

Neuropsykologipalvelu Leena Himanen

Tietoturvasuunnitelma

9.11.2025

Leena Himanen

Neuropsykologian erikoispsykologi, FT

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus	3
2. Tietoturvasuunnitelman kohde ja päivityskäytännöt	3
3. Yleiset tietoturvakäytännöt	3
4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta	4
5. Henkilökunnan koulutus	4
6. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täytyminen	4
Toistaiseksi ei ole käytössä Kanta-palveluihin liittyviä tietojärjestelmiä.	4
Käyttäjien tunnistautumisessa ja todentamisessa noudatetaan seuraavia käytäntöjä:	4
Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt	4
7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt.....	4
7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta.....	4
7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta	5
7.3. Alusta- ja verkkopalvelujen tietoturallinen käyttö tietosuojan ja varautumisen kannalta	5
8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt	6

1. Tietoturvasuunnitelman käyttötarkoitus

Tämä dokumentti on Neuropsykologipalvelu Leena Himasen tietoturvasuunnitelma. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää asiakastietolain¹ 703/2023 77 §:n 1 ja 2 momentin ja THL:n määräyksen 3/2024 mukaiset velvoitteet.

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluu:

- Neuropsykologipalvelu Leena Himanen
- Nimi: Neuropsykologipalvelu Leena Himanen
- Y-tunnus: 1797645-6
- Vastuuhenkilö: Leena Himanen
- Toimipaikat/palveluyksiköt: Linnankatu 18 3. krs., 20100 Turku
- Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:
- Suunnitelman ja sen päivittämisen vastuuhenkilö: Leena Himanen
- Suunnitelman toteuttamisen vastuuhenkilöt: Leena Himanen
- Katselmointi- ja päivityskäytännöt: Minimissään suunnitelma tarkastetaan vuosittain. Mikäli käytäntöön tulee uudenlaisia dokumentaatiota tai tietojärjestelmiä, niin aina uuden dokumentointitavan tai tiedonkeruun yhteydessä.
- Suunnitelman seuranta ja seurannan dokumentointi: Mikroyrittäjänä FT Leena Himanen on vastuussa seurannasta ja seurannan dokumentoinnista.
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: Luottamuksellisuus on tämän työn ytimessä. Sen vuoksi uuden tietojärjestelmän mahdollisessa hankinnassa tietoturva-asiat ovat ensiarvoisen tärkeitä. Viralliset suositukset esim. Valviran taholta ovat keskeisiä. Toisaalta on mahdollista konsultoida lähisukulaista, joka on nettiturvallisuuteen erikoistunut tietotekniikan DI.
- Päätös suunnitelman hyväksymisestä ja käyttöönotosta: Alan käytänteet ja suositukset tunteva FT Leena Himanen vastaa suunnitelman hyväksymisestä ja käyttöönotosta.

3. Yleiset tietoturvakäytännöt

Henkilötietoja käsitellään luottamuksellisesti, työ kuuluu korostuneen tietosuojan piiriin. Tietosuojaa ensisijaisesti korostavana toimijana käytössä EI ole sähköistä potilastietojärjestelmää. Käytössä on kuitenkin ns. paperiarkisto, johon talletetaan lakisääteiset, työstä säilytettävät dokumentit. Pääsääntöisesti neuropsykologisen tutkimuksen testipapereita säilytetään 12 vuotta. Arkistokaappi sijaitsee ns. kolmen lukon takana toimitilan ulko-ovesta. Potilaiden henkilötietoja sisältäviä dokumentteja työstetään prosessin ollessa kesken tietokoneella, jolloin henkilötiedot ovat sekä salasanan että sormenjälkitunnisteen takana. Tietokonetta säilytetään lukitussa kaapissa. Niitä dokumentteja, joita laki ei edellytä säilytettävän, tuhoetaan. Sähköpostissa ei käytetä asiakkaiden tunnistetietoja tai muuten niin, että henkilö olisi tunnistettavissa. Sopimuskumppaneiden (mm. Kela, Varha) kanssa noudatetaan palvelutuottajasopimuksessa sovittuja käytäntöjä, esim. Varha edellyttää Palsea käytettävän potilasasiakirjan tallentamisessa ja toimittamisessa hyvinvointialueen toimipisteeseen.

