

Vainu Lastensuojelupalvelut Oy

Tietoturvasuunnitelma

12.8.2025, 1/1

Vainu Lastensuojelupalvelut Oy – Ossi Rantala

THL:n määräyksen 3/2024 (THL/4/4.05.00/2024) mukainen tietoturvasuunnitelma lastensuojelun sijaishuollon laitospalveluun, jota tuottaa Vainu Lastensuojelupalvelut Oy

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus	3
2. Tietoturvasuunnitelman kohde ja päivityskäytännöt	4
3. Yleiset tietoturvakäytännöt	6
4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta	7
5. Henkilökunnan koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturallinen käyttäminen	9
5.1. Henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen	9
6. Tietojärjestelmien tietoturvakäytännöt.....	10
6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täytyminen	10
7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt	13
7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta	13
8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt.....	14
9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat.....	15
9.3. Järjestelmät Y (luokkaan B kuuluvat).....	15

1. Tietoturvasuunnitelman käyttötarkoitus

Tietoturvasuunnitelman tavoitteena on ohjata ja selkeyttää tietoturvatoimenpiteitä lastensuojelun laitoshoidossa siten, että turvataan asiakkaiden (lapsien ja nuorten), henkilöstön sekä yhteistyökumppaneiden luottamuksellisuus, eheys ja käytettävyys ko. toimintayksikön tietojärjestelmissä ja -ympäristöissä.

Erityisesti tarkoituksena on:

1. Luottamuksellisuuden varmistaminen

Varmistaa, että hoidossa olevien lasten, nuorten ja heidän perheidensä henkilötiedot sekä muut luottamukselliset tiedot (esimerkiksi sosiaalihuollon asiakastiedot, terveystiedot ja arvioinnit) ovat suojattuna ja käytettävissä vain niillä henkilöillä, joilla on siihen oikeus ja selkeä tehtävärooli.

2. Tietojen eheys

Turvata, että tiedot pysyvät muuttumattomina ja eheinä niin tietojen siirrossa, tallennuksessa kuin käsittelyssäkin – siten, että väärinkirjoitus, tiedon tahaton tai tarkoituksellinen muutos ja tuhonta voidaan estää ja havaita.

3. Järjestelmien ja prosessien käytettävyys

Tukea toimintavarmuutta: varmistaa, että laitoshoidon järjestelmät, kuten asiakastietojärjestelmät, viestintävälineet (esim. sähköposti, potilastietojärjestelmät) ja muut kriittiset tietojärjestelmät ovat käytettävissä silloin, kun niitä tarvitaan asiakastyössä — ottaen huomioon erityisesti kiireelliset tilanteet ja jatkuvuuden varmistus.

4. Lainsäädännön ja viranomaisohjeiden noudattaminen

Tukea THL:n 3/2024 -määräyksen mukaista toiminnan lainmukaisuutta, sekä varmistaa että sitoutuminen tietosuoja- ja tietoturvasäätelyyn (esim. EU:n yleinen tietosuoja-asetus — GDPR, sosiaalihuollon laki ja asetus) toteutuu käytännössä.

5. Luottamuksen rakentaminen asiakkaisiin ja sidosryhmiin

Edistää luottamuksen syntymistä lasten, nuorten ja perheiden kanssa varmistamalla, että heidän yksityisyytensä, tiedonhallintaoikeutensa ja turvallisuutensa otetaan toiminnassa vakavasti.

6. Tietoturvakulttuurin vahvistaminen

Luoda selkeä viitekehys, jonka avulla henkilöstö tietää velvollisuutensa, toimintaohjeensa ja roolinsa tietoturvan ylläpitämisessä. Tietoturva-vaalimiehet, vastuut ja toimintatavat kuvataan selkeästi, jotta poikkeamiin voidaan reagoida tehokkaasti.

Tämä dokumentti on Vainu Lastensuojelupalveluiden tietoturvasuunnitelma. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää asiakastietolain¹ 703/2023 77 §:n 1 ja 2 momentin ja THL:n määräyksen 3/2024 mukaiset velvoitteet. Suunnitelma kokoaa yhteen palvelunantajalta, apteekilta, välittäjältä ja Kansaneläkelaitokselta edellytettävät selvitykset ja vaatimukset.

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat:

- Vainu Lastensuojelupalvelut Oy, Veikkolan yksikkö
- Nimi: Vainu Lastensuojelupalvelut Oy, Veikkolan yksikkö
- Y-tunnus: 3351138-4
- Vastuuhenkilö/johtaja: Jarmo Voutilainen
- Toimipaikat/palveluyksiköt: Nuorisokoti Vainu, Turuntie 692, 02880, Veikkola
- Suunnitelman piiriin kuuluvat alihankkijat ja sopimuskumppanit: Ei alihankkijoita

Tämä tietoturvasuunnitelma koskee Vainu Lastensuojelupalvelut Oy:n lastensuojelun laitoshoidon yksiköiden ja hallinnon toimintaa. Suunnitelma kattaa kaikki tietojen käsittelyyn, tallennukseen, siirtoon ja suojaamiseen liittyvät prosessit, järjestelmät ja palvelut, joita käytetään asiakas- ja henkilöstötietojen hallintaan.

Suunnitelman piiriin kuuluvat erityisesti:

- Asiakastietojen käsittely:

Sosiaalihuollon asiakastiedot, terveystiedot, hoito- ja kasvatussuunnitelmat, yhteydenpidon rajoituksiin liittyvät päätökset, sekä muut arkaluonteiset tiedot, joita käsitellään osana laitoshoidoa.

- Henkilöstötiedot:

Työsuhteeseen, työvuorosuunnitteluun, osaamisen hallintaan ja työterveyshuoltoon liittyvät tiedot.

- Tietojärjestelmät ja laitteet:

Asiakastietojärjestelmät, sähköposti, tiedostojenhallintajärjestelmät, mobiililaitteet, tietokoneet ja muut välineet, joilla tietoja käsitellään.

Esimerkkejä: [täydennettävä organisaation käyttämillä järjestelmillä ja ohjelmistoilla].

- Verkko- ja tietoliikenneyhteydet:

Kiinteät ja langattomat sisäverkot, etäyhteyksratkaisut sekä tietojen siirrossa käytettävät salaus- ja tunnistusmenetelmät.

- Tietojen säilytys ja arkistointi:

Paperiaineisto, sähköinen tallennus, varmuuskopiot ja arkistointikäytännöt, mukaan lukien tietojen säilytysajat ja hävittäminen.

- Kolmansien osapuolten palvelut:

Kaikki ulkoistetut tai kumppaneiden tarjoamat palvelut, joissa käsitellään organisaation asiakas- tai henkilöstötietoja (esim. järjestelmätoimittajat, pilvipalvelut, IT-tuki).

Tämä suunnitelma kattaa niin normaaliolosuhteet kuin poikkeus- ja häiriötilanteet. Se koskee kaikkia työntekijöitä, harjoittelijoita, sijaisia ja muita henkilöitä, joilla on pääsy organisaation tietoihin tai järjestelmiin.

3. Yleiset tietoturvakäytännöt

[Määräys 3/2024: 6.1 Yleiset tietoturvakäytännöt]

Vainu Lastensuojelupalvelut Oy noudattaa tietoturva- ja tietosuojakäytännöissään voimassa olevaa lainsäädäntöä, viranomaisohjeita sekä organisaation omia tietoturvapoliittikoja ja menettelyohjeita. Tietoturvallisuustyö on osa jokapäiväistä toimintaa ja se kytkeytyy kiinteästi laatu- ja riskienhallintatyöhön.

Tietoturvallisuus, tietosuoja, riskienhallinta ja asiakastietojen käsittelyn omavalvonta toteutetaan seuraavien dokumenttien ja ohjeiden mukaisesti:

- Tietoturvapoliittikka (Vainu Lastensuojelupalvelut Oy)
- Tietosuojapolitiikka ja rekisteriselosteet
- Riskienhallintasuunnitelma
- Henkilötietojen käsittelytoimien selosteet (GDPR 30 art.)
- Alihankkija- ja palvelusopimukset, jotka sisältävät tietoturva- ja tietosuojaliitteet
- Asiakastietojärjestelmän toimittajan (Fastroi Oy, Nappula) tietoturvaohjeet ja -sertifikaatit
- Etä- ja hybridityöohjeet (sis. tietoturvan varmistamisen ohjeistus)
- Tietoturvapoikkeamien hallintaohje

Tietoturvallisuustyön organisointi ja vastuut

- Tietosuojavastaava: Jenny Rantala

Vastaa tietosuoja-asioiden koordinoinnista, henkilöstön neuvonnasta, yhteydenpidosta viranomaisiin sekä tietosuojapoikkeamien hallinnasta.

- Tieturvasta vastaava johtoryhmän jäsen: Ossi Rantala

Vastaa tietoturvapoliittikan toimeenpanosta, teknisen ja hallinnollisen tietoturvan seurannasta sekä kehittämisestä.

- Yksikön esimiehet:

Valvovat, että henkilöstö noudattaa tietoturva- ja tietosuojakäytäntöjä päivittäisessä työssä.

- Kaikki työntekijät:

Ovat velvollisia noudattamaan tietoturva- ja tietosuojakäytäntöjä sekä ilmoittamaan havaitsemistaan poikkeamista välittömästi esimiehelle tai tietosuojavastaavalle.

Sopimuskumppanit ja alihankkijat

Kaikkien sopimuskumppanien, joilla on pääsy organisaation tietoihin, on noudatettava vähintään Vainu Lastensuojelupalvelut Oy:n tietoturva vaatimuksia. Tämä varmistetaan sopimusliitteillä, joissa määritellään tietosuoja- ja tietoturva velvoitteet.

Tietosuojavastaavana toimii: Jenny Rantala

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

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

Vainu Lastensuojelupalvelut Oy varautuu toiminnassaan erilaisiin virhe-, häiriö- ja poikkeustilanteisiin, jotta asiakastietojen luottamuksellisuus, eheys ja käytettävyys voidaan varmistaa kaikissa tilanteissa.

4.1 Varautuminen poikkeustilanteisiin ja jatkuvuudenhallinta

- Organisaatiolla on jatkuvuussuunnitelma, joka määrittää toimintatavat teknisissä häiriöissä, fyysisissä uhkatilanteissa ja muissa kriisitilanteissa.
- Asiakastyön kannalta kriittiset prosessit on tunnistettu ja niiden jatkuvuus varmistetaan mm. seuraavasti:
 - Varmuuskopiointi: Asiakastietojärjestelmä (Fastroi Nappula) varmuuskopioidaan toimittajan palvelimilla. Varmistukset tarkistetaan säännöllisesti.
 - Manuaaliset toimintatavat: Sähköisten järjestelmien ollessa poissa käytöstä käytetään kirjallisia lomakkeita ja varaprosesseja, jotka tallennetaan myöhemmin järjestelmään.
 - Häiriöharjoitukset: Poikkeustilanteiden hallintaa harjoitellaan vähintään kerran vuodessa.
 - Jatkuvuussuunnitelma tarkistetaan vähintään kerran vuodessa ja aina merkittävien muutosten yhteydessä.

4.2 Virhe- ja ongelmatilanteiden hallinta

- Ilmoitusvelvollisuus: Kaikilla työntekijöillä on velvollisuus ilmoittaa havaitsemistaan teknisistä vioista, tietoturva poikkeamista tai epäilyttävistä tilanteista välittömästi esimiehelle, tietosuojavastaavalle tai IT-tuelle.
- Tukipalvelut ja yhteystiedot:
 - Asiakastietojärjestelmä (Nappula) – Fastroi Oy:n tuki: [yhteystiedot täydennetään]
 - IT- ja laitetuki: [palveluntarjoajan nimi ja yhteystiedot]
 - Tietoturva- ja tietosuoja-asiat: Jenny Rantala, tietosuojavastaava ([sähköposti] / [puhelin])
 - Poikkeamien käsittelyprosessi:
 1. Poikkeama havaitaan ja kirjataan (sis. ajankohta, kuvaus, toimenpiteet).
 2. Tilanne analysoidaan ja luokitellaan vakavuuden mukaan.
 3. Toteutetaan välittömät rajoittavat toimet (esim. tunnusten sulkeminen, verkon eristäminen).
 4. Selvitetään juurisyyn ja ryhdytään korjaaviin toimenpiteisiin.
 5. Dokumentoidaan tapahtuma ja tehdään tarvittavat viranomaisilmoitukset.

- Tietosuojavaltuutettu (72 tunnin kuluessa, jos kyseessä tietosuoja-asetuksen mukainen henkilötietojen tietoturvaloukkaus).
- Valvira (jos järjestelmäpoikkeama aiheuttaa merkittävän riskin asiakasturvallisuudelle).
- Esimerkkejä käsiteltävistä poikkeamista:
- Asiakastietojen luvaton katselu tai luovutus.
- Haittaohjelma tai virustartunta.
- Verkko- ja tietoliikennehäiriöt.
- Laitteiston tai ohjelmiston kriittinen vika.

4.3 Toiminta ilman tietojärjestelmiä

- Mikäli asiakastietojärjestelmä tai verkko ei ole käytettävissä:
- Käytetään valmiiksi tulostettuja paperilomakkeita, jotka säilytetään lukitussa kaapissa.
- Tallennetaan tiedot järjestelmään viivytyksettä palvelun palautuessa.
- Huolehditaan, että paperidokumentit hävitetään tietoturvallisesti tallennuksen jälkeen.

4.4 Jatkuvuuden kehittäminen

- Jokaisen poikkeustilanteen jälkeen tehdään jälkiarviointi ja tarvittavat muutokset prosesseihin.
- Poikkeamat ja kehitystoimet käsitellään johtoryhmän kokouksissa.
- Henkilöstölle tiedotetaan opit ja muutokset toimintamalleissa.

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

5.1. Henkilökunnan koulutus sekä osaamisen ylläpito ja kehittäminen

Vainu Lastensuojelupalvelut Oy varmistaa, että kaikki työntekijät saavat riittävän koulutuksen asiakastietojen käsittelyyn, tietosuojaan ja tietoturvan toteuttamiseen sekä käytössä olevien tietojärjestelmien (Fastroi Nappula) hallintaan.

Koulutuksen ja osaamisen ylläpidon käytännöt:

- Perehdytyskoulutus:

Uusille työntekijöille järjestetään perehdytys, joka sisältää:

- Asiakas- ja henkilötietojen käsittelyn periaatteet.
- Organisaation tietosuoja- ja tietoturvapoliitikat.
- Fastroi Nappula -järjestelmän käytön perusteet.
- Poikkeamatilanteiden toimintaohjeet.
- Säännöllinen täydennyskoulutus:

Kaikille työntekijöille järjestetään vähintään kerran vuodessa tietosuoja- ja tietoturvakoulutus. Tarpeen mukaan koulutus järjestetään useammin, jos toimintaympäristössä tapahtuu muutoksia (esim. lakimuutokset, tietojärjestelmäpäivitykset).

- Osaamisen seuranta:
- Osallistumiset koulutuksiin dokumentoidaan.
- Esihenkilöt seuraavat henkilöstön osaamistasoa ja ilmoittavat koulutustarpeista tietosuojavastaavalle.
- Erityiskoulutus:

Pääkäyttäjät ja muut erityisrooleissa toimivat saavat syventävää koulutusta järjestelmien hallintaan ja tietoturvan varmistamiseen.

5.2 Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

Käyttöohjeiden hallinta ja saatavuus:

- Kaikilla järjestelmän käyttäjillä on pääsy ajantasaisiin käyttöohjeisiin (sähköinen intranet / dokumenttivarasto).

- Fastroi Nappula -järjestelmän toimittajan ohjeet ovat saatavilla järjestelmän sisäisen ohjetoiminnon kautta sekä erillisinä pdf-ohjeina.
- Ohjeet ovat ymmärrettävässä muodossa ja saatavilla suomeksi.

Ohjeiden päivittäminen ja tiedottaminen:

- Käyttöohjeet päivitetään aina järjestelmäpäivitysten tai toimintatapamuutosten yhteydessä.
- Päivityksistä tiedotetaan sähköpostitse ja henkilöstöpalaverissa.
- Päivitysvastuu: tietosuojavastaava ja järjestelmäpääkäyttäjä yhdessä.

Ohjeiden noudattamisen varmistaminen:

- Esihenkilöt seuraavat, että työntekijät käyttävät järjestelmiä ohjeiden mukaisesti.
- Tarvittaessa järjestetään lisäperehdytys tai ohjaus.

Tuki ja neuvonta:

- Käyttäjät voivat kääntyä järjestelmäpääkäyttäjän, esihenkilön tai Fastroi Nappula -tuen puoleen ongelmatilanteissa.
- Tukipalvelujen yhteystiedot ovat helposti saatavilla intranetissä ja työpisteissä.

6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

Käytössä oleva asiakastietojärjestelmä:

- Nimi: Nappula
- Versio: [päivitetään ajantasainen versiotieto]
- Toimittaja: Fastroi Oy
- Yhteystiedot: [yhteystiedot täydennetään]
- Luokka: B (sosiaalihuollon asiakastietoja käsittelevä järjestelmä)
- Käyttötarkoitus: Lastensuojelun asiakastietojen tallennus, hallinta ja seuranta; hoito- ja kasvatussuunnitelmien dokumentointi; yhteydenpidon ja rajoitusten hallinta.
- Käyttäjryhmät: Sosiaalialan ohjaajat, ohjaajat, esimiehet, hallinto.

Olennaisten vaatimusten täyttäminen:

- Fastroi Nappula täyttää asiakastietolain (703/2023) ja THL:n määräyksen 3/2024 mukaiset olennaiset vaatimukset luokan B järjestelmälle.
- Toimittaja toimittaa vuosittain tietoturvallisuuden arviointia koskevan todistuksen ja tiedot tarkistetaan Valviran tietojärjestelmärekisteristä.
- Sopimukseen sisältyy vaatimus tietoturvaominaisuuksien ylläpidosta ja raportoinnista.

6.2 Tietojärjestelmien asennus, ylläpito ja päivitys

- Nappulan tekninen ylläpito, päivitykset ja varmuuskopiointi hoidetaan Fastroi Oy:n toimesta pilvipalveluna.
- Päivitykset tehdään hallitusti, ja niistä tiedotetaan etukäteen käyttäjille.
- Uudet versiot testataan toimittajan ympäristössä ennen tuotantokäyttöä.
- Omissa työasemissa ja mobiililaitteissa huolehditaan käyttöjärjestelmän ja tietoturvaohjelmistojen ajantasaisuudesta (vastuu: IT-tuki).



6.3 Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

- Käyttöoikeudet myönnetään vain henkilöille, joiden työtehtävät sitä edellyttävät (minimiperiaate).
- Käyttöoikeuspyynnöt hyväksyy yksikön esimies ja toteuttaa järjestelmäpääkäyttäjä.
- Poistuvien työntekijöiden tunnukset suljetaan viimeistään työsuhteen päättymispäivänä.
- Tunnistautuminen tapahtuu henkilökohtaisella käyttäjätunnuksella ja salasanalla; salasanojen tulee täyttää organisaation vahvuusvaatimukset.
- Yhteiskäyttötunnukset eivät ole sallittuja.

6.4 Asiakastietojärjestelmän pääsynhallinnan ja käytön seurannan käytännöt

- Nappula-järjestelmä tuottaa lokitiedot kaikista asiakastietojen katseluista, muokkauksista ja luovutuksista.

- Lokitietoja seuraa tietosuojavastaava säännöllisesti ja tarvittaessa epäilyttävissä tilanteissa.
- Lokit säilytetään vähintään lainsäädännön edellyttämän ajan.
- Epäilyistä väärinkäytöksistä tehdään välittömät selvitykset ja tarvittavat ilmoitukset viranomaisille.

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

- Toimitilojen turvallisuus:

Kaikki toimipisteet ovat lukittavia ja niissä on kulunvalvonta (avaimet, kulkukortit tai koodilukot).

Ulkopuolisilla ei ole pääsyä työtiloihin ilman henkilöstön saattajaa.

- Näyttöpäätteiden suojaaminen:

Työasemat sijoitetaan niin, ettei asiattomilla ole näköyhteyttä näytöille. Tarvittaessa käytetään näytönsuojakalvoja.

Näytöt lukittuvat automaattisesti 5 minuutin käyttämättömyyden jälkeen.

- Paperiaineisto:

Arkaluonteiset asiakastietoja sisältävät asiakirjat säilytetään lukituissa kaapeissa.

Hävittäminen tehdään silppuamalla tai lukittuihin tietosuojalaatikoihin.

- Tulostimet:

Tulostimet sijoitetaan henkilöstötiloihin. Tarvittaessa käytössä on turvatulostus, jossa asiakirja tulostuu vasta käyttäjän tunnistautumisen jälkeen.

7.2 Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

- Työasemat:

Kaikissa työasemissa on ajan tasalla oleva virustorjunta ja automaattiset tietoturvapäivitykset.

Vain organisaation hyväksymiä ohjelmia saa asentaa, ja asennusoikeudet on rajattu IT-tuelle.

- Mobiililaitteet:

Työntekijöiden käytössä olevat kannettavat, tabletit ja puhelimet ovat suojattuja salasanalla, PIN-koodilla tai biometrisellä tunnistuksella.

