[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]

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus

[Tämä THL:n määräykseen 3/2024 (THL/4/4.05.00/2024) kuuluva liite, tietoturvasuunnitelman mallipohja on dokumenttipohja, joka on tarkoitettu tietoturvallisuuden omavalvonnan kohteiden tietoturvasuunnitelman laatimisen tueksi. Mallipohjadokumentin rakenne on informatiivinen, suunnitelman tekemistä helpottava ja ohjaava.]

[Hakasulkeissa ja samalla pienemmällä fontilla (Arial 10) olevat tekstit ovat mallipohjaan liittyviä kommentteja tai ohjeita, jotka voi valmiista tietoturvasuunnitelmasta poistaa tai jättää tarpeen mukaan esimerkiksi alaotsikkoina tms. näkyviin. Ohjeiden välissä on joissain kohdissa valmiita, suunnitelman jäsentämistä helpottavia lauseita suuremmalla fontilla (Arial 11), myös niitä kohtia voi vapaasti muokata tarpeen mukaan.]

[Hakasulkeissa olevissa ohjeissa (alkaen tämän tietoturvasuunnitelman luvusta 3) viitataan aina luvun alussa THL:n määräyksen 3/2024 lukuihin. Viitteenä on lihavoidulla sinisellä '**Määräys 3/2024**:' ja sen jälkeen ko. luvun numero ja nimi.]

Tämä dokumentti on [organisaation nimi]n tietoturvasuunnitelma. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää asiakastietolain[1] 703/2023 77 §:n ja THL:n määräyksen 3/2024 mukaiset velvoitteet. Suunnitelma kokoaa yhteen palvelunantajalta, apteekilta, välittäjältä ja Kansaneläkelaitokselta edellytettävät selvitykset ja vaatimukset.

Tietoturvasuunnitelmaa tulee päivittää säännöllisesti. Tietoturvasuunnitelman laadinnan ja noudattamisen vastuu on sosiaali- ja terveydenhuollon palvelunantajan vastaavalla johtajalla ja apteekkarilla asiakastietolain 78 §:n mukaisesti.

[Tietoturvallisuuden mallipohja on tarkoitettu vapaaehtoisesti hyödynnettäväksi. Tietoturvallisuuden omavalvonnan kohteet voivat laatia tietoturvasuunnitelman tarkoituksenmukaiseksi katsomallaan tavalla, kunhan mallipohjasta ja, tai sen liitteistä käyvät THL:n määräyksessä 3/2024 esitetyt asiat selkeästi ilmi. Tietoturvasuunnitelma on käytännön työväline kokonaisturvallisuuden ylläpitämisessä ja kehittämisessä.]

[Mallipohjasta on määräyksen liitteeksi laadittu ainoastaan tämä yksi versio. Kooltaan ja toiminnaltaan hyvinkin erilaiset sote-palvelunantajat voivat soveltaa tai täydentää mallipohjaa omaan toimintaansa peilaten. Oleellista on täyttää asiakastietolain 703/2023 77 §:n 1 ja 2 momentin vaatimukset.]

[Vanhat tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelmat on päivitettävä voimassa olevan asiakastietolain mukaisiksi tietoturvasuunnitelmiksi. Päivittämisessä on suositeltavaa lähteä liikkeelle kriittisimmistä kohteista tietoturvallisuuden omavalvonnan kohteen omassa toiminnassa tunnistettujen riskien ja tietoturvallisuuden tilan tarkastelun kannalta.]

[Tietoturvasuunnitelman laatimisessa voi hyödyntää esimerkiksi seuraavia lähteitä:

- Kyberturvallisuuskeskuksen kybermittari – Työkalu organisaatioiden kyberturvallisuuden arviointiin ja kehittämiseen: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari
- Valtiovarainministeriön julkaisuja – 2021:65: Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta: https://julkaisut.valtioneuvosto.fi/handle/10024/163596

[1] Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä, https://www.finlex.fi/fi/laki/alkup/2023/20230703#Pidm46494958192992

- Tietosuojavaltuutetun toimisto – Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle
- Kyberturvallisuuskeskus – Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja]
- Digi- ja väestötietovirasto 12/2022 – Digitaalisen turvallisuuden arkkitehtuuri -viitekehys: https://wiki.dvv.fi/display/DTARK/

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat:

[Tietoturvasuunnitelman kappaleessa 2 selvitetään se taho tai ne tahot, tietoturvallisuuden omavalvonnan kohde, jota juuri tämä tietoturvasuunnitelma koskee:

- yhtä tai useampaa palvelunantajaa; tai
- välittäjää tai välittäjiä; tai
- Kelaa.

Vrt. THL:n määräyksen 3/2024:n luvut: 1 Määräyksen soveltamisala, 2 Määritelmät ja 3 Vastuut tietoturvan sekä asiakastietojen asianmukaisen käsittelyn varmistamisessa.]

[Tähän kirjataan tietoturvasuunnitelman kohteena olevan tahon perustiedot]

- Nimi: [palvelunantajan/toimintayksikön nimi]
- Y-tunnus: [Y-tunnus]
- Vastuuhenkilö/johtaja: [palvelunantajan/toimintayksikön johtajan nimi]
- Toimipaikat/palveluyksiköt: [kaikki palveluyksiköt ja/tai toimipaikat, joita suunnitelma koskee]
- Suunnitelman piiriin kuuluvat alihankkijat ja sopimuskumppanit: [tämän suunnitelman piirissä (esim. toimeksianto- tai alihankintasopimuksella) toimivat palvelunantajat, joita tämä suunnitelma koskee]
- …

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

- Suunnitelman ja sen päivittämisen vastuuhenkilö: [nimi]
- Suunnitelman toteuttamisen vastuuhenkilöt: [käytännön tietosuoja- ja tietoturvatoimenpiteiden toteuttamisen vastuuhenkilöt]
- Tarkistus- ja päivityskäytännöt: [kuvaus käytännön toimista ja menetelmistä, joilla suunnitelma otetaan aktiiviseen käyttöön ja kuvaus siitä, kuinka usein suunnitelma tarkastetaan ja tarvittaessa päivitetään säännöllisesti, myös missä tilanteissa suunnitelmaa tarkastetaan ja päivitetään]
- Suunnitelman seuranta ja seurannan dokumentointi: [kuvaus siitä, millä tavalla suunnitelman toteuttamista säännöllisesti seurataan ja kuinka seuranta dokumentoidaan. Mahdollisten tietoturvallisuustyöryhmien tai vastaavien roolit]
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: [kuvaus siitä, kuinka suunnitelmassa kuvatut toimenpiteet huomioidaan hankittaessa tai päivitettäessä tietojärjestelmiä]
- Päätös suunnitelman hyväksymisestä ja käyttöönotosta: [kuka, ketkä/mikä taho ja milloin on päättänyt suunnitelman hyväksymisestä ja käyttöönotosta, kuinka päätetään suunnitelman uusien versioiden hyväksymisestä ja käyttöönotosta]
- …

