Alina Hoivatiimi Oy

Sarin Hoiva-Apu Oy / Alina Tampere, Keskusta

Tietoturvasuunnitelma

5.1.2026

Laatijat

Ketjuhallinto

Hyväksytty 28.10.2024

Alina Hoivatiimi Oy:n liiketoimintajohtaja Antti Sahlström

Alina Hoivatiimi Oy:n tietosuojavastaava

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus

Tämä dokumentti on Alina Hoivatiimi Oy:n tietoturvasuunnitelma, ja käyttäjänä Franchise -yritys Alina Tampere, Keskusta / Sarin Hoiva-Apu Oy. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää uuden asiakastietolain[1] 784/2021 27 §:n ja THL:n määräyksen 3/2021 mukaiset velvoitteet. Suunnitelma kokoaa yhteen asiakastietolaissa vaaditut omavalvonnan kohteelta edellytettävät selvitykset ja vaatimukset.

Uuden asiakastietolain (784/2021) voimaantulo toi mukanaan päivitetyt vaatimukset tietoturvan ja tietosuojan osalta, jotka eroavat vanhan asiakastietolain (159/2007) asettamista vaatimuksista. Tämä tietoturvasuunnitelma päivittää olemassa olevat omavalvontasuunnitelmat vastaamaan uusia tietoturva- ja tietosuojavaatimuksia.

Tietoturvasuunnitelma tarkistetaan vähintään kerran vuodessa ja aina merkittävien lainsäädännöllisten tai toiminnallisten muutosten yhteydessä. Tietoturvasuunnitelman laadinnan ja noudattamisen operatiivinen vastuu on palvelunantajan IT-osastolla ja strateginen vastuu vastaavalla johtajalla, joka valvoo, että suunnitelma noudattaa lainsäädännön ja viranomaisten asettamia velvoitteita. Tietoturvasuunnitelman laatimisessa on hyödynnetty seuraavia lähteitä, jotka tarjoavat kattavat työkalut ja ohjeet organisaation kyberturvallisuuden arviointiin, tietoturvan ja tietosuojan parantamiseen sekä hankintojen tietoturvavaatimuksiin. Näitä lähteitä käytetään erityisesti suunnitelman riskienhallinnan, vaatimustenmukaisuuden ja tietosuojan arviointiin.

- 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
- 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]

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat kaikki Alina hoivatiimi Oy:n Franchise ketjuun kuuluvat itsenäiset yritykset, joissa yrityksen johtaja sitoutuu noudattamaan ketjuhallinnon laatimaa tietoturvallisuussuunnitelmaa.

Tietoturvasuunnitelman kohteena olevan yksikön perustiedot:

- Nimi: Sarin Hoiva-Apu Oy
- Y-tunnus: 3260837-9
- Vastuuhenkilö/johtaja: Sari Lantto
- Toimipaikat/palveluyksiköt: Alina Tampere, Keskusta

- 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: Tietosuojavastaava Heli Sydänpuro
- Suunnitelman toteuttamisen vastuuhenkilöt: Käytännön tietosuoja- ja tietoturvatoimenpiteiden toteuttamisesta vastaa laaditun suunnitelman mukaisesti Franchise ketjuun kuuluvan yrityksen johtaja.
- Franchise-yritysten johtajat ovat sitoutuneet noudattamaan ketjuhallinnon laatimaa tietoturvasuunnitelmaa. Ketjuhallinto valvoo suunnitelman noudattamista säännöllisillä auditoinneilla sekä seuraa aktiivisesti tietoturvaan liittyvien toimenpiteiden toteuttamista
- Suunnitelman piiriin kuuluvat myös alihankkijat ja sopimuskumppanit, joiden on sopimuksen mukaisesti sitouduttava noudattamaan tietoturvasuunnitelman vaatimuksia ja parhaita käytäntöjä.
- Tarkistus- ja päivityskäytännöt: Suunnitelma tarkastetaan ja päivitetään säännöllisesti vuosittain sekä tarvittaessa muutosten myötä useammin.
- Suunnitelman seuranta ja seurannan dokumentointi: Suunnitelman noudattamista seurataan sisäisten ja ulkoisten auditointien yhteydessä vuosittain ja suunnitelma käydään ketjuhallinnon toimesta läpi yrittäjien kanssa. Auditoinnit suoritetaan vuosittain alkuvuoden aikana, ja poikkeamat korjataan kolmen kuukauden sisällä auditoinnista. Korjaavat toimenpiteet dokumentoidaan, ja niiden toteuttamista seurataan aktiivisesti osana laatujärjestelmää.
- Tietoturvallisuudesta vastaa Franchise ketjuun kuuluvien itsenäisten yritysten johtajat, jotka nimeävät sisäisesti tietoturvallisuuden vastuuhenkilöt. Tietoturvallisuussuunnitelman vastuualueet käydään auditointien yhteydessä läpi vuosittain.
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: Tietojärjestelmien hankinnoissa ja päivityksissä varmistetaan, että järjestelmät täyttävät sosiaali- ja terveysalan kansalliset tietosuojavaatimukset sekä Euroopan unionin yleisen tietosuoja-asetuksen (GDPR) asettamat velvoitteet.
- Päätös suunnitelman hyväksymisestä ja käyttöönotosta: Suunnitelman hyväksymisestä vastaa Alina Hoivatiimi Oy:n tietosuojavastaava sekä liiketoimintajohtaja. Uuden version hyväksymisen jälkeen tiedotetaan kenttäpäälliköitä, jotka vastaavat suunnitelman käyttöönottamisesta Franchise-yrityksissä. Kenttäpäälliköiden vastuulla on myös varmistaa, että suunnitelman muutokset ymmärretään ja otetaan käyttöön tehokkaasti. Suunnitelma tarkistetaan vuosittain ja uuden version käyttöönoton hyväksyy ketjun tietosuojavaltuutettu sekä liiketoimintajohtaja.

