

Psykoterapia ja psykologipalvelut Noora Laine

Tietoturvasuunnitelma

29.11.2025, ensimmäinen versio

Laatinut Noora Laine

Sisältö

1 Johdanto	3
2 Suunnitelman kohde ja päivityskäytännöt	3
3 Yleiset tietoturvakäytännöt	4
Koulutus, ohjeistus ja käyttökokemus ja niiden seuranta	4
Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt	5
4 Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt	6
5 Kanta-palvelujen käytön tietoturvakäytännöt	7
6 Tietojärjestelmät	7
7 Tietojärjestelmäkohtaiset ohjeet ja suunnitelmat	7
7.1 Atostek eRA (luokkaan A3 kuuluva)	7
7.2 Järjestelmä MinduuPro (luokkaan A1 kuuluva)	7
7.3 Mahdolliset muut järjestelmät	7
8 Liitteet:	8

1 Johdanto

Tämä dokumentti on yrityksen Psykoterapia ja psykologipalvelut Noora Laineen tietoturvasuunnitelma. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää uuden asiakastietolain 784/2021 27 §:n ja THL:n määräysten mukaiset velvoitteet. Suunnitelma kokoaa yhteen asiakastietolaissa vaaditut omavalvonnan kohteelta edellytettävät selvitykset ja vaatimukset.

2 Suunnitelman kohde ja päivityskäytännöt

Psykoterapia ja psykologipalvelut Noora Laine / Noora Laine

Y-tunnus: 3372706-2

Toimipaikan osoite: Kotolankatu 2 C 3, 26100 Rauma

Aluehallintoviraston toimiluvan myöntämispäivä / Itsenäisen ammatinharjoittajan aloittamisilmoittamisilmoituksen päivämäärä: 1.9.2023

Ammatinharjoittaja (nimi ilmoitettu kohdassa 2) on vastuussa tietoturvasuunnitelman päivittämisestä ja päivittää suunnitelman aina tarvittaessa. Ammatinharjoittaja vastaa myös tiedon siirtämisestä käytäntöön ja suunnitelman toteutumisen seurannasta. Ammatinharjoittaja toimii tietosuojavastaavana ja arkistonhoitajana.

Tämän omavalvontasuunnitelman piiriin kuuluvat seuraavat järjestelmät:

- Atostekin tekemä eRA-järjestelmä, minkä kautta käytetään Kanta-palveluita konesalista tarjottavana pilvipalveluna.
- MinduuPro asiakashallintaohjelmisto sekä käyttöliittymä Atostekin eRA-järjestelmään, joka tarjotaan pilvipalveluna

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

- Suunnitelman ja sen päivittämisen vastuuhenkilö: Noora Laine
- Suunnitelman toteuttamisen vastuuhenkilöt: Noora Laine
- Tarkistus- ja päivityskäytännöt: Yrityksen ammatinharjoittaja on vastuussa suunnitelman ajantasaisuudesta. Suunnitelma päivitetään tarpeen mukaan. Tämän lisäksi suunnitelmaa tarkastellaan ja päivitetään aina uusia tietojärjestelmiä tai laitteita hankittaessa sekä esimerkiksi muutettaessa toiseen toimipisteeseen

- Suunnitelman seuranta ja seurannan dokumentointi: Tietoturvasuunnitelman ylläpitämisestä vastaa yrityksen ammatinharjoittaja. Tietoturvasuunnitelman viimeisin päivitys merkitään suunnitelman ensimmäiselle sivulle. Suunnitelmaan tehdyistä muutoksista ei pidetä erillistä muutoslokia, mutta suunnitelman vanhat versiot tallennetaan erilliseen kansioon.
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: Hankittaessa käyttöön uusia tietosuojaan vaikuttavia järjestelmiä (kuten pilvipalveluita, potilastietojärjestelmiä, asiakashallintajärjestelmiä tai asiakirjojen hallintajärjestelmiä) selvitetään tämän suunnitelman käytännön toteuttaminen uusissa tietojärjestelmissä. Tarvittaessa suunnitelmaa täydennetään tai muutetaan yhteensopivaksi uusien tietojärjestelmien kanssa siten, että tietosuoja- ja tietoturvavaatimukset täyttyvät.

3 Yleiset tietoturvakäytännöt

eRA-tietojärjestelmän ja MinduuPron tietoturvakäytännöistä on kuvaus MinduuPro ja eRA-järjestelmien omavalvontasuunnitelmaliitteessä (liitteet 1 ja 2).

Ammatinharjoittaja on vastuussa yrityksen tietoturvasta ja vastaa tietoturvan organisoinnista, seurannasta ja valvonnasta. Ammatinharjoittaja toimii käytettävien tietojärjestelmien pääkäyttäjänä.

Yrityksessä psykoterapia ja psykologipalvelut Noora Laine noudatetaan yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

- <https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pienyritysten-kyberturvallisuusopas>
- kts. erillinen omavalvontasuunnitelma
- kts. erillinen potilas-, laskutus- ja asiakasrekisteriseloste sekä tietosuojaseloste

Koulutus, ohjeistus ja käyttökokemus ja niiden seuranta

Toimintamallien koulutus ja perehdytys

MinduuPro ja eRA-tietojärjestelmän käyttäjien koulutus on kuvattu liitteissä (liitteet 1 ja 2).