3. Yleiset tietoturvakäytännöt

[**Määräys 3/2024**: 6.1 Yleiset tietoturvakäytännöt]

[Tähän lukuun kuvataan tietoa yleisistä tietoturvakäytännöistä, politiikoista, tietoturvallisuustyön vastuuttamisesta ja organisoinnista (voi olla kuvattuna politiikoissa), selosteet henkilötietojen käsittelytoimista, sopimuksista, keskeisistä tietoturvallisuusohjeista sekä tietosuojavastaavista]

[Organisaation nimi]:ssa noudatetaan seuraavia yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

Tietoturvallisuustyötä tehdään seuraavien dokumenttien mukaisesti:

[Viittaukset dokumentteihin, joita organisaatiossa käytetään tietosuojan ja tietoturvallisuuden varmistamisessa ja kehittämisessä, esimerkiksi:

- tietoturvapolitiikka, tietosuojapolitiikka, digitaalisen turvallisuuden politiikka tai vastaava asiakirja/asiakirjat
- riskienhallintapolitiikka ja riskienhallintaan liittyvät ylläpito- ja kehittämissuunnitelmat
- selosteet henkilötietojen käsittelytoimista[2]
- lista tietoturvasuunnitelmaan kuuluvista tietojenkäsittelyyn ja tietoturvallisuuteen liittyvistä sopimuskumppaneista alihankkijoineen: käyttöympäristön tukipalvelut, tietojärjestelmäpalvelut ja muut mahdolliset palvelut
- tietojärjestelmäpalvelun tuottajien tietoturvallisuusohjeet
- omat tietoturvallisuusohjeet
- etä- ja hybridityöohjeistukset tietoturvallisuuden osalta
- luettelo muista noudatettavista ohjeista ja kuvauksista
- mahdollinen laatukäsikirja
- …]

Tietosuojavastaavana toimii: [Tähän kirjataan tietosuojavastaavan/tietosuojavastaavien nimet]

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

[**Määräys 3/2024**: 6.2 Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuuden hallinta]

[Tietoturvasuunnitelman laatimisessa voi tässä luvussa tarvittaessa hyödyntää kaikille avoimia eOppivan aineistoja: https://www.eoppiva.fi/koulutukset/turvaa-digitaalinen-toiminta-hairiotilanteissa]

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja:

[Jatkuvuussuunnittelun ja varautumisen järjestäminen, esimerkiksi:

- aihepiiriin kuuluvat erilaiset suunnitelmat (jatkuvuus, toipuminen, varautuminen)
- käytännön harjoittelu, valmiustoiminta, ohjeistukset, ohjeiden saatavuus
- mahdolliset hankinnat liittyen tietojärjestelmähäiriöistä toipumiseen
- normaalista poikkeavat olosuhteet, lyhyt- ja pitkäkestoiset häiriöt, poikkeusolosuhteet
- varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä ja/tai alusta- ja verkkopalveluita
- tietojärjestelmien kriittisyysluokitukset ja niiden mahdolliset vaikutukset varautumisen toteuttamisen käytäntöihin
- …]

[2] Tietosuojavaltuutetun toimisto: Seloste käsittelytoimista

Virhe- ja ongelmatilanteissa sekä niistä toipumisessa noudatetaan seuraavia toimintatapoja:

[Kuvaus siitä, miten menetellään virhe- ja ongelmatilanteiden selvittämisessä ja niistä toipumisessa, vastuut virhe- ja poikkeustilanteissa, tarvittaessa erityyppiset virhe- ja ongelmatilanteet erikseen, esimerkiksi:

- verkko- tai tietoliikenneongelmat (menettelyt ja yhteystiedot verkkopalvelujen tuottajille, mahdolliset tuottajien ohjeet)
- tietojärjestelmien käyttöön liittyvät ongelmat (menettelyt, jos järjestelmä ei toimi, ei käynnisty tai toimii virheellisesti, eri järjestelmätoimittajien yhteystiedot ja tukipalvelut)
- tietojärjestelmien, niiden osajärjestelmien ja komponenttien hallintatoimenpiteet
  - valvonta-, huolto- ja päivitystoimet
  - …
- epäiltyjen, havaittujen tai toteutuneiden tietoturva- tai tietosuojauhkien tai ongelmien hallinta
  - toimenpiteet, jos asiakas- tai potilastietoja tai muita suojattavia tietoja on vuotanut sivullisille
  - toimenpiteet, jos havaintaan virus- tai haittaohjelma
  - toimenpiteet, jos työntekijän tunnukset ovat vuotaneet ulkopuolisille
  - toimenpiteet, jos havaitaan tietojen kalastelua
- toimenpiteet, jos asiakas- tai potilastietoja käsittelevät tietojärjestelmät toimivat selvästi väärin suhteessa niille asetettuihin kansallisiin vaatimuksiin, kuinka asiasta ilmoitetaan tietojärjestelmäpalvelun tuottajalle tai valvontaviranomaisille
  - eli luokan A tai luokan B järjestelmien olennaisten vaatimusten täyttymisessä havaittujen merkittävien poikkeamien ilmoittaminen tietojärjestelmäpalvelun tuottajalle
- toimenpiteet, jos asiakas- tai potilastietoja käsittelevät tietojärjestelmät aiheuttavat riskin asiakas- ja/tai potilasturvallisuudelle
  - eli luokan A tai luokan B järjestelmien merkittävien poikkeamien ilmoittaminen Valviralle, jos poikkeama aiheuttaa merkittävän riskin asiakas- ja/tai potilasturvallisuudelle tai tietoturvalle
  - esimerkiksi tilanteessa, jossa asiakas- ja/tai potilastiedot ja/tai reseptitiedot ovat menneet väärälle asiakkaalle/potilaalle järjestelmävirheen vuoksi
- toimenpiteet tietosuojapoikkeamissa, ilmoittaminen tietosuojavaltuutetulle ja rekisteröidyille
- toimenpiteet toipumisvaiheessa /-vaiheissa sekä jatkokehittämistoimenpiteet saatujen kokemusten pohjalta toiminnan palauduttua normaalitilanteeseen -> jatkuvuudenhallinnan jatkuva kehittäminen
- …]

5. Henkilöstön koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen

5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

[**Määräys 3/2024**: 6.3 Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen]

[Mahdolliset viittaukset erillisiin koulutus- ja/tai osaamisen seurannan suunnitelmiin]

[Miten varmistetaan, että henkilöstölle on annettu koulutus tietojärjestelmien käyttöön, asiakas- ja potilastietojen käsittelyyn sekä tietosuoja- ja tietoturva-asioihin. Lisäksi tulee kuvata, miten seurataan ja ylläpidetään henkilöstön osaamista.]