3. Yleiset tietoturvakäytännöt

Yleiset tietoturvakäytännöt määrittävät organisaation periaatteet ja toimenpiteet, joiden avulla varmistetaan tietojen luottamuksellisuus, eheys ja saatavuus. Käytännöt ohjaavat tietojen suojaamista kaikissa prosesseissa, ja niiden noudattaminen on osa jokaisen työntekijän vastuuta. Alina Hoivatiimi Oy:ssa noudatetaan seuraavia yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

Tietoturvallisuustyötä tehdään seuraavien dokumenttien mukaisesti:

- Tietosuojapolitiikka
- Omavalvontasuunnitelma
- Riskienhallintapolitiikka ja riskienhallintaan liittyvät ylläpito- ja kehittämissuunnitelmat.
- Selosteet henkilötietojen käsittelytoimista
- Lista muista mahdollisista yrityksissä olevista tietoturvasuunnitelmaan kuuluvista tietojenkäsittelyyn ja tietoturvallisuuteen liittyvistä sopimuskumppaneista alihankkijoineen, mikäli alihankkijoita hyödynnetään: käyttöympäristön tukipalvelut, tietojärjestelmäpalvelut ja muut mahdolliset palvelut.
- Tietojärjestelmäpalvelun tuottajien tietoturvallisuusohjeet, yhteystiedot.
- Omat tietoturvallisuusohjeet (tietoturvallisuussuunnitelma, käsikirjat)
- Laatukäsikirja käytössä yrityksissä, joissa hyväksytty ulkoinen laatusertifikaatti.

Riskienhallintapolitiikka sisältää tietoturvaan liittyvät riskit ja määrittää niiden hallintakeinot. Tietoturvariskit arvioidaan säännöllisesti, ja niihin kohdistetaan ennaltaehkäiseviä toimenpiteitä osana organisaation kokonaisvaltaista riskienhallintaa. Alihankkijat ja sopimuskumppanit sitoutuvat noudattamaan Alina Hoivatiimi Oy tietoturvakäytäntöjä, ja heidän toiminnastaan laaditaan tietoturvasopimukset. Näissä sopimuksissa varmistetaan, että kaikki alihankkijat ja palveluntarjoajat noudattavat samoja tietoturva- ja tietosuojavaatimuksia.

Laatukäsikirja tukee tietoturvan hallintaa, erityisesti yrityksissä, joissa on käytössä ulkoisesti hyväksytty laatusertifikaatti, kuten ISO 27001. Tietoturvasertifioinnit osoittavat, että yrityksen tietoturvakäytännöt ovat kansainvälisesti hyväksyttyjen standardien mukaisia

Alina Hoivatiimi Oy tietosuojavastaavana toimii Vesa Hietanen, joka vastaa tietoturva- ja tietosuojakäytäntöjen valvonnasta sekä niiden ajantasaisuudesta. Häneen voi ottaa yhteyttä sähköpostitse: vesa.hietanen@norlandia.com tai puhelimitse: 0505635169.

Yrittäjän omat tiedot yksityiskohtaisesta tietosuojavastaavan roolista:

Nimi ja asema yrityksessä:	Sari Lantto
Puhelinnumero:	044 455 8710
Sähköposti:	sari.lantto@alinahoivatiimi.fi

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja:

- aihepiiriin kuuluva valmius- ja jatkuvuussuunnitelma
- käytännön harjoittelu, valmiustoiminta, ohjeistukset, ohjeiden saatavuus
- normaalista poikkeavat olosuhteet, lyhyt- ja pitkäkestoiset häiriöt, poikkeusolosuhteet
- varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä ja/tai alusta- ja verkkopalveluita
- poikkeustilanteissa, joissa tietojärjestelmiä tai verkkopalveluita ei voida käyttää, organisaatio siirtyy manuaalisiin prosesseihin. Tämä voi sisältää esimerkiksi fyysisten

asiakirjojen käyttöä. Kyseisistä prosesseista on olemassa erilliset ohjeet, ja henkilöstölle järjestetään säännöllistä koulutusta poikkeustilanteiden hallitsemiseksi.
- käytetään viitekehyksenä kyberturvallisuuden parantamiseksi NIST Cybersecurity Framework

Virhe- ja ongelmatilanteissa noudatetaan seuraavia toimintatapoja:

Verkko- tai tietoliikenneongelmat: Franchise yritysten vastaavat johtajat hankkivat itsenäisesti internetyhteydet ja laitteet. Palveluntarjoajan yhteystiedot ovat esillä yrityksissä mahdollisia tietoliikenneongelmia varten. Yrityksestä ollaan yhteydessä siihen palveluntarjoajaan mistä internetyhteys on hankittu. Puhelimien liittymät ovat hankittu keskitetysti DNA:lta, joten puhelinverkko ongelmatilanteissa olemme yhteydessä palveluntarjoajaan.

Tietojärjestelmien käyttöön liittyvät ongelmat:

- Domacare-järjestelmä / Invian / tuki@domacare.fi
- Netvisor-järjestelmä / Visma / tuki.netvisor@visma.com
- Tietojärjestelmien, niiden osajärjestelmien ja komponenttien hallintatoimenpiteet: Palveluntarjoaja on velvollinen ilmoittamaan järjestelmien päivityksistä, huoltotoimista ja mahdollisista järjestelmäkatkoksista etukäteen. Yhteistyö ketjunhallinnan IT-päällikön ja tietosuojavastaavan kanssa varmistaa, että kaikki päivitykset suoritetaan hallitusti, ja tietojärjestelmien käyttöön liittyvät riskit minimoidaan.
- Epäiltyjen, havaittujen tai toteutuneiden tietoturva- tai tietosuojauhkien tai ongelmien hallinta:

    - Tietoturvapoikkeamien sattuessa on oltava välittömässä yhteydessä ketjun tietoturva- ja tietosuojavastaavaan. Ilmoitukset tehdään **sähköpostitse / tietoturvalomakkeella Tietoturvaloukkauksen ilmoituslomake** vastaaville henkilöille. Jokaisella tietoturvaloukkauksella on määritelty vastuuosapuoli, joka johtaa korjaustoimenpiteitä ja varmistaa, että uhka on eliminoitu.
    - Haittaohjelman havaitsemisen jälkeen laite irrotetaan verkosta ja viedään puhdistettavaksi organisaation tietoturvaosaston ohjeistuksen mukaisesti. Tarvittaessa laitteen käyttö estetään ja varmuuskopiot tarkistetaan ennen palautusta verkkoon
    - Vuotaneiden tunnusten vaihto suoritetaan välittömästi tietoturvavastaavan valvonnassa, ja käyttäjälle annetaan ohjeet, kuinka toimia tietojen turvaamiseksi. Uudet tunnukset luodaan ketjun tietoturvapolitiikan mukaisesti.
    - Jos tietojen kalasteluyritys havaitaan, kyseinen laite eristetään välittömästi verkosta ja suoritetaan perusteellinen haittaohjelmien tarkistus ja puhdistus. Samalla kaikki altistuneet käyttäjätunnukset vaihdetaan välittömästi uusiin, ja käytetään monivaiheista tunnistautumista (MFA) vahinkojen minimoimiseksi. Tapahtumasta raportoidaan ketjun tietoturvavastaavalle, ja kaikki toimenpiteet dokumentoidaan tietoturvaloukkauksien hallintajärjestelmään.
    - Tietoturvaloukkