[OMAVALVONTASUUNNITELMAN MALLIPOHJA SOTE-YRITTÄJILLE]

[KORVAA HAKASULUISSA OLEVAT TIEDOT OMAN YRITYKSESI TIEDOILLA TAI POISTA TARVITTAESSA]
[ks. ohje mallipohjan käytölle ennen johdanto-lukua]

[Kirjoita tähän yrityksen / omavalvonnan kohteen nimi]

TIETOSUOJAN JA TIETOTURVALLISUUDEN OMAVALVONTASUUNNITELMA

Päivitetty: [Päiväys ja mahdolliset versiotiedot]
Laatijat: [Laatijat]
Hyväksytty: [Mahdolliset hyväksymismerkinnät, päiväys]

Sisältö

1 Johdanto 3
2 Suunnitelman kohde 4
3 Yleiset tietoturvakäytännöt 5
4 Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt 7
5 Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt 10
6 Kanta-palvelujen käytön tietoturvakäytännöt 12
7 Tietojärjestelmät 14
8 Tietojärjestelmäkohtaiset ohjeet ja suunnitelmat 15

[PÄIVITÄ SISÄLLYSLUETTELO, KUN DOKUMENTTI ON VALMIS]

***[Ohje mallipohjan käytölle:** Poista omasta pohjasta hakasulkeiden teksti ja lisää sinne oman organisaation kannalta kyseiseen kohtaan tulevat tiedot.]*

[Tämä on dokumenttipohja, joka on tarkoitettu omavalvontasuunnitelman tuottamisen tueksi. Tämä mallipohjaversio on suunnattu erityisesti tilanteisiin, jossa omavalvonnan kohteena on pienen yksityisen sosiaali- tai terveydenhuollon palveluntuottajan toiminta. Dokumentin rakenne tai sisällön yksityiskohdat eivät ole sitovia. Dokumenttipohjaan on kuitenkin koottu seikat ja otsikot, joiden kuvaamista edellytetään tietoturvallisuuden ja tiedonhallinnnan omavalvonnan säädöksissä. Varsinaisessa suunnitelmassa on kuvattava kaikki THL:n määräyksen 2/2015 mukaiset seikat, jotka ovat relevantteja omavalvonnan kohteen kannalta. Määräys sisältää tarkempia vaatimuksia ja kuvauksia useisiin dokumenttipohjan kohtiin. Dokumenttipohjan mustat tekstit voivat suoraan toimia pohjana lopulliselle dokumentille. Punaiset tekstit on tarkoitettu muokattavaksi tai poistettavaksi.

Suunnitelman lopullinen rakenne ja sisältö on muodostettava suunnitelman käyttäjille tarkoituksenmukaisesti, ja esimerkiksi ne määräyksen seikat jotka eivät ole sovellettavissa omavalvonnan kohteen toiminnassa voidaan todeta suunnitelman liitteessä. Suunnitelmaan on mahdollista täydentää myös muita kohteen kannalta olennaisia seikkoja.

Suunnitelman sisällön tai siinä viitattujen muiden dokumenttien pohjalta on tarvittaessa pystyttävä todentamaan, että suunnitelma on laadittu, se sisältää suunnitelmalta edellytetyt asiat ja miten suunnitelman toteutumista seurataan.]

1 Johdanto

Sosiaali- ja terveydenhuollon palvelun antajien, apteekkien ja itsenäisten ammatinharjoittajien, Kansaneläkelaitoksen sekä Kanta-välityspalveluiden tuottajien tulee tehdä omavalvontasuunnitelma. (Määräys 2/2015,THL/1305/4.09.00/2014). Suunnitelma tulee olla tietojärjestelmiä käyttävillä sosiaali- ja terveydenhuollon palvelujen antajilla. Suunnitelman avulla ylläpidetään ja kehitetään organisaation tietoturvaa ja tietosuojaa sekä varmistetaan riittävän selkeät vastuut tietosuojaan ja tietoturvaan liittyen. Omavalvontasuunnitelman tarkoituksena on varmistaa, että palvelunantaja ja palvelunantajan henkilökunta