Asiakas- ja potilastietojen käsittelyn, tietojärjestelmien käytön sekä tietosuojan ja tietoturvan toteuttamisen koulutuksissa, ohjeistuksissa ja seurannassa toimitaan seuraavasti:

[Kuvaus esimerkiksi ainakin siitä,

- miten huolehditaan asiakas- ja potilastietojen käsittelyn toimintamallien/-tapojen koulutuksesta ja perehdytyksestä (esim. asiakkaiden ja potilaiden informointi, tietopyyntöihin vastaaminen, tietojen luovuttaminen jne.)

- miten huolehditaan tietojärjestelmien ja niiden uusien versioiden käyttökoulutuksesta ja perehdytyksestä sekä osaamisen säännöllisestä ylläpidosta erilaisissa työtehtävissä ja rooleissa
- miten tietosuoja- ja tietoturva koulutukset tai kouluttautuminen toteutetaan, tarvittaessa viittaukset erillisiin koulutussuunnitelmiin
- miten koulutusten osaamista seurataan (esim. todistukset tai ylläpidettävät tiedot koulutuksiin osallistumisista arkistoidaan)
- mikä taho kulloinkin vastaa erilaisten koulutusten kustannuksista, tarvittaessa viittaukset asiaa koskeviin sopimuksiin
- …]

5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

[**Määräys 3/2024**: 6.4 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö]

Tietojärjestelmien käyttöohjeiden hallinnassa, saatavuudessa ja ohjeiden mukaisessa käytössä toimitaan seuraavasti:

[Kuvaukset esimerkiksi ainakin siitä,

- miten on varmistettu, että tietojärjestelmän käyttäjällä on saatavilla tarpeelliset käyttöohjeet käyttäjälle ymmärrettävässä (ml. kaikki tarvittavat kieliversiot) muodossa kirjallisesti – ohjeet tarvittaessa sekä organisaatio- että tietojärjestelmäkohtaisesti
- miten ohjeet asiakas- ja potilastietojen käsittelystä on dokumentoitu ja todennettavissa
- miten dokumentoidusti osoitetaan henkilöstön osallistuminen asiakas- ja potilastietojen käsittelyyn järjestettäviin koulutuksiin
- miten on järjestetty henkilöstön tietämyksen ylläpito
- miten käyttöohjeiden päivittäminen ja jakelu toteutetaan ohjelmistojen versiopäivitysten sekä muiden muutosten yhteydessä (toimintamallit)
- kuinka tuetaan (perehdytys, ohjaus, neuvonta) erilaisissa työtehtävissä ja rooleissa toimivia työntekijöitä asiakas- tai potilastietojärjestelmien käyttämisessä
- …]

6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

[**Määräys 3/2024**: 6.5 Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen]

Kuvaukset käytössä olevista tietojärjestelmistä ja siitä, millaisia käytäntöjä asiakastietojen käsittelyn, tietosuojan ja tietoturvallisuuden toteuttamisessa ja seurannassa noudatetaan näitä tietojärjestelmiä käytettäessä:

[Tämän kohdan sisältö on usein tarkoituksenmukaista koota ensimmäisten asioiden joukossa]

[Tarkemmat kuvaukset tietojärjestelmistä **käyttötarkoituksineen**: **Vrt. mallipohjan luku 9**. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat]

[Esimerkiksi viittaus erikseen ylläpidettävään ja ajantasaiseen tietojärjestelmien luetteloon, tietojärjestelmäsalkkuun tai tietojärjestelmäportfolioon, tai luettelo käytettävistä järjestelmistä. Tarvittaessa tehtävissä yhteistyössä tietojärjestelmä- tai ratkaisutoimittajan kanssa]

[Mukaan otetaan ainakin järjestelmät, joilla on vaikutusta sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn, tietoturvaan ja tietosuojaan]

6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3)

[Luettelo, jossa kustakin järjestelmästä järjestelmän perustiedot: nimi, versio (tai vastaava statustieto), toimittaja, yhteystiedot, tiedot tietoturvallisuuden arviointia koskevasta todistuksesta ja sen vastaavuus Valviran tietojärjestelmärekisterin tietoihin]

6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1)

[Luettelo, jossa kustakin järjestelmästä järjestelmän perustiedot: nimi, versio (tai vastaava statustieto), toimittaja, yhteystiedot, tiedot tietoturvallisuuden arviointia koskevasta todistuksesta ja sen vastaavuus Valviran tietojärjestelmärekisterin tietoihin]

6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)

[Luettelo, jossa kustakin järjestelmästä järjestelmän perustiedot; nimi, versio (tai vastaava statustieto), toimittaja, yhteystiedot ja vastaavuus Valviran tietojärjestelmärekisterin tietoihin]

6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta

[Luettelo, jossa kustakin järjestelmästä järjestelmän perustiedot: nimi, versio (tai vastaava statustieto), toimittaja ja yhteystiedot, myös tarvittaessa tiedot sellaisista hyvinvointisovelluksista, jotka liittyvät omaan toimintaan]

6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen

[Kuvattava omavalvonnan kohteen varmistavat toimenpiteet tietojärjestelmien olennaisten vaatimusten täyttymisessä, muun muassa:

- hankinnat, sopimukset ja niiden osana varmistukset siitä, että tietojärjestelmät täyttävät toiminnassa tarvittavien vähimmäisvaatimusten profiilien mukaiset vaatimukset
- käytettävien tai päivitettävien tietojärjestelmien tietojen ja vaatimustenmukaisuuden voimassaolon tarkistaminen Valviran tietojärjestelmärekisteristä
- tietojen ylläpitomenettelyt
- tietojärjestelmien suorituskyvyn varmistaminen erilaisissa tilanteissa tietoturva- ja tietosuojaominaisuuksien vaarantumatta
- …]

6.2. Tietojärjestelmien asennus, ylläpito ja päivitys

[**Määräys 3/2024**: 6.6 Tietojärjestelmien asennus, ylläpito ja päivitys]

Tietojärjestelmien asennuksissa, ylläpidossa ja päivityksissä noudatetaan seuraavia toimintatapoja:

[Järjestelmäkohtaisia erityiskäytäntöjä voidaan kuvata mallipohjan luvuissa 6.1 ja 9, jos käytössä on useita järjestelmiä ja jos ne poikkeavat tässä määritellyistä käytännöistä]

[Kuvataan järjestelmien asennuksen, ylläpidon ja päivityksien roolit, muutoshallinnan, testauksen ja hyväksymisen menettelyt sekä vastuut yleisesti tietoturvallisuuden varmistamistoimenpiteineen ainakin seuraavin kohdin:

- tietojärjestelmän tuotantokäytön kelpoisuuden varmistaminen Valviran tietojärjestelmärekisteristä
- henkilöt ja toimijat, jotka saavat suorittaa järjestelmien asennustoimenpiteitä

- kuinka estetään se, että muut eivät pääse suorittamaan järjestelmien tai ohjelmistojen asennuksia, esimerkiksi edellytetäänkö joissakin tehtävissä tai palveluissa toimivilta henkilöiltä tai palveluntuottajilta tietoturvaselvityksiä tai turvallisuusselvityksiä
- asennus-, ylläpito- ja päivitystoimenpiteitä suorittavilta henkilöiltä vaadittava ammatillinen osaaminen tai asianmukainen koulutus
- mitä palveluita ja mitä sovelluksia on tietojärjestelmissä tai niiden osajärjestelmissä
- kuvattava tietojärjestelmiä asentavien, ylläpitävien ja päivittävien henkilöiden roolit ja vastuut suhteessa tietoturvallisuuden omavalvonnan kohteeseen sekä tietojärjestelmäpalvelun tuottajaan
- kuinka estetään se, ettei tietojärjestelmissä tai laiteohjelmistoissa ole aktiivisia oletustunnuksia tai muita mahdollisesti oletuksena tulevia tietoturvallisuuden kannalta huonoja asetuksia (viittaukset esimerkiksi kovennusohjeisiin)
- kuinka tietojärjestelmät suojataan tyypillisimmiltä tietoturvapuutteilta ja www-sovellusten haavoittuvuuksilta
- toimintatavat, jos käytössä olevaan järjestelmään tehdään päivitys
- mitä on vähintään testattava ja varmistettava ennen kuin järjestelmä tai uusi järjestelmäversio otetaan tuotantokäyttöön
- miten hyväksytään uuden järjestelmän tai järjestelmäversion käyttöönotto, hyväksymisvastuut
- tarvittaessa viittaukset tai mallitekstit sopimuksiin tai muihin dokumentteihin (esim. testauksen ja muutoshallinnan osalta), joissa näitä asioita kuvataan
- tärkeimpien ja kriittisimpien sosiaali- ja terveydenhuollon tietojärjestelmien sekä niiden toiminnassa tarvittavien laitteiden fyysisten ja ohjelmallisten osien sekä niihin liittyvien yksittäisten komponenttien huolto-, uusimis-, ylläpito- ja päivitysmenettelyt
- kriittisimmiksi luokiteltujen sosiaali- ja terveydenhuollon tietojärjestelmien luotettavuudesta huolehtiminen (mm. kahdennukset, tilapäisratkaisut, varaosat ja erityiskomponentit) aktiivisilla valvonta- ja huoltotoimilla]
- …]

6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

[**Määräys 3/2024**: 6.7 Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt]

[Järjestelmäkohtaisia erityiskäytäntöjä voidaan kuvata mallipohjan luvuissa 6.1 ja 9, jos käytössä on useita järjestelmiä ja, jos ne poikkeavat tässä määritellyistä käytännöistä]

[Tarvittaessa viittaukset erillisiin omiin tai ulkoisiin ohjeisiin tai kuvauksiin]

Tietojärjestelmien ja laitteiden käyttäjiä ja käyttäjäryhmiä hallinnoidaan seuraavasti:

[Kuvaukset ainakin seuraavista:

- miten ja missä ylläpidetään ajantasaista luetteloa käyttäjistä ja tarvittaessa käyttäjäryhmistä, jotka käyttävät sosiaalihuollon asiakastieto- ja/tai potilastietojärjestelmiä
- miten ja missä ylläpidetään ajantasaista luetteloa käyttäjistä ja tarvittaessa käyttäjäryhmistä, jotka käyttävät yrityksen laitteita (työasemat, mobiililaitteet, muut laitteet)
- miten ja missä ylläpidetään ajantasaista luetteloa käyttöoikeuksista Kanta-palvelujen käyttöön
- miten ja missä ylläpidetään ajantasaista luetteloa käyttöoikeuksista muihin sähköisiin järjestelmiin
- …]

Käyttöoikeuksien ja käyttövaltuuksien osalta noudatetaan seuraavia toimintatapoja:

[Kuvaukset ainakin seuraavista:

- käyttövaltuuksien hallintaan liittyvät erilaiset roolit ja henkilöt, jotka eri rooleissa toimivat (käyttöoikeuden hakeminen, myöntäminen, muuttaminen, peruminen, poistaminen)
- käyttövaltuuksien hallintamenettelyt (mahdollisesti käytössä olevat IAM-järjestelmät)

- käyttövaltuuksien hakemisen, myöntämisen, seurannan, muuttamisen, tarkistamisen/varmistamisen ja poistamisen käytännöt, esimerkiksi:
    - kuinka uudelle työntekijälle tai sijaiselle (erilaisissa käytännön tilanteissa ja kellonajankohdissa) saadaan tunnukset ja käyttöoikeudet
    - kuinka sijaisten henkilöllisyys varmistetaan ennen käyttöoikeuksien myöntämistä
    - kuinka ja milloin poistuneiden työntekijöiden tunnukset ja käyttöoikeudet poistetaan
    - kenellä/keillä on oikeus hyväksyä käyttöoikeuksia
    - …
- käytännön toiminta kiireellisissä käyttöoikeuksien tai tunnusten poistamistilanteissa
- käyttöoikeuksien hallinnointi Kanta-palvelujen käyttämisessä
- …]