Tietojärjestelmien käyttökoulutus

MinduuPro ja eRA-tietojärjestelmän käyttäjien koulutus on kuvattu liitteissä (liitteet 1 ja 2).

Riittävä kokemus

MinduuPro ja eRA-tietojärjestelmän käyttäjien koulutus on kuvattu liitteissä (liitteet 1 ja 2).

Ohjeet ja koulutus potilastietojen käsittelystä

MinduuPro ja eRA-tietojärjestelmän käyttäjien koulutus on kuvattu liitteissä (liitteet 1 ja 2).

Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt**Menettelyt virhe- ja ongelmatilanteissa**

Kun ammatinharjoittaja havaitsee ongelman, hän ilmoittaa siitä järjestelmän tukipalveluihin. MinduuPro ja eRA-tietojärjestelmän käytön osalta virhe- ja ongelmatilanteiden selvitys on kuvattu liitteissä 1 ja 2.

Mikäli esim. järjestelmävirian vuoksi pääsy sähköiseen tietojärjestelmään estyy, siirrytään tarvittaessa väliaikaisesti paperiarkistoon. Paperisten potilasasiakirjojen väliaikainen säilytys toteutetaan lainsäädännön vaatimalla tavalla ja tiedot siirretään mahdollisimman pian sähköiseen järjestelmään ja paperiasiakirjat tuhotaan asianmukaisesti.

Järjestelmien käyttöohjeiden hallinnointi ja saatavuus

MinduuPro ja eRA-tietojärjestelmän käyttöohjeiden hallinnointi ja jakelu on kuvattu liitteissä (liitteet 1 ja 2).

Järjestelmien asennus ja ylläpito yleisesti

MinduuPro ja eRA-tietojärjestelmän osalta järjestelmien muutoshallinta on kuvattu liitteissä (liitteet 1 ja 2).

Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus

Toiminnan fyysiset tilat ovat lukolliset. Potilastietoja käsitellään siten, että tietoja sisältävä näyttö ei ole suojaamattomana kohti oviaukkoja tai muita henkilöitä. Käytettävät tietokoneet ja mobiililaitteet on suojattu salasanalla ja mobiilipuhelimien kohdalla puhelimen avauskoodilla tai sormenjälkitunnistuksella sekä sim-koodilla. Laitteet lukittuvat määrääjän kuluttua jos laite on käyttämättömänä. Jos tietoja käsitellään Windows- tai Android -laitteilla, niihin on asennettu virustorjuntaohjelma, joka päivitetään säännöllisesti. Vain yrityksen pääkäyttäjällä eli ammatinharjoittajalla on oikeus asentaa oheisohjelmia käytettäville laitteille.

Mahdolliset paperiset potilasasiakirjat ja potilastietoja sisältävät paperitulosteet on sijoitettu paloturvallisesti lukittuna kahden lukon taakse. Potilastietoja sisältävien asiakirjojen tulostus tapahtuu aina siten, ettei ulkopuolisilla ole pääsyä tulosteiden luo. Mikäli potilastietoja sisältävää materiaalia on tarpeen siirtää ulkoiselle kovalevylle tai muistitikulle, nämä ovat salasanalla suojattuja.

Muut käyttöympäristön käytännöt.

MinduuPro ja eRA-tietojärjestelmän tietoliikenteen vastuualueet on liitteissä (liitteet 1 ja 2).

Järjestelmää käytetään salasanalla suojatuissa langattomissa verkoissa, johon ei ole pääsyä asiattomilla henkilöillä. Jos mobiiliyhteydessä, verkkoyhteydessä tai reitittimen toiminnassa ilmenee ongelmia, pyydetään tukea verkkoyhteyden tarjoajalta tai reitittimen myyneeltä toimijalta.

4 Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt

Käyttövaltuushallinnan ja käytön seurannan käytännöt

MinduuPro ja eRA-tietojärjestelmän käyttäjien tunnistamisen ja todentamisen dokumentaatio on kuvattu liitteissä (liitteet 1 ja 2).

5 Kanta-palvelujen käytön tietoturvakäytännöt

Liitteessä 1 on kuvattu seuraavat tietoturvakäytännöt:

- Kanta-palveluiden edellyttämät tunnistamis- ja todentamiskäytännöt
- Kanta-palveluiden edellyttämät varmenneratkaisut
- Kanta-palveluiden pääsynhallinnan toteuttaminen
- Vaatimustenmukaisuustodistus
- Kanta-palveluiden edellyttämät käyttövaltuuksien hallinnat ja kytkentä työntekijöiden työrooleihin
- Kanta-palveluiden käytön seuranta-työkalut

6 Tietojärjestelmät

Kanta-palveluihin liittyvät tietojärjestelmät (luokka A)

Atostekin eRA, katso liite 1

Muut asiakas- tai potilastietoja käsittelevät järjestelmät (luokka B)

MinduuPro, katso liite 2

7 Tietojärjestelmäkohtaiset ohjeet ja suunnitelmat

7.1 Atostek eRA (luokkaan A3 kuuluva)

Katso liite 1

7.2 Järjestelmä MinduuPro (luokkaan A1 kuuluva)

Katso liite 2

8 Liitteet:

Liite 1: [ERA järjestelmäkuvaus](#)

Liite 2: [MinduuPro järjestelmäkuvaus](#)