- hallitsee käytössään olevien tietojärjestelmien käytön
- ottaa huomioon asiakas- ja potilastietojen salassapitoon ja tietoturvaan liittyvät vaatimukset
- ymmärtää väärinkäyttöön liittyvät seuraamukset
- [listaa voi haluttaessa myös täydentää itse]

[Omavalvontasuunnitelmassa viitataan aina kuin mahdollista olemassa oleviin erikseen ylläpidettäviin ohjeisiin ja dokumentteihin. Olennaista on, että suunnitelman linkkien tai tietojen avulla on selvää, mistä dokumentaatio on löydettävissä tai vaatimuksen täyttyminen on todennettavissa. Mikäli muuta valmista dokumentaatiota ei ole olemassa tai saatavissa, on mahdollista kuvata vaadittavat asiakokonaisuudet ja toimintatavat suoraan omavalvontasuunnitelmaan.]

[Omavalvontasuunnitelman laadinnan ja noudattamisen vastuu on toimintayksikön vastaavalla johtajalla (sosiaali- ja terveydenhuollon palvelunantajalla)].

2 Suunnitelman kohde

[Aloita suunnitelman tekeminen tai päivittäminen tästä kohdasta!]

Tämän omavalvontasuunnitelman piiriin kuuluvat:
[Kappaleessa selvitetään se taho tai ne tahot, jota tämä omavalvontasuunnitelma koskee. Tähän kirjataan suunnitelman piirissä olevan / olevien yrityksen/yritysten tai yksityisen elinkeinonharjoittajan/-jien tai itsenäisen ammatinharjoittajan 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 palveluntuottajat, 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 päivityskäytäntö: [kuvaus siitä, kuinka usein suunnitelma tarkastetaan ja tarvittaessa päivitetään säännöllisesti, myös missä tilanteissa suunnitelma tarkastetaan ja päivitetään (esim. organisaatiomuutokset)]
- Suunnitelman seuranta ja seurannan dokumentointi: [kuvaus siitä, millä tavalla suunnitelman toteuttamista säännöllisesti seurataan ja kuinka seuranta dokumentoidaan]
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: [kuvaus siitä, kuinka suunnitelmassa kuvatut toimenpiteet huomioidaan hankittaessa tai päivitettäessä tietojärjestelmiä]
- Päätös suunnitelman hyväksymisestä ja käyttöönotosta: [kuka ja milloin on päättänyt suunnitelman hyväksymisestä ja käyttöönotosta, kuinka päätetään suunnitelman uusien versioiden hyväksymisestä ja käyttöönotosta]

3 Yleiset tietoturvakäytännöt

Yrityksessä noudatetaan seuraavia yleisiä tietoturvakäytäntöjä:
[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:]

Tietosuojavastaavana toimii: *[Tähän kirjataan: tietosuojavastaavan nimi[1]]*

Tietojärjestelmien käyttöä sekä tietosuojan ja tietoturvallisuuden toteuttamista tehdään seuraavien dokumenttien mukaisesti:
[Viittaukset muihin dokumentteihin, joita käytetään tietosuojan ja tietoturvallisuuden toteuttamisessa esim.:

- *seloste henkilötietojen käsittelystä[2]*
- *mahdollinen laatukäsikirja*
- *tietojärjestelmäpalvelujen tuottajien ohjeet*
- *omat tietoturvallisuusohjeet*
- *tietoturvapolitiikka, mikäli sellainen on laadittu*
- *sopimukset, joissa määritellään suunnitelman piiriin liittyviä asioitaluettelo muista noudatettavista ohjeista ja kuvauksista]*

Tietojen käsittelyssä sekä tietosuojan ja tietoturvallisuuden toteuttamisessa seurataan ja noudatetaan seuraavia viranomaisten ohjeita ja määräyksiä:
[Luettelo käytettävistä ja noudatettavista omavalvontaan, käyttövaltuuksiin ja käytön seurantaan ym. liittyvistä ohjeista kuten THL:n asiaan liittyvät ohjeet ja määräykset[3]. Kuvaus siitä, kuinka usein ohjeet ja määräykset tarkistetaan ja kuinka uudet ohjeet otetaan käyttöön ja tarvittaessa koulutetaan tai perehdytetään.]

Koulutus, ohjeistus ja käyttökokemus ja niiden seuranta

Asiakastietojen käsittelyn, tietojärjestelmien käytön sekä tietosuojan ja tietoturvallisuuden toteuttamisen koulutuksissa, ohjeistuksissa ja seurannassa toimitaan seuraavasti:
[Kuvaus siitä:

- *miten tietosuojan ja tietoturvallisuuden koulutus tai kouluttautuminen toteutetaan ja tarvittaessa viittaus erilliseen koulutussuunnitelmaan*
- *kuvaus siitä, miten huolehditaan asiakas- ja potilastietojen käsittelyn toimintamallien/-tapojen koulutuksesta ja perehdytyksestä (esim. asiakkaiden informointi, tietopyyntöihin vastaaminen jne.)*
- *kuvaus siitä, miten huolehditaan tietojärjestelmien ja niiden uusien versioiden käyttökoulutuksesta ja perehdytyksestä*

---

[1] Mikäli tietosuojavastaava on nimetty. Tietosuojatyöryhmän tietosuojavastaavia koskeva ohje WP243, kohta 2.1.3.

[2] Tietosuojavaltuutetun toimisto: Seloste käsittelytoimista

[3] https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset
https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/ohjeet-ja-soveltaminen/ohjeet

- *kuvaus siitä, miten koulutusten osaamista seurataan (esim. todistukset tai ylläpidettävät tiedot koulutuksiin osallistumisista arkistoidaan)*
- *tarvittaessa kuvaus siitä, kuka vastaa koulutusten kustannuksista, tarvittaessa viittaus asiaa koskevaan sopimukseen*
- *tarvittaessa kuvaus siitä, kuinka seurataan ja kuvataan sitä, kuinka pitkä ja millainen kokemus työntekijöillä on käytössä olevien asiakas- tai potilastietojärjestelmien käytöstä ja kuinka tuetaan (perehdytys, ohjaus) niitä työntekijöitä joilla ei ole paljon kokemusta käytöstä]*

4 Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt

[Kuvaus siitä, mistä löytyvät seuraavat tiedot, tai sisältö kirjoitetaan osaksi tätä suunnitelmaa:]

Menettelyt virhe- ja ongelmatilanteissa

Virhe- ja ongelmatilanteissa noudatetaan seuraavia toimintatapoja:
[Kuvaus siitä, miten menetellään virhe- ja ongelmatilanteiden selvittämisessä, vastuut virhe- ja poikkeustilanteissa, tarvittaessa erilaiset virhe- ja ongelmatilanteet erikseen:

- *verkko- tai tietoliikenneongelmat (menettelyt ja yhteystiedot verkkopalvelujen tuottajille, mahdolliset tuottajien ohjeet)*
- *järjestelmien käyttöön liittyvät ongelmat (menettelyt, jos järjestelmä ei toimi, ei käynnisty tai toimii virheellisesti, eri järjestelmäntoimittajien yhteystiedot ja tukipalvelut)*
- *havaittujen tai toteutuneiden tietoturva- tai tietosuojauhkien tai ongelmien hallinta*
    - *toimenpiteet, jos asiakastietoja 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 tietojärjestelmän valmistajalle*
    - *eli luokan A tai luokan B järjestelmien olennaisten vaatimusten täyttymisessä havaittujen merkittävien poikkeamien ilmoittaminen tietojärjestelmän valmistajalle*
- *toimenpiteet, jos asiakas- tai potilastietoja käsittelevät tietojärjestelmä aiheuttavat riskin potilasturvallisuudelle*
    - *eli luokan A tai luokan B järjestelmien merkittävien poikkeamien ilmoittaminen Valviralle, jos poikkeama aiheuttaa merkittävän riskin potilasturvallisuudelle*
    - *esimerkiksi tilanteessa, jossa potilas- ja/tai asiakastiedot ja/tai reseptitiedot ovat menneet väärälle asiakkaalle/potilaalle järjestelmävirheen vuoksi]*

Järjestelmien käyttöohjeiden hallinnointi ja saatavuus

Järjestelmien käyttöohjeiden hallinnoinnissa ja hyödyntämisessä toimitaan seuraavasti:
[Kuvataan seuraavat asiat ja kenen vastuulla asia on:

- *missä tietojärjestelmän käyttöohjeet ovat, kuka huolehtii asiasta*
- *miten tarvitsija saa tietojärjestelmän / järjestelmien käyttöohjeet, mistä löytyy*
- *miten tietojärjestelmän toimittajalta / tietojärjestelmäpalvelun tuottajalta saadaan tai hankitaan ajantasaiset ja riittävät käyttöohjeet*
    - *myös miten käyttöohjeiden päivittäminen ja jakelu toteutetaan ohjelmistojen ja niiden versiopäivitysten sekä muiden muutosten yhteydessä*
- *kuinka, milloin ja kenen toimesta käyttöohjeita päivitetään, myös jos tehdään omia täydentäviä ohjeita*

- *miten henkilöstön perehdytys tietojärjestelmän käyttöön toteutetaan ja seuranta on järjestetty (voidaan viitata perehdytysohjelmaan)*
- *miten varmistetaan, että tietojärjestelmiä käytetään valmistajan antamien ohjeistusten mukaisesti tai niitä tarkoituksenmukaisesti soveltaen tai täydentäen*
- *miten edellä kuvatut kohdat dokumentoidaan, esim. jos on poikkeamia / puutteita ohjeiden saatavuudessa tai ohjeiden mukaisessa käytössä.]*

Järjestelmien asennus ja ylläpito yleisesti

Järjestelmien asennuksessa ja ylläpidossa noudatetaan yleisesti seuraavia toimintatapoja:
[Järjestelmäkohtaisille seikoille on paikka luvussa 8, jos käytössä on useita järjestelmiä ja jos ne poikkeavat tässä määritellyistä käytännöistä]

[Kuvataan seuraavat asiat:

- *henkilöt ja toimijat, jotka saavat suorittaa järjestelmien asennustoimenpiteitä*
- *kuinka estetään se, että muut eivät pääse suorittamaan järjestelmien tai ohjelmistojen asennuksia*
- *asennus- ja päivitystoimenpiteitä suorittavilta vaadittava osaaminen tai koulutus*
- *toimintatavat, jos käytössä olevaan järjestelmään tehdään päivitys*
- *kuvaus siitä, mitä vähintään on testattava ja varmistettava ennen kuin järjestelmä tai uusi järjestelmäversio otetaan tuotantokäyttöön*
- *miten hyväksytään uuden järjestelmän tai järjestelmäversion käyttöönotto*
- *tarvittaessa viittaukset sopimuksiin tai muihin dokumentteihin, joissa näitä asioita kuvataan]*

Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus

Tilojen, työasemien, tallennusvälineiden ja tulosteiden tietoturvallisuudesta huolehditaan seuraavasti:
[Kuvaukset,

a) *miten huolehditaan toimitilojen lukitseminen ulkopuolisilta ja esim. kulunvalvonta, jos se on käytössä*
b) *näyttöpäätteiden sijoittuminen ja suojauskäytännöt, jotta sivullisilla ei ole näköyhteyttä esim. päätteiden sijoittelu, näytönsuojakalvot, käyttämättömän päätteen lukittumisaika ja salasanat*
c) *miten virusturvan toimivuus ja päivitykset on varmistettu*
d) *miten verkon palomuurin toimivuus on järjestettty*
e) *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*
f) *kenellä on oikeus asentaa ohjelmistoja ja sovelluksia yrityksen laitteille, kuinka huolehditaan siitä että vain nämä henkilöt pääsevät tekemään asennuksia*
g) *tulostimien sijaintipaikat ja kuinka estetään ulkopuolisten pääsy tulostimille*
h) *asiakas- tai potilastietoja sisältävien paperitulosteiden säilyttäminen paloturvallisesti lukittuna ja suojassa sivullisilta sekä niiden hävittäminen siten, että sivulliset eivät pääse tietoihin*

i) *sallitaanko ulkoisten kovalevyjen ja muistitikkujen käyttö ja mitkä ovat niiden suojauskäytännöt esim. vain yrityksen itse hankkimat välineet, suojaus salasanalla, kuinka estetään se että ulkopuoliset toimijat eivät voi tuoda muistivälineitä työasemille tai sisäverkkoon (mm. haittaohjelmilta suojautuminen)*

Muut käyttöympäristön käytännöt.

Muita tietojen hallintaan ja tietoturvallisuuden toteuttamiseen liittyviä käytäntöjä ovat:
[Kuinka huolehditaan yleisistä käyttöympäristön tukipalveluista: esimerkiksi käyttöjärjestelmän päivitykset, varusohjelmistojen kuten Office päivitykset]

[Kuinka on sovittu tietoliikenneoperaattoreista ja tietoliikenteen tietoturvaan liittyvistä vastuista, onko sopimuksissa mukana tietoturvallisuus- ja palvelun saatavuusasioita, mukaan lukien yhteydenotot ja menettelyt häiriötilanteissa]

[Etäyhteydet ja niiden tietoturva:
- *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 etänä käytettyjä palveluja voi ja saa käyttää (esim. VPN-yhteydet)]*

[Verkkolaitteet, langattomat verkot ja reitittimet ja niiden tietoturva:
- *salasanojen vaatiminen langattomissa verkoissa, salasanojen vaihtamiskäytäntö, yrityksen oman langattoman verkon suojaaminen ulkoisilta käyttäjiltä*
- *mikäli asiakkaille tarjotaan langaton verkko, sen erottaminen yrityksen omasta verkosta*
- *reitittimien ja muiden verkkolaitteiden päivitysten ja suojausten huolehtimisen vastuut ja näihin mahdollisesti liittyvät sopimukset*
- *reitittimien ja muiden verkkolaitteiden laite- ja laiteohjelmistojen päivitykset]*

5 Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt

[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:]

[Järjestelmäkohtaiset seikat ovat luvussa 8, jos ne poikkeavat tässä määritellyistä käytännöistä]

Käyttäjät ja käyttäjäryhmät

Tietojärjestelmien ja laitteiden käyttäjiä ja käyttäjäryhmiä hallinnoidaan seuraavasti:
[Kuvataan, mistä löytyy

- *ajantasainen luettelo käyttäjistä ja tarvittaessa käyttäjäryhmistä, jotka käyttävät asiakas- ja/tai potilastietojärjestelmiä*
- *ajantasainen luettelo käyttäjistä ja tarvittaessa käyttäjäryhmistä, jotka käyttävät yrityksen laitteita (työasemat, mobiililaitteet, muut laitteet)*
- *ajantasainen luettelo käyttöoikeuksista Kanta-palvelujen käyttöön*
- *ajantasainen luettelo käyttöoikeuksista muihin sähköisiin järjestelmiin]*

Käyttövaltuushallinnan ja käytön seurannan käytännöt

Käyttöoikeuksien, käyttövaltuuksien ja käytön seurannan osalta noudatetaan seuraavia toimintatapoja:

[Käyttövaltuuksien hakemisen, myöntämisen, seurannan, muuttamisen, tarkistamisen / varmistamisen ja poistamisen käytännöt, esimerkiksi kuinka uudelle työntekijälle tai sijaiselle saadaan tunnukset ja käyttöoikeudet, kuinka sijaisten henkilöllisyys varmistetaan ennen käyttöoikeuksien myöntämistä, kuinka ja milloin poistuneiden työntekijöiden tunnukset ja käyttöoikeudet poistetaan]

[Käyttäjien tunnistamisen ja todentamisen käytännöt: toimikorttien ja salasanojen sekä muiden kirjautumis- ja tunnistamisvälineiden hallinnan suunnitelma; näkökulmina ainakin kulunvalvonta, työasemien ja järjestelmien kirjautumiset, mobiililaitteiden kirjautumis- ja tunnistautumiskäytännöt]

[Luettelo järjestelmien ja asiakastietojen käytön seurantaan koottavista lokeista (lokitiedostot, lokijärjestelmät). Lokien hallinnan ja käytön seurannan käytännöt esimerkiksi asiakkaiden tietopyyntöihin vastaaminen, kuka kokoaa lokiraportit ja kuinka usein, kuka seuraa lokiraportteja tai lokitietoja ja kuinka usein, kuvaus siitä kuinka toimitaan jos lokitiedoista paljastuu virhetilanteita tai epäilyjä rikkomuksista tai epäasianmukaisesta käytöstä. Ks. myös luku 6 / Kanta-luovutusloki ja käyttöloki.]

[Kelan lokitietojen saanti ja hankinta seurannan ja valvonnan toteuttamiseksi. Kela voi luovuttaa luovutuslokirekisterin tietoja ko. rekisterin rekisterinpitäjälle.]

[Toimintamalli epäiltäessä tai havaittaessa säädösten vastaista asiakas- tai potilastietojen käsittelyä].

[Tarvittaessa viittaukset erillisiin omiin tai ulkoisiin ohjeisiin / kuvauksiin]

6 Kanta-palvelujen käytön tietoturvakäytännöt

[Ajantasaiset kuvaukset seuraavista tai viittaukset ajantasaisiin kuvauksiin:]

[Nämä seikat on mahdollista kuvata myös aiempien lukujen vastaavien kohtien yhteydessä (luvut 3-5) tai järjestelmäkohtaisesti (luku 8)]

[Kuvaus siitä kuinka käyttäjät koulutetaan tai perehdytetään tuntemaan Kanta-palvelut ja niiden tietoturvallinen käyttö, esim. perehdytysmateriaali, verkkokoulut/kyselyt jne. ja kuinka varmistetaan, että perehdyttäminen on suoritettu]
[Kanta-palvelujen edellyttämien tunnistamis- ja todentamisratkaisujen: Kanta-palveluja käyttävien järjestelmien kirjautumiskäytännöt,

[Sote-organisaatiorekisteritietojen tai IAH-koodiston tietojen tarkistaminen: yksityisten palvelunantajien lupatiedot välitetään koodistopalveluun Valveri-rekisteristä (yksityisten sosiaali- ja terveydenhuollon palvelunantajien rekisteri). Organisaatio tarkistaa tiedot koodistopalvelun SOTE-organisaatiorekisteristä. Itsenäinen ammatinharjoittaja tarkistaa tiedot IAH-koodistosta. Virheellisten tietojen korjaukset ja lisäykset tehdään aina oman alueen AVI:in tai Valviraan. Huomioitava myös muutostilanteissa tehtävät päivitykset.]

[Kanta-palveluiden edellyttämien varmenneratkaisujen toteuttaminen (eri tyyppiset VRK:lta tilattavat henkilöiden toimikortit ja tietoteknisten palvelujen palvelinvarmenteet)]

[Kanta-palveluiden edellyttämien käyttöoikeuksien / käyttövaltuuksien hallinta ja kytkentä työntekijöiden työrooleihin – tarvittaessa myös pääkäyttäjä, arkistonhoitaja, tietosuojavastaava tehtäviin liittyvät oikeudet ja tehtävät]

[Kanta-palveluiden ja niihin liittyvien järjestelmien käytön seuranta, mukaan lukien asiakastietojen käyttölokin ja luovutuslokin seuranta: kuka seuraa, millä tavoin, kuinka usein. Ks myös luku 5 / Luettelo järjestelmien ja asiakastietojen käytön seurantaan koottavista lokeista].

[Kanta-palveluiden pääsynhallinnan toteuttaminen käytetyissä tietojärjestelmissä]

[Kuvaus siitä, kuinka on toteutettu sosiaalihuollon ja terveydenhuollon dokumenttien ja eri rekisterien erottaminen]

[Kuvaus siitä, miten ja kuinka usein varmistetaan että Kanta-palveluihin liittyvillä tietojärjestelmillä ja välityspalveluilla on voimassa oleva vaatimustenmukaisuustodistus, ja tiedot Valviran Tietojärjestelmät-rekisterissä (A-luokan järjestelmä)]

[Kuvaus siitä, miten ja kuinka usein varmistetaan että muut asiakas- tai potilastietojen käsittelyyn tarkoitetut tietojärjestelmät on ilmoitettu Valviralle ja niiden tiedot ovat ajan tasalla Valviran Tietojärjestelmät-rekisterissä (B-luokan järjestelmä)]

[Kuvaus siitä, kuinka varmistetaan, että hankittava tai päivitettävä järjestelmä täyttää sitä koskevat olennaiset viranomaisvaatimukset (kuinka asia kuvataan sopimuksissa, mitä tarkistuksia tehdään esim. THL:n määräyksistä, järjestelmäprofiileista ja järjestelmältä vaadit-

tavasta vaatimustenmukaisuustodistuksesta, Valviran Tietojärjestelmät-rekisteristä ja Kelan Yhteistestauksen tuloksista)]

[Toiminta ja vastuut tilanteessa, jossa käytössä olevalta järjestelmältä peruutetaan vaatimustenmukaisuustodistus määräajaksi tai kokonaan jossa vaatimustenmukaisuustodistusta rajoitetaan, tai tilanteessa jossa tietojärjestelmän käyttö kielletään, kuvaus siitä kuinka asia huomioidaan sopimuksissa]

7 Tietojärjestelmät

[Tämän kohdan sisältö on usein järkevää koota ensimmäisten asioiden joukossa.]

[Esimerkiksi viittaus 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 asiakas- tai potilastietojen käsittelyyn, tietoturvaan ja tietosuojaan]

Kanta-palveluihin liittyvät tietojärjestelmät (luokka A)
[luettelo, jossa kustakin järjestelmästä järjestelmän nimi, versio, toimittaja, yhteystiedot, tiedot vaatimustenmukaisuustodistuksesta ja sen vastaavuus Valviran tietojärjestelmärekisterin tietoihin, tarvittaessa muita tietoja]

Muut asiakas- tai potilastietoja käsittelevät järjestelmät (luokka B)
[luettelo, jossa kustakin järjestelmästä järjestelmän nimi, versio, toimittaja, yhteystiedot, vastaavuus Valviran tietojärjestelmärekisterin tietoihin, tarvittaessa muita tietoja]

Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakas- ja potilastietojen suojaamisen kannalta
[luettelo, jossa kustakin järjestelmästä järjestelmän nimi, versio, toimittaja, yhteystiedot, tarvittaessa muita tietoja]

[Lisäksi tarvittaessa keskeisimmistä tai kaikista järjestelmistä lukujen 3-6 mukaisia tietoja lukuun 8, jos niissä on järjestelmäkohtaisia eroja]

8 Tietojärjestelmäkohtaiset ohjeet ja suunnitelmat

[Viittaukset järjestelmäkohtaisiin kuvauksiin tai tässä luvussa kuvattuja järjestelmäkohtaisia osioita. Soveltuvin osin eri kohtiin voidaan käyttää samantyyppisiä kuvauksia kuin aiempien lukujen vastaavissa osissa. Alla olevissa pohjissa on malli luokan A (Kantapalveluihin liittyvät), luokan B (muut asiakas- tai potilastietojen käsittelyyn tarkoitettu) ja muiden järjestelmien (joita voidaan tarvittaessa ottaa mukaan omavalvontasuunnitelmaan) kuvaamiseen.]

[8.1 Järjestelmä X (luokkaan A kuuluva)]

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

[tarvittavin ja soveltuvin osin, mikäli poikkeavat luvuissa 3-6 kuvatuista yleisistä 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 vaatimustenmukaisuustodistuksen tietojen varmistaminen (luokka A):
-järjestelmän tiedot Kelan testaustulokset sivulla (luokka A):
-järjestelmän tiedot Valviran rekisterissä (luokka A ja B):

[8.2 Järjestelmä Y (luokkaan B kuuluva)]

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

[tarvittavin ja soveltuvin osin, mikäli poikkeavat luvuissa 3-6 kuvatuista yleisistä 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 rekisterissä:

[8.3 Järjestelmä Z (muu järjestelmä)]

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

[tarvittavin ja soveltuvin osin, mikäli poikkeavat luvuissa 3-6 kuvatuista yleisistä 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