Käyttäjien tunnistautumisessa ja todentamisessa noudatetaan seuraavia käytäntöjä:

[Kuvaukset ainakin seuraavista:

- toimikorttien ja salasanojen sekä muiden kirjautumis- ja tunnistamisvälineiden hallinta (erillinen suunnitelma). Näkökulmina ainakin kulunvalvonta, työasemien ja järjestelmien kirjautumiset, mobiililaitteiden kirjautumis- ja tunnistautumiskäytännöt
- muun vahvan sähköisen tunnistamisen käyttäminen
- käyttäjätunnus- ja salasanatunnistautumisen käyttäminen
- yhteiskäyttöisten tunnusten käyttäminen rajatuissa ja välttämättömissä kohteissa (ei-tunnisteelliset) ja estäminen muissa kohteissa
- monivaiheisen tunnistautumisen (MFA) mahdollinen hyödyntäminen
- pääkäyttäjien ja tietojärjestelmäasiantuntijoiden toiminta ja tunnistautuminen virhetilanneselvityksissä
- tietoteknisten turvakäytäntöjen mahdollinen hyödyntäminen kulunvalvonnassa (liittyy mallipohjan kohtaan 7.1)
- …]

6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

[**Määräys 3/2024**: 6.8 Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt]

[Tarvittaessa viittaukset erillisiin omiin tai ulkoisiin ohjeisiin/kuvauksiin]

Asiakastietoja käsittelevien järjestelmien pääsynhallintaa ja käytön seurantaa toteutetaan seuraavasti:

[Kuvataan tietosuojaan ja asiakastietojen käsittelyn valvontaan liittyvässä seuranta- ja valvontasuunnitelmassa vähintään:

- millaisia pääsynhallinnan tarkistuksia tehdään laitteisiin kirjautumisessa, tietojärjestelmien käynnistämisessä ja mahdollisesti muissa tilanteissa, kuten kulunvalvonnassa

- pääsynhallinnan tekniset käytännöt ei-sallitun käytön estämiseen sosiaalihuollon asiakastietoja tai potilastietoja käsittelevissä tietojärjestelmissä sekä omavalvonnan kohteen omat ohjeet ja toimintatavat oikeisiin toimintatapoihin ja tietojenkäsittelyyn

- luettelot tai vastaavat koonnit tietojärjestelmien tuottamista ja sosiaalihuollon asiakastietojen ja potilastietojen käytön seurantaan koottavista lokeista (mm. lokitiedostot, lokienhallintajärjestelmät, …)

- lokienhallinnan ja käytön seurannan käytännöt valvonnassa ja tietopyyntöihin vastaamisessa
  - keskeiset roolit, kuvattava mm. tietosuojavastaavan, tietohallinnon ja rekisterinpidosta vastaavien roolit asiakastiedon käytön seurannassa
  - käytössä olevat lokienhallintajärjestelmät ja/tai muut raportointimenettelyt
  - asiakkaiden tietopyyntöihin vastaaminen, kuka/ketkä kokoavat lokiraportit ja kuinka usein
  - kuka/ketkä seuraavat lokiraportteja tai lokitietoja ja kuinka usein

- toimintamalli epäiltäessä tai havaittaessa säädösten vastaista sosiaalihuollon asiakastietojen tai potilastietojen käsittelyä
  - kuvaus sisäisen valvonnan toimintatavoista liittyen mahdollisiin epäilyihin rikkomuksista
  - kuvaus siitä kuinka toimitaan, jos lokitiedoista paljastuu virhetilanteita tai epäilyjä rikkomuksista tai epäasianmukaisesta käytöstä

- Kelan lokitietojen saanti ja hankinta seurannan ja valvonnan toteuttamiseksi. Kela voi luovuttaa luovutuslokirekisterin tietoja ko. rekisterin rekisterinpitäjälle ja reseptikeskuksen lokitietoja palvelunantajalle tai apteekille seurannan ja valvonnan toteuttamiseksi
  - kuvaus toimintamallista ja käytännön menettelyistä

- mahdolliset muut seuranta- ja raportointimenettelyt, kuten esim. tietotilinpäätöksen hyödyntäminen rekisterinpitäjän osoitusvelvollisuuden täyttämisessä

- …]

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

[**Määräys 3/2024**: 6.9 Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta]

Fyysisestä turvallisuudesta osana tietoturvallisuuden varmistamista huolehditaan asiakastietojen ja tietojärjestelmien käyttöympäristössä seuraavasti:

[Kuvaukset ainakin seuraavista:

- miten huolehditaan toimitilojen lukitseminen ulkopuolisilta, kulunvalvonnan järjestelyt yms.
- näyttöpäätteiden sijoittuminen ja suojauskäytännöt, jottei sivullisilla ole näköyhteyttä ruuduille, esim. päätteiden sijoittelu, näytönsuojakalvot, käyttämättömän päätteen lukittumisaika ja salasanat
- kuinka ja millaisilla aikarajoilla määritellään istunnon aikakatkaisu tai käyttöliittymän lukittumisen aikaraja järjestelmissä, joissa käyttöliittymän käyttö on estettävä/lukittava
- etä- ja hybridityökäytännöt erilaisissa liikkuvissa potilas- ja asiakastyötehtävissä
- kenellä on oikeus asentaa ohjelmistoja ja sovelluksia organisaation laitteille, kuinka huolehditaan siitä, että vain nämä henkilöt pääsevät tekemään asennuksia
- sallitaanko ulkoisten kovalevyjen ja muistitikkujen käyttö ja mitkä ovat niiden suojauskäytännöt, esim. vain yrityksen itse hankkimat tallennusvälineet, suojaus salasanalla, kuinka estetään se, että ulkopuoliset toimijat eivät voi tuoda muistivälineitä työasemille tai sisäverkkoon (liittyy mm. haittaohjelmilta suojautumiseen)
- tulostimien sijaintipaikat ja, kuinka estetään ulkopuolisten pääsy tulostimille, mahdolliset turvatulostusratkaisut
- arkistotoimeen liittyen sosiaalihuollon asiakastietoja tai potilastietoja sisältävien paperitulosteiden säilyttäminen paloturvallisesti lukittuna ja suojassa sivullisilta sekä niiden hävittäminen siten, etteivät sivulliset pääse tietoihin

- paperitulosteiden hävittämisen käytännön ratkaisut, esim. lukittavat säilytysastiat ja paperisilppurit, tulostajan ja tulosteiden käyttäjän vastuut tulosteiden turvallisuudesta
- tietoteknisten turvakäytäntöjen mahdollinen hyödyntäminen kulunvalvonnassa (liittyy mallipohjan kohtaan 6.4)
- …]

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

[**Määräys 3/2024**: 6.10 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta]

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

[Kuvaukset ainakin seuraavista:

Työasemat ja mobiililaitteet,

- miten virusturvan toimivuus ja päivitykset on käytännössä varmistettu työasemilla
- miten mobiililaitteiden (tabletit ja älypuhelimet, mahdolliset kannettavat työasemat) suojauskäytännöt on järjestetty, esim. käyttäjätunnukset, salasanat, PIN-koodit, SIM-korttien hallinta ja laitteiden virusturvaohjelmat, kadonneiden mobiililaitteiden etälukitseminen ja/tai tyhjentäminen
- …

Käyttöympäristön tukipalvelut,

- kuinka huolehditaan yleisistä käyttöympäristön tukipalveluista: esimerkiksi käyttöjärjestelmän päivitykset ja varusohjelmistojen, kuten esim. MS Office-päivitykset, mahdolliset koventamiset, yhteentoimivuuden varmistaminen ja tilanteen seuranta sote-tietojärjestelmien kanssa
- …

Käyttöympäristön kuvaus liittyen vastuu- ja työnjakokysymyksiin oman ja ulkoistetun toiminnan välillä,

- erilaiset roolit ja toimintakäytännöt käyttöympäristössä
- sopimuskumppanit ja heidän mahdolliset alihankkijansa
- …]

7.3. Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

[**Määräys 3/2024**: 6.11 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta]

Alusta- ja verkkopalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

[Kuvaukset esimerkiksi (jos tällaisia palveluita on omavalvonnan kohteella käytössä) seuraavista:

Yleistä,

- Luettelot käytössä olevista alusta- ja verkkopalveluista sekä niiden hallinnan vastuukysymykset: palvelunantaja, tietojärjestelmäpalvelujen tuottaja(t), kolmannet osapuolet (alihankkijat)
- Tietosuojasäädösten lainmukaisuuden osoittaminen omassa toiminnassa käytettäessä ulkoisten palveluntuottajien alusta- ja verkkopalveluita (esimerkiksi mahdolliset viittaukset sopimuksiin ja tietoturvakäytänteisiin)
- Varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä (vrt. mallipohjan luku 4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta)

Palvelimet ja palvelinympäristöt,

- mitä palveluita ja mitä sovelluksia palvelimilla on ja kuka vastaa niiden asentamisesta ja ylläpidosta
- kuinka ne palvelimet, joilla tietojärjestelmät toimivat suojataan haittaohjelmilta, ja millainen on haittaohjelmien torjunnassa olevien ohjelmien päivityskäytäntö
- kuinka estetään se, ettei palvelinympäristössä ole aktiivisia oletustunnuksia tai muita oletuksena tulevia tietoturvallisuuden kannalta huonoja asetuksia
- kuinka palvelinten tietoturvapäivitysten asentaminen on kuvattu ja järjestetty, miten päivitysten kriittisyys ja tarve arvioidaan, miten päivitykset testataan ja hyväksytään erillisessä testausympäristössä ennen tuotantoympäristöön asentamista
- …

Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet,

- kuinka on sovittu tietoliikenneoperaattoreista ja tietoliikenteen tietoturvaan liittyvistä vastuista, onko sopimuksissa mukana tietoturvallisuus- ja palvelun saatavuusasioita, mukaan lukien yhteydenotot ja menettelyt häiriötilanteissa
- miten käytössä olevien verkkojen tietoturvallisuuskäytänteet on järjestetty (esimerkiksi segmentoinnit, palomuurit, reititykset)
- salasanojen vaatiminen langattomissa verkoissa, salasanojen vaihtamiskäytäntö, yrityksen oman langattoman verkon suojaaminen ulkoisilta käyttäjiltä
- mikäli asiakkaille tarjotaan langaton verkko, sen erottaminen organisaation omasta verkosta
- reitittimien ja muiden verkkolaitteiden päivitysten ja suojausten huolehtimisen vastuut ja näihin mahdollisesti liittyvät sopimukset
- reitittimien, muiden verkkolaitteiden ja niiden komponenttien sekä laite- ja laiteohjelmistojen päivitykset
- …

Etäyhteydet ja niiden tietoturva – tässä voidaan viitata organisaation mahdollisiin etätyöohjeistuksiin, jossa vastaavia tietoturvaan ja tietosuojaan liittyviä asioita on käsitelty,

- mitä palveluja tai järjestelmiä on sallittua käyttää etänä, miten huolehditaan muiden palvelujen etäkäytön estämisestä/kieltämisestä
- mitä tai minkälaisia palveluja Internetin kautta saa ja ei saa käyttää työasemilla
- millaisilla yhteyksillä ja tietoturvaratkaisuilla etänä käytettyjä palveluja voi ja saa käyttää (esim. VPN-yhteydet)
- laitteistojen ja ohjelmistojen huoltoyhteydet -ja käytännöt
- työntekijöille ja muille käyttäjille annettavat etäkäytön ohjeistukset esimerkiksi tietosuojaan ja tietoturvallisuuteen liittyen
- …

Pilvipalvelut, pilvipohjaiset ratkaisut, etähallintapalvelut, palvelinvuokraus, palvelinhallinta, varmistus- ja konesalipalvelut,

- henkilötietojen käsittelyyn liittyvien riskien arviointi (EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi) kaikissa toiminnoissa ja niihin liittyvissä mahdollisissa alihankintaketjuissa

- kuvaukset henkilötietojen kolmansiin maihin siirtojen riskitason arvioinnista niihin liittyvine tarkasteluineen tarvittavista organisatorisista, sopimuspohjaisista ja teknisistä suojatoimista tapaus- ja maakohtaisesti

- kuvaukset kaikista käytössä olevista pilvipalveluista (pilvipalveluiden erilaiset tyypit ja eroavaisuudet) liittyen käytössä oleviin tietojärjestelmiin; myös viittaukset näihin liittyviin sopimuksiin

- sopimusten ajantasaisuus vastaamaan voimassa olevia säädöksiä (mm. EU:n yleinen tietosuoja-asetus, tarvittaessa henkilötietojen siirtämisen perusteet ETA-alueen ulkopuolelle)

- kuvaukset käytössä olevien alusta- ja verkkopalveluiden (mukaan lukien pilvipalvelut) tilanteen jatkuvasta ja säännöllisestä seurannasta muun muassa toimivuuden, tietoturvallisuusriskien, häiriötilanteiden ja palveluiden käyttöehtojen näkökulmasta (sopimusten ja käytäntöjen päivittäminen muuttunutta tilannetta vastaavaksi)

- huolto- päivitys- ja uusimissuunnitelma tietojärjestelmien, osajärjestelmien, laitekomponenttien, verkkojen sekä huolto- ja päivitystoimenpiteiden osalta sekä toimintamalli huoltotoimenpiteisiin liittyvään päätöksentekoon

- varautumisen näkökulma, kun tietoon kohdistuu tarve olla käytettävissä myös normaalista poikkeavissa olosuhteissa; suunnitelmassa on kuvattava muun muassa, kuinka tiedon hallinnointi järjestetään mahdollisessa tilanteessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle.]

[Tarvittaessa voi hyödyntää muun muassa seuraavia lähteitä:

- Tietosuojavaltuutetun toimisto, Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle: https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle

- Pilvipalveluiden turvallisuuden arviointikriteeristöä (PiTuKri): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf]

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

[**Määräys 3/2024**: 6.12 Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt]

[Seuraavat kohdat on mahdollista kuvata myös aiempien lukujen vastaavien kohtien yhteydessä tai järjestelmäkohtaisesti]

Kanta-palvelujen osalta noudatetaan seuraavia tietoturvakäytäntöjä ja asiakastietojen käsittelyn käytäntöjä:

[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:

- kuinka käyttäjät koulutetaan tai perehdytetään tuntemaan Kanta-palvelut ja varmistetaan niiden tietoturvallinen käyttö, esim. perehdytysmateriaali, verkkokoulut/kyselyt jne., ja kuinka varmistetaan, että perehdyttäminen on tehty, henkilöstön ohjeistukset (mm. tietojen lähettäminen viivytyksettä Kanta-palveluihin), asiakkaiden informointi

- toimintamalli Kanta-palvelujen käytön aktiivisesta seurannasta

- Kanta-palvelujen edellyttämien tunnistamis- ja todentamisratkaisujen toteuttaminen: Kanta-palveluja käyttävien järjestelmien kirjautumiskäytännöt

- Sote-organisaatiorekisteritietojen tai IAH-koodiston tietojen tarkastaminen:
    - organisaatio tarkastaa tiedot kansallisen koodistopalvelun Sote-organisaatiorekisteristä
    - itsenäinen ammatinharjoittaja tarkastaa tiedot IAH-koodistosta
    - virheellisten tietojen korjaukset ja lisäykset tehdään aina oman alueen AVI:in tai Valviraan
    - otettava huomioon myös muutostilanteissa tehtävät päivitykset

- Kanta-palvelujen edellyttämien varmenneratkaisujen toteuttaminen (erityyppiset Digi- ja väestötietovirastosta tilattavat henkilöiden toimikortit ja tietoteknisten palvelujen palvelinvarmenteet)

- Kanta-palvelujen edellyttämien käyttöoikeuksien/käyttövaltuuksien hallinta ja kytkentä työntekijöiden työrooleihin – tarvittaessa myös seuraaviin rooleihin liittyvät oikeudet ja tehtävät: pääkäyttäjä(t), arkistonhoitaja(t), tietosuojavastaava(t)

- Kanta-palvelujen ja niihin liittyvien järjestelmien käytön seuranta, mukaan lukien sosiaalihuollon asiakastietojen ja potilastietojen käyttölokin ja luovutuslokin seuranta: kuka/ketkä seuraavat, millä tavoin, kuinka usein

- Kanta-palvelujen pääsynhallinnan toteuttaminen käytetyissä tietojärjestelmissä

- kuinka on toteutettu sosiaalihuollon ja terveydenhuollon dokumenttien ja eri rekisterien erottaminen

- miten ja kuinka usein varmistetaan, että Kanta-palveluihin liittyvillä tietojärjestelmillä (erityisesti A2 tai A3-luokan järjestelmät) ja muilla sertifiointia edellyttävillä tietojärjestelmillä ja välityspalveluilla (luokan A1 järjestelmät) on voimassa oleva todistus tietoturvallisuuden arvioinnista, ja tiedot Valviran tietojärjestelmärekisterissä (A1, A2 tai A3-luokan järjestelmä). Jos palvelunantajan toiminnassa käytetään hyvinvointisovelluksia, vastaavat varmistukset on tehtävä myös niiden osalta

- miten ja kuinka usein varmistetaan luokan A tietojärjestelmien vaatimustenmukaisuuden voimassaolo Valviran tietojärjestelmärekisteriä ja tietojärjestelmäpalvelun tuottajilta saatavia tietoja hyödyntäen (mm. tietoturvallisuustodistuksen voimassaolo, järjestelmään toteutetut olennaisten vaatimusten profiilit ja Kanta-palveluihin liittyneille järjestelmille tehtyjen yhteistestausten vastaavuus Kanta-palveluissa edellytettyihin määrittelyihin). Jos palvelunantajan toiminnassa käytetään hyvinvointisovelluksia, vastaavat varmistukset on tehtävä myös niiden osalta

- miten ja kuinka usein varmistetaan, että muut sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitetut tietojärjestelmät on ilmoitettu Valviralle ja niiden tiedot ovat ajan tasalla Valviran tietojärjestelmärekisterissä (B-luokan järjestelmä)

- kuinka varmistetaan, että hankittava tai päivitettävä järjestelmä täyttää sitä koskevat olennaiset vaatimukset (kuinka asia kuvataan sopimuksissa, mitä tarkistuksia tehdään esim. THL:n määräyksistä, järjestelmäprofiileista ja järjestelmältä vaadittavasta todistuksesta tietoturvallisuuden arvioinnista, Valviran tietojärjestelmärekisteristä ja Kelan yhteistestauksen tuloksista). Jos palvelunantajan toiminnassa käytetään hyvinvointisovelluksia, vastaavat varmistukset on tehtävä myös niiden osalta

- toiminta ja vastuut tilanteessa, jossa käytössä olevalta järjestelmältä peruutetaan todistus tietoturvallisuuden arvioinnista määräajaksi tai kokonaan, jossa todistusta tietoturvallisuuden arvioinnista rajoitetaan tai tilanteessa, jossa tietojärjestelmän käyttö kielletään, kuvaus siitä kuinka asia huomioidaan sopimuksissa. Jos palvelunantajan toiminnassa käytetään hyvinvointisovelluksia, vastaavat varmistukset on tehtävä myös niiden osalta.]

9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat

[**Määräys 3/2024**: 6.5 Tietojärjestelmien perustiedot ja tarkemmat kuvaukset]

[Perustiedot tietojärjestelmistä: Vrt. mallipohjan luku 6.1. Tietojärjestelmien perustiedot]

[Tässä tietoturvasuunnitelman luvussa 9 kuvataan tarvittaessa kaikki tai keskeisimmät tietojärjestelmät tarkemmin, mm. niihin liittyvät ohjeistukset ja suunnitelmat. Jos käytössä on vain yksi tietojärjestelmä, tietojärjestelmäkohtaisia osioita ei välttämättä tarvita. Täältä voidaan myös viitata erikseen ylläpidettäviin järjestelmäkohtaisiin kuvauksiin]

[Seuraavassa kuvattuihin eri kohtiin voidaan soveltuvin osin käyttää samantyyppisiä kuvauksia kuin tietoturvasuunnitelman aiempien lukujen vastaavissa osissa. Seuraavissa pohjissa on yksi esimerkkimalli luokan A2 ja A3 (Kanta-palveluihin liittyvät), luokan A1 (muusta syystä tietoturva-auditoidut tietojärjestelmät), luokan B (muut sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitettu) ja muiden järjestelmien (joita voidaan tarvittaessa ottaa mukaan tietoturvasuunnitelmaan) kuvaamiseen]

[Tietoturvasuunnitelmaan kuvataan tarvittavat alaluvut tietoturvallisuuden omavalvonnan kohteessa käytössä olevien tietojärjestelmien mukaisesti. Mikäli kyseisen alaluvun järjestelmiä ei lainkaan ole, voidaan kyseinen luku kokonaan poistaa. Alaluvuissa olevat symbolit X, Y ja Z kuvaavat mallipohjan alaluvussa mainittuun luokkaan tai luokkiin kuuluvia järjestelmiä X1, X2, …Y1, Y2, … Z1, Z2, …, joista jokaisesta laaditaan omat kuvaukset kyseisessä alaluvussa esitetyn mallin mukaisesti]

9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat)

- järjestelmä, versio, toimittaja, yhteystiedot: [löytyy osin myös Valviran tietojärjestelmärekisteristä, luokka A]
- käyttötarkoitus: [kuvaus löytyy myös Valviran tietojärjestelmärekisteristä, luokka A]
- käyttäjäryhmät:

[Seuraavat kohdat tarvittavin ja soveltuvin osin, mikäli poikkeavat tietoturvasuunnitelman muissa luvuissa kuvatuista käytännöistä]

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:
- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
- käyttövaltuushallinta järjestelmässä:
- tunnistautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen:
- Kantaan liittyvän järjestelmän tietoturvallisuuden arviointia koskevan todistuksen tietojen varmistaminen (luokka A):
- järjestelmän tiedot Kelan testaustulokset sivulla (luokka A):
- järjestelmän tiedot Valviran tietojärjestelmärekisterissä:
    - tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
    - tietojärjestelmän tietoturvallisuustodistuksen voimassaolon päättymispäivä
    - tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
    - tietojärjestelmälle hyväksytysti suoritetut Kelan Kanta-palvelujen yhteistestaukset (Valviran tietojärjestelmärekisteristä ja/tai Kelan testaustulokset sivulta)

    - Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat

9.2. Järjestelmät X (luokkaan A1 kuuluvat)

- järjestelmä, versio, toimittaja, yhteystiedot: [löytyy osin myös Valviran tietojärjestelmärekisteristä, luokka A]
- käyttötarkoitus: [kuvaus löytyy myös Valviran tietojärjestelmärekisteristä, luokka A]
- käyttäjäryhmät:

[Seuraavat kohdat tarvittavin ja soveltuvin osin, mikäli poikkeavat tietoturvasuunnitelman luvuissa 3-5 kuvatuista käytännöistä]

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:
- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
- käyttövaltuushallinta järjestelmässä:
- tunnistautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen:
- Luokkaan A1 kuuluvan järjestelmän tietoturvallisuuden arviointia koskevan todistuksen tietojen varmistaminen:
- järjestelmän tiedot Kelan testaustulokset sivulla (luokka A):
- järjestelmän tiedot Valviran tietojärjestelmärekisterissä:
    - tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
    - tietojärjestelmän tietoturvallisuustodistuksen voimassaolon päättymispäivä
    - tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
    - mahdolliset maininnat järjestelmän osallistumisesta yhteistestaukseen osana laajempaa tietojärjestelmäkokonaisuutta (Valviran tietojärjestelmärekisteristä ja/tai Kelan testaustulokset sivulta)
    - Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat

9.3. Järjestelmät Y (luokkaan B kuuluvat)

- järjestelmä, versio, toimittaja, yhteystiedot: [löytyy osin myös Valviran tietojärjestelmärekisteristä, luokka B]
- käyttötarkoitus: [kuvaus löytyy myös Valviran tietojärjestelmärekisteristä, luokka B]
- käyttäjäryhmät:

[Seuraavat kohdat tarvittavin ja soveltuvin osin, mikäli poikkeavat tietoturvasuunnitelman luvuissa 3-5 kuvatuista käytännöistä]

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:

- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
- käyttövaltuushallinta järjestelmässä:
- tunnistautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen:
- järjestelmän tiedot Valviran tietojärjestelmärekisterissä:
    - tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
    - tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
    - Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat

9.4. Järjestelmät Z (muut järjestelmät, jotka eivät kuulu luokkiin A tai B)

- järjestelmä, versio, toimittaja, yhteystiedot:
- käyttötarkoitus:
- käyttäjäryhmät:

[Seuraavat kohdat tarvittavin ja soveltuvin osin, mikäli poikkeavat tietoturvasuunnitelman luvuissa 3-5 kuvatuista käytännöistä]

- käyttöohjeet:
- ohjeiden päivittäminen ja jakelu:
- menettelyt virhe- ja ongelmatilanteissa:
- järjestelmäkohtaiset tukipalvelut:
- asennus- ja ylläpitovastuut ja -vaatimukset:
- menettelytavat ja vastuut virhe- ja poikkeustilanteissa:
- käyttövaltuushallinta järjestelmässä:
- tunnistautuminen järjestelmässä:
- lokit:
- järjestelmän lukittuminen: