastietojen turvallista käsittelyä
- parantaa ja yhdenmukaistaa sote-toimijoiden tietosuojaa ja tietoturvaa
- vahvistaa tietoturvallisuuden ja tietosuojan suunnittelun ja toteuttamisen käytäntöjä
- auttaa erityisesti hallitsemaan tämän päivän **digitaaliseen turvallisuuteen liittyviä riskejä**.

- Tietoturvasuunnitelman laativat kaikki sosiaali- ja terveydenhuollon palvelunantajat, apteekit, välittäjät ja Kansaneläkelaitos.
- Organisaation **velvollisuutena** on **toimia tietoturvasuunnitelman mukaisesti**, **katselmoida** ja ylläpitää suunnitelmaa säännöllisesti sekä **seurata aktiivisesti** sen toteutumista.

! **Tietoturvasuunnitelman laatimiseen velvoitetuista tahoista** eli sosiaali- ja terveydenhuollon palvelunantajista, apteekeista, välittäjistä ja Kansaneläkelaitoksesta (Kela), käytetään määräyksessä ja määräyksen liitteessä yleisnimeä tietoturvallisuuden omavalvonnan kohde.

Riskit hallintaan tietoturvasuunnitelmalla 1/2

- **Kumulatiivinen riski** – riski, jonka suuruus muodostuu useiden riskitekijöiden yhteisvaikutuksista
- **Välitön riski** – riski, jonka lähde vaikuttaa suoraan kohteeseen
- **Välillinen riski** – riski, jonka lähde vaikuttaa epäsuorasti kohteeseen
- **Digitaalisen toiminnan riski** – digitaalisessa toimintaympäristössä vaikuttava, digitaaliseen toimintaympäristöön kohdistuva tai siitä johtuva riski
- **Jäännösriski** – riskin käsittelyn jälkeen jäljellä oleva riski.

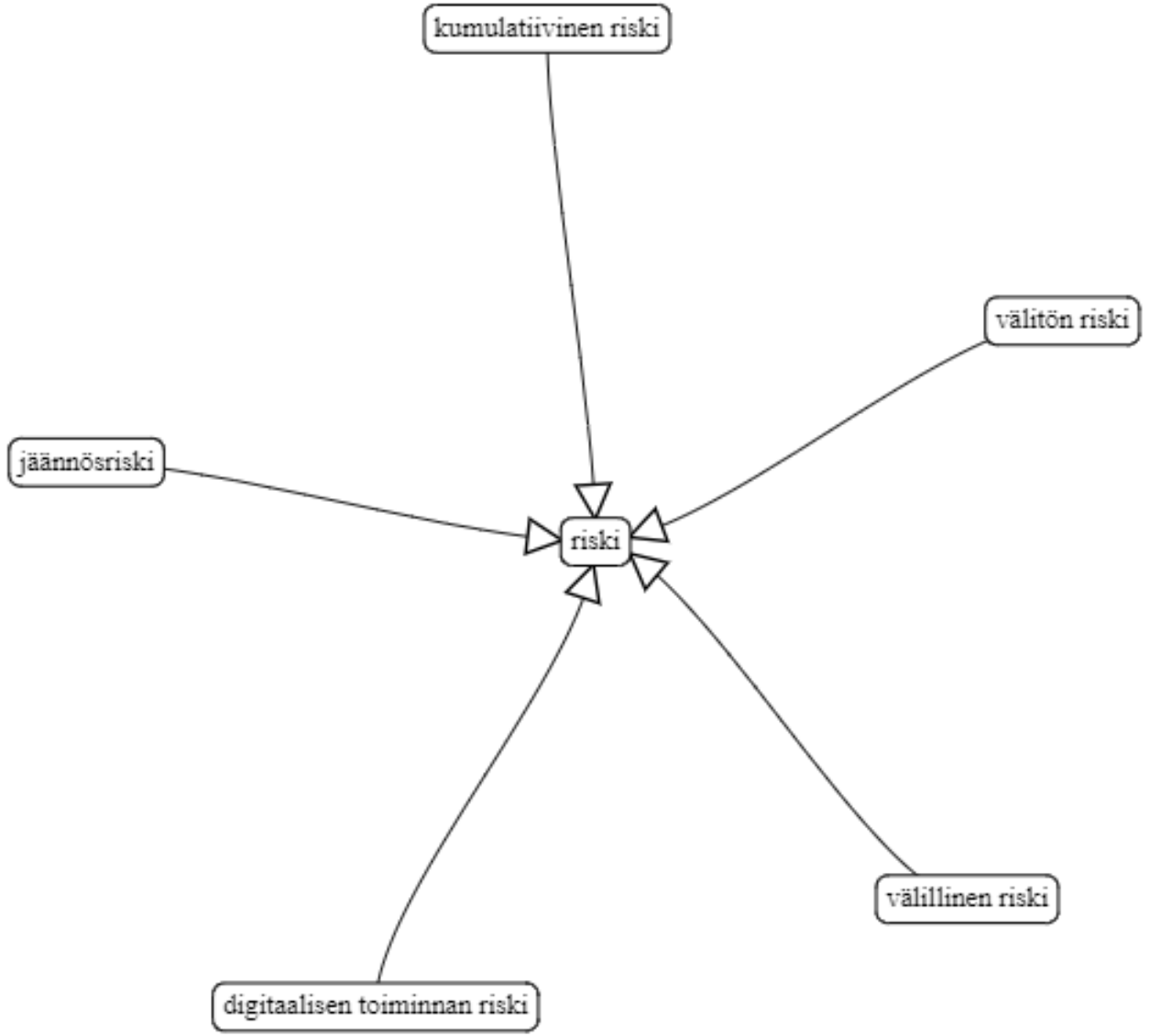
thl

Tässä olevien riskimäärittelyjen lähde, VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön (DVV)

Riskit hallintaan tietoturvasuunnitelmalla 2/2

”Tietoturvallisuuden omavalvonnan kohteen **velvollisuutena** on toimia laatimansa tietoturvasuunnitelman mukaisesti, **säännöllisesti ylläpitää ja katselmoida** suunnitelmaansa sekä seurata aktiivisesti sen toteutumista.

Kyse on jatkuvasta ja säännöllisestä riskienhallinnasta, asianmukaisten tietoturvallisuuden ja asiakastietojen käyttöön liittyvien käytäntöjen varmistamisesta sekä niiden toteuttamisesta.”



[Kuvan lähde, VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön (DVV)]

Mitä tietoturvasuunnitelma sisältää 1/2?

- Tietoturvasuunnitelma kuvaa, miten organisaatio järjestää toiminnassaan tietoturvan ja -suojan omavalvonnan

- Tietoturvasuunnitelmasta tulee selvitä, miten palveluntuottaja täyttää asiakas- ja potilastietojen ja tietojärjestelmien käsittelyyn liittyvät asiakastietolain vaatimukset

- Tietoturvasuunnitelmaa ja siitä viitattuja liitedokumentteja tulee käsitellä ja säilyttää tietoturvallisesti. Ne tulee suojata sivullisilta, ja tarvittaessa niihin tulee merkitä salassa pidettävä -tieto. Tietoturvasuunnitelma on aina ei-julkinen asiakirja.

Mitä tietoturvasuunnitelma sisältää 2/2?

- Asiakastietolain (77 §) vaatimukset tietoturvasuunnitelmalle:
  - tietojärjestelmien käyttäjillä on käytön vaatima koulutus
  - käyttöohjeet ovat saatavilla järjestelmän yhteydessä
  - käyttäjät noudattavat tietojärjestelmäpalvelun tuottajan ohjeita
  - tietojärjestelmiä ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti
  - käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen käyttöön ja varmistaa tietoturvan ja tietosuojan
  - tietojärjestelmiin kohdistuvien riskien hallinnasta huolehditaan
  - tietojärjestelmiin liitetyt muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia
  - tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus
  - tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset olennaiset vaatimukset.

Tietoturvasuunnitelmaa koskevan määräyksen sisältö

thl

MÄÄRÄYS 3/2024 1(23)
THL/4/4.05.00/2024

Tiedonvälittäjät
Tieto ja tiedonhallinnan ohjaus 20.2.2024

MÄÄRÄYS TIETOTURVASUUNNITELMAAN SISÄLLYTETTÄVISTÄ SELVITYKSISTÄ JA VAATIMUKSISTA

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) 77 § 3 momentti

Kohderyhmät

Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Välittäjät
Kansaneläkelaitos (Kela)

Voimaantulo

Tämä määräys tulee voimaan 22. päivänä helmikuuta 2024 ja on voimassa toistaiseksi.

Tämä määräys korvaa aiemman Terveyden ja hyvinvoinnin laitoksen (THL) määräyksen THL 3/2021 Tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) kumoaa aiemman määräyksen antamiseen valtuuttaneen lain sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021), jonka nojalla annetut alemman asteiset säädökset kumoutuvat.

thl

2(23)

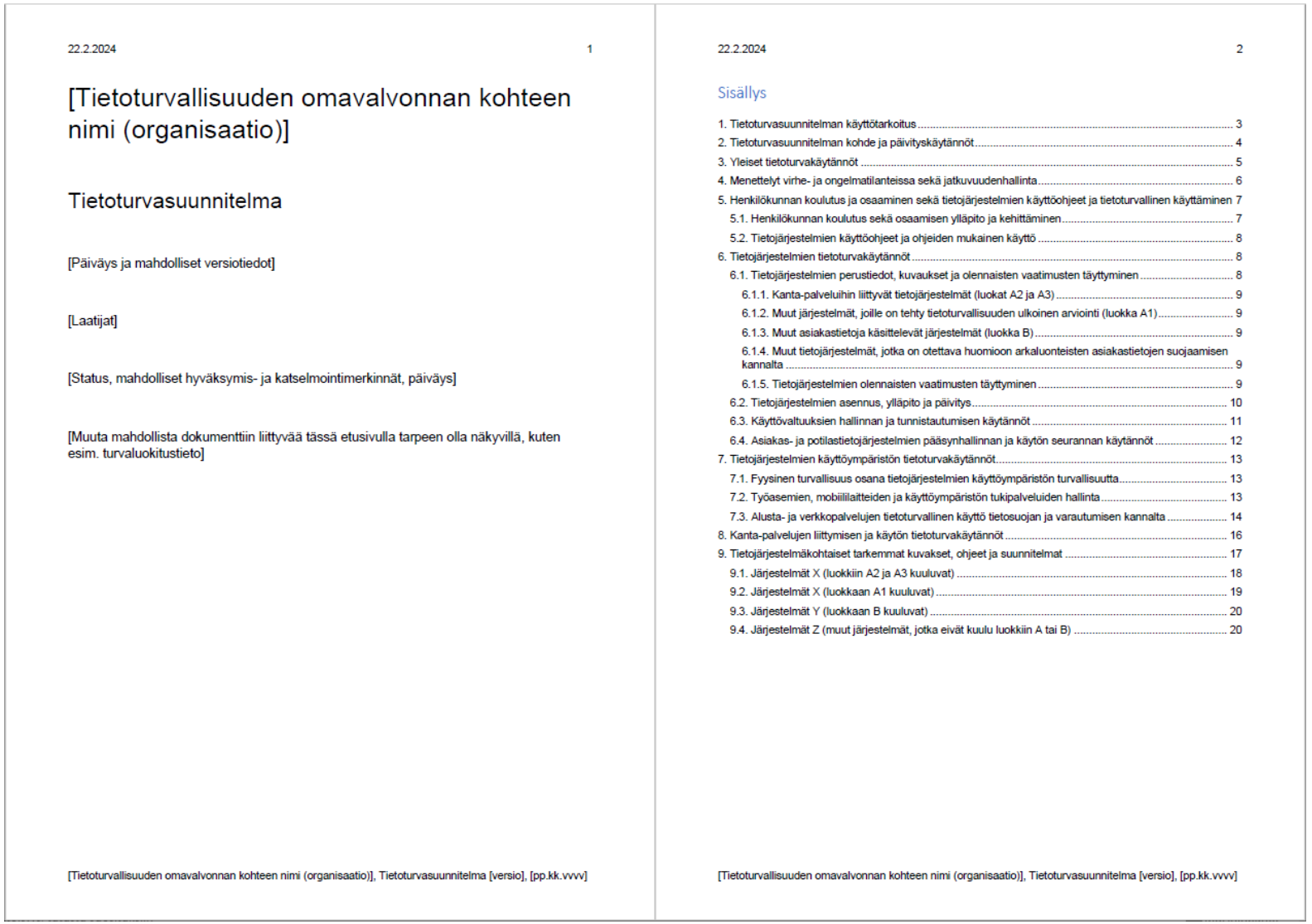
Sisällys

1 Määräyksen tarkoitus ja soveltamisala ... 3
2 Määritelmät ... 4
3 Vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa ... 6
4 Suhde THL:n muihin määräyksiin, yleisiin viitekehyksiin sekä eräisiin muihin säädöksiin ... 7
5 Yleistä tietoturvasuunnitelmasta ... 8
6 Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset ... 9
6.1 Yleiset tietoturvakäytännöt ... 9
6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta ... 10
6.3 Henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen ... 11
6.4 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö ... 12
6.5 Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen ... 13
6.6 Tietojärjestelmien asennus, ylläpito ja päivitys ... 15
6.7 Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt ... 16
6.8 Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt ... 17
6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta ... 18
6.10 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta ... 19
6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta ... 19
6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt ... 21
7 Ohjaus ja neuvonta ... 22
8 Voimaantulo ... 22
Tiedoksi ... 23

Liite Tietoturvasuunnitelman mallipohja

Tietoturvasuunnitelman laatimisen tueksi mallipohja

- Mallipohja ohjaa tietoturvasuunnitelman laatimista
- Mallipohjan avulla organisaatio varmistaa, että määräyksessä vaadittavat asiat huomioidaan
- Mallipohja sopii sekä pienille että suurille ja toiminnoiltaan erilaisille organisaatioille
- Tietoturvasuunnitelman sisältö tulee suhteuttaa oman toiminnan laajuuteen ja organisaation toimintaympäristössä tarvittaviin asianmukaisiin tietoturva- ja tietosuojakäytäntöihin.



22.2.2024 1

[Tietoturvallisuuden omavalvonnan kohteen nimi (organisaatio)]

Tietoturvasuunnitelma

[Päiväys ja mahdolliset versiotiedot]

[Laatijat]

[Status, mahdolliset hyväksymis- ja katselmointimerkinnät, päiväys]

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

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

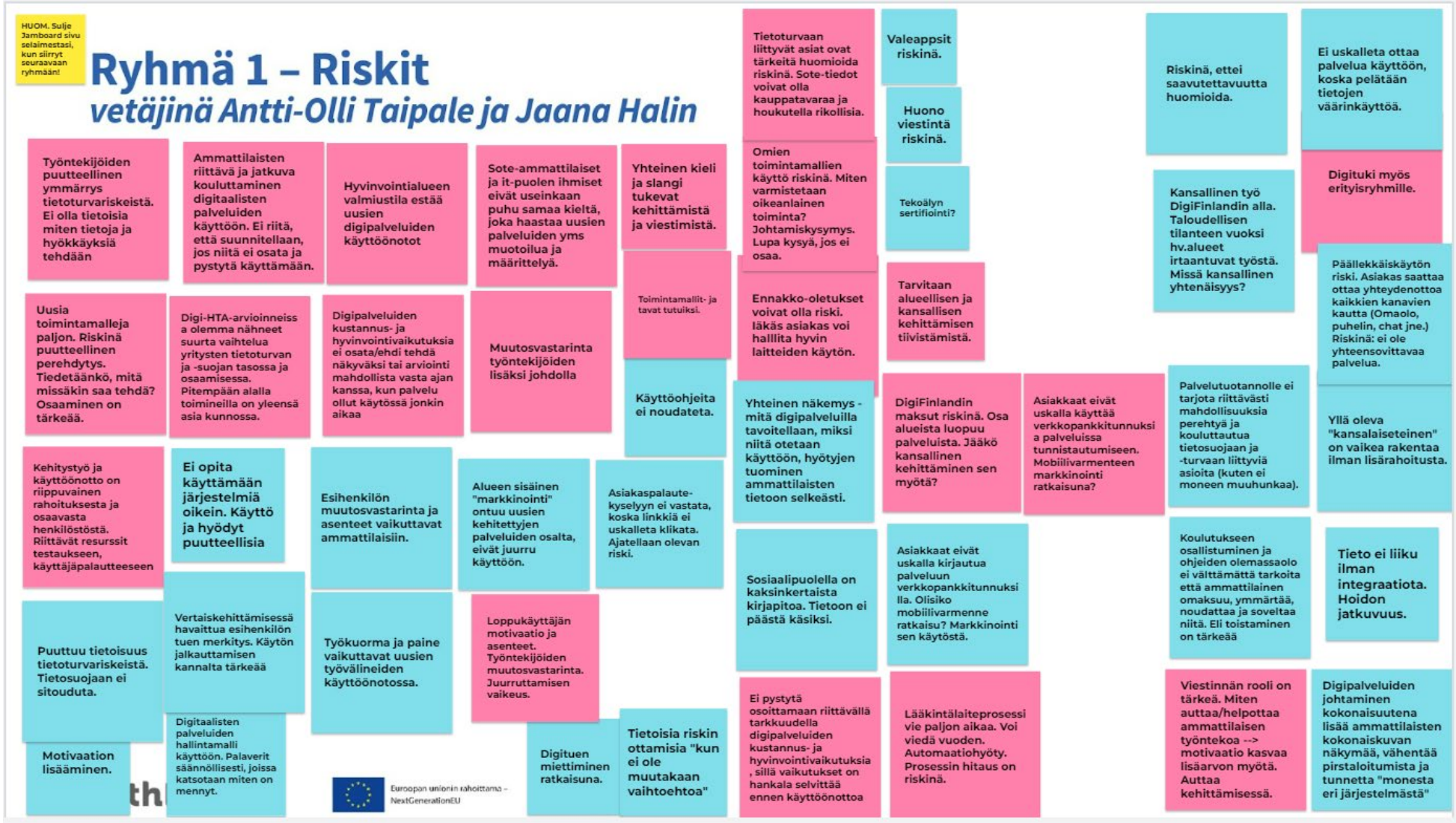
22.2.2024 2

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus 3
2. Tietoturvasuunnitelman kohde ja päivityskäytännöt 4
3. Yleiset tietoturvakäytännöt 5
4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta 6
5. Henkilökunnan koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen 7
5.1. Henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen 7
5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö 8
6. Tietojärjestelmien tietoturvakäytännöt 8
6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen 8
6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 ja A3) 9
6.1.2. Muut järjestelmät, joille on tehty tietoturvallisuuden ulkoinen arviointi (luokka A1) 9
6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B) 9
6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta 9
6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen 9
6.2. Tietojärjestelmien asennus, ylläpito ja päivitys 10
6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt 11
6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt 12
7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt 13
7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta 13
7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta 13
7.3. Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta 14
8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt 16
9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat 17
9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat) 18
9.2. Järjestelmät X (luokkaan A1 kuuluvat) 19
9.3. Järjestelmät Y (luokkaan B kuuluvat) 20
9.4. Järjestelmät Z (muut järjestelmät, jotka eivät kuulu luokkiin A tai B) 20

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

Mitä sote-kentällä ajatellaan riskeistä?



Riskien ”hillotaulu” -yhteenveto RRP:n investointi 4:n verkostotapaamisesta 1.2.2024

Kiteytys – mistä tietoturva-suunnitelman omavalvonnan kohde **vastaa tietoturvan** ja **asiakastietojen asianmukaisen käsittelyn** varmistamisessa**?**

- **Tietoturvasuunnitelma** on laadittu
- Tietoturvasuunnitelma sisältää suunnitelmalta edellytettävät asiat THL:n määräyksen 3/2024 mukaisesti
- Tietoturvasuunnitelmassa on kuvattu, miten suunnitelmaa säännöllisesti päivitetään, katselmoidaan ja…
- … palvelunantajan henkilökunta ja kaikki ulkoiset kumppanit käytännössä arjessa toimivat suunnitelman mukaisesti ja…
- …miten **tietoturvasuunnitelman toteutumista seurataan**?

KIITOS!

THL:n määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista on julkaistu viranomaisten määräyskokoelmissa (FINLEX ®) ja täällä:

https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset

Tietoturvasuunnitelmasta THL:n Tiedonhallinnan ohjaus -sivulla:

https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/tiedonhallinnan-ohjaus/tietoturvasuunnitelma