Kadonneet tai varastetut laitteet voidaan etälukita tai tyhjentää.

- Tietojen poistaminen:

Laitteiden luovutuksen tai käytöstä poiston yhteydessä kaikki tiedot poistetaan pysyvästi tietoturvaohjelmistolla.

- Käyttöympäristön tukipalvelut:

Käyttöjärjestelmä- ja ohjelmistopäivityksistä vastaa IT-tuki. Päivitykset asennetaan viivytyksettä tietoturvariskien minimoimiseksi.

7.3 Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta

- Verkkoyhteydet:

Kaikki sisäverkot on suojattu palomuuureilla ja salasanailla suojatuilla langattomilla yhteyksillä.

Asiakkaille mahdollisesti tarjottu Wi-Fi on erotettu organisaation sisäverkosta.

- Etäyhteydet:

Etätyössä käytetään salattua VPN-yhteyttä.

Etäkäyttö on sallittua vain organisaation hallitsemilta ja tietoturva-vaatimukset täyttäviltä laitteilta.

- Palvelimet ja pilvipalvelut:

Asiakastiedot sijaitsevat Fastroi Oy:n hallinnoimissa suojatuissa palvelinympäristöissä EU/ETA-alueella.

Palveluntarjoajalta edellytetään sopimuksin tietoturvasoa, joka vastaa vähintään organisaation omaa tasoa.

- Varautuminen häiriötilanteisiin:

Häiriöiden varalle on määritelty varayhteysmenettelyt ja mahdollisuus siirtyä manuaalisiin toimintatapoihin (ks. kohta 4).

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

Vainu Lastensuojelupalvelut Oy ei tällä hetkellä käytä Kanta-palveluja, koska käytössä oleva asiakastietojärjestelmä Fastroi Nappula (luokka B) ei ole liitetty Kanta-järjestelmään. Asiakastietojen käsittely tapahtuu järjestelmässä paikallisesti ja palveluntarjoajan hallinnoimassa suojatussa pilviympäristössä.

8.1 Valmius Kanta-liittymiseen

- Organisaatio seuraa lainsäädännön ja THL:n määräysten kehittymistä liittyen sosiaalihuollon tietojen tallentamiseen Kanta-arkistoon.
- Fastroi Oy:n kanssa ylläpidetään yhteyttä, jotta Kanta-liittymisen mahdollistuessa voidaan toteuttaa liittymisprojekti hallitusti.
- Liittymisen yhteydessä varmistetaan:
- Käytettävä järjestelmä on luokiteltu luokkaan A2 tai A3 ja se täyttää Kanta-yhteensopivuuden olennaiset vaatimukset.
- Käyttäjät saavat koulutuksen Kanta-palveluiden käyttöön ja toimintatapoihin.

- Käyttövaltuudet, tunnistautuminen ja lokiseuranta toteutetaan Kanta-vaatimusten mukaisesti.

8.2 Tietoturvakäytännöt Kanta-liittymisen varalta

- Tunnistautuminen ja pääsynhallinta:

Kanta-palvelujen käytössä sovelletaan vahvaa sähköistä tunnistautumista (henkilökohtaiset varmenteet, toimikortit).

- Lokiseuranta:

Kanta-yhteyden myötä lokitietoja seurataan säännöllisesti tietosuojavastaavan toimesta ja lokit säilytetään lainsäädännön mukaisesti.

- Varmuuskopiointi ja varautuminen:

Kanta-liittymisen yhteydessä varmistetaan, että tiedot tallentuvat sekä paikallisesti että Kanta-arkistoon, ja että varmistukset toimivat moitteettomasti.

- Poikkeamatilanteet:

Kanta-palvelujen häiriöissä käytetään manuaalisia toimintamalleja, ja tiedot tallennetaan viiveettä palvelun palautuessa.

8.3 Liittymättömyyden perustelu nykytilanteessa

- Sosiaalihuollon Kanta-liittymisen ei ole vielä pakollinen kaikille palveluntuottajille.
- Käytössä oleva järjestelmä (Nappula) ei ole A2/A3-luokan Kanta-yhteensopiva järjestelmä, mutta toimittajalla on kehityspolku liittymisen mahdollistamiseksi.

9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat

9.3. Järjestelmät Y (luokkaan B kuuluvat)

Järjestelmän nimi: Nappula

Versio: [päivitetään ajantasainen versiotieto]

Toimittaja: Fastroi Oy

Yhteystiedot: [yhteystiedot täydennetään]

Luokka: B (sosiaalihuollon asiakastietoja käsittelevä järjestelmä)

Käyttötarkoitus:

- Lastensuojelun asiakastietojen kirjaaminen ja hallinta

- Hoito- ja kasvatussuunnitelmien laadinta ja ylläpito
- Yhteydenpitoon ja rajoitustoimenpiteisiin liittyvien tietojen tallennus
- Asiakasdokumenttien arkistointi
- Raportointi ja seurantatiedot viranomaisille

Käyttäjärühmät:

- Sosiaalialan ohjaajat
- Ohjaajat
- Esimiehet
- Hallinto
- Tietosuojavastaava

Käyttöohjeet:

- Järjestelmän käyttöohjeet ovat saatavilla sähköisesti järjestelmän sisäisessä ohjetoiminnossa ja organisaation intranetissä.
- Käyttöohjeet kattavat kirjautumisen, asiakastietojen tallentamisen ja muokkaamisen, raporttien hakemisen, asiakirjojen tulostamisen ja poikkeustilanteiden toimintaohjeet.

Ohjeiden päivittäminen ja jakelu:

- Toimittaja (Fastroi Oy) päivittää ohjeet järjestelmäpäivitysten yhteydessä.
- Tietosuojavastaava ja järjestelmäpääkäyttäjä huolehtivat, että ohjeiden muutoksista tiedotetaan käyttäjille sähköpostitse ja henkilöstöpalavereissa.

Menettelyt virhe- ja ongelmatilanteissa:

- Käyttäjät ilmoittavat häiriöistä välittömästi esimiehelle ja järjestelmäpääkäyttäjälle.
- Vakavissa häiriöissä otetaan yhteys Fastroi Oy:n tukeen ([yhteystiedot]).
- Poikkeustilanteiden hallinta noudattaa tietoturvasuunnitelman kohtaa 4.

Järjestelmäkohtaiset tukipalvelut:

- Fastroi Oy:n asiakastuki (puhelin, sähköposti, tukilomake).

- Sisäinen IT-tuki laite- ja verkkoyhteysongelmissa.

Asennus- ja ylläpitovastuut ja -vaatimukset:

- Järjestelmä toimii pilvipalveluna Fastroi Oy:n hallinnoimissa konesaleissa.
- Toimittaja vastaa palvelinympäristön tietoturvasta, päivityksistä ja varmuuskopioinnista.
- Käyttäjälaitteiden tietoturvasta vastaa organisaation IT-tuki.

Menettelytavat ja vastuut virhe- ja poikkeustilanteissa:

- Pääkäyttäjä seuraa järjestelmän toimintaa ja raportoi ongelmista tietosuojavastaavalle.
- Tietosuojavastaava huolehtii tietosuojapoikkeamien käsittelystä ja viranomaisilmoituksista.

Käyttövaltuushallinta järjestelmässä:

- Käyttöoikeudet myönnetään vain työtehtävien edellyttämälle tasolle.
- Käyttöoikeuspyynnöt hyväksyy esimies ja toteuttaa järjestelmäpääkäyttäjä.
- Poistuvien työntekijöiden tunnukset suljetaan viimeistään työsuhteen päättyessä.

Tunnistautuminen järjestelmässä:

- Henkilökohtainen käyttäjätunnus ja salasana.
- Salasanat vaihdetaan vähintään kerran vuodessa tai tarvittaessa (esim. tietoturvapoikkeaman jälkeen).
- Monivaiheinen tunnistautuminen otetaan käyttöön, jos toimittaja sen mahdollistaa.

Lokit:

- Järjestelmä tallentaa lokitiedot kaikista asiakastietojen katseluista, muokkauksista ja luovutuksista.
- Lokiseurannasta vastaa tietosuojavastaava.
- Lokit säilytetään vähintään lainsäädännön mukaisen ajan.

Järjestelmän lukittuminen:

- Käyttöistunto sulkeutuu automaattisesti 15 minuutin käyttämättömyyden jälkeen.
- Käyttäjän on kirjauduttava uudelleen jatkaakseen.

Tietojärjestelmän tiedot Valviran tietojärjestelmärekisterissä:

- Tarkistetaan vuosittain tietosuojavastaavan toimesta.
- Varmistetaan, että järjestelmän luokitus ja olennaisten vaatimusten täyttymisen tiedot ovat ajan tasalla.