Tietosuojavastaavana toimii: Leena Himanen

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Ongelmatilanteissa ei toistaiseksi voi olla kyse digitaalisen tietoturvan ongelmasta, koska sähköistä potilastietojärjestelmää ei ole käytössä. Tilannetta seurataan ja mikäli Kantaan liittyminen tulee myös itsenäiselle ammatinharjoittajalle pakolliseksi, hankintaan tulee A-luokan järjestelmä.

5. Henkilökunnan koulutus

Neuropsykologipalvelu Leena Himanen on mikroyritys, eikä muuta henkilökuntaa ole.6. Tietojärjestelmien tietoturvakäytännöt

6. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täytyminen

Käytössä on laajan suojauksen (F-secure) sisältävä tietokone, jossa on sähköpostiohjelma ja suojattu kuvayhteyden ohjelma. Neuropsykologisen diagnostiikan ollessa kesken tietokoneella on tallennettuna keskeneräinen potilaslausunto word-tiedostona. Valmiit lausunnot arkistoidaan ainoastaan paperiversioina. Sähköistä potilastietojärjestelmää ei toistaiseksi ole. Tietokonepohjaisten testien tulokset printataan paperille, eikä potilastietoja talleteta.

Toistaiseksi keskeisin tietoturvavauha liittyy kirjeitse lähetettäviin potilastietoihin. Tämä on kuitenkin Kelan ohjeiden mukaista, joten tämä ei liene tämän toimijan vastuulla.

Toistaiseksi ei ole käytössä Kanta-palveluihin liittyviä tietojärjestelmiä.

Potilastietojärjestelmiä vielä ole, mutta mikäli se tulee, vastaa asennuksesta, ylläpidosta ja päivityksestä Nova Digital (nettiturvallisuuden erikoistunut toimija, poikani ja tämän vaimon yritys). Nova Digital vastaa teknisestä osuudesta, eikä tällä taholla ole oikeutta päästä käsiksi tietosuojan alaisiin tietoihin. Leena Himanen vastaa siitä, että järjestelmät ovat Valviran ohjeiden mukaisia

Käyttäjien tunnistautumisessa ja todentamisessa noudatetaan seuraavia käytäntöjä:

Vain Leena Himasella on oikeus käyttää tietosuojattuja materiaaleja.

Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Mikroyrittäjänä potilastietojen käsittely on kokonaan yrittäjän vastuulla. Pitkän työuran aikana vastuuntunto lienee kehittynyt siten, että herkällä korvalla tulee puututtua mahdollisiin riskeihin ja epäkohtiin. Myös asiakkaat itse ovat tarkkoja ja varmasti huomauttaisivat, mikäli epäilisivät omien tietojen epäasiallisesta käsittelystä.

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

Toimitilan rakennus on lukittu ja ulko-ovet avautuvat summerin avulla toimitiloista käsin. Etäkone on synkronoitu ja on saman tietoturvan alainen kuin työpaikan kone. Vain ammatinharjoittajalla on oikeus asentaa ohjelmistoja (Leena Himanen). Ulkopuoliset eivät saa asentaa ohjelmia tai käyttää muistitikkuja. Muistitikulle ei talleteta potilaiden henkilötietoja, mutta niitä saa käyttää esim. kuntoutusharjoitusten liikuttamiseen. Tulostin on vain ammatinharjoittajan (Leena Himanen)

käytössä. Lakisääteiset potilasasiakirjat arkistoidaan kahden lukon taakse paloturvalliseen tilaan. Käytössä on sekä paperisilppuri että laajemman tietoturvamateriaalin hävittämiskäytännöt.

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

Puhelimessa on sama tietoturva (F-secure) kuin työkoneella. Lisäksi on käytössä kasvojen tunnistamisella tai pin-koodilla aukeava puhelintiedostot. Kun laitteet poistuvat käytöstä, tyhjennetään koneet 0-tilaan ennen kiertoa tai myyntiä.

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

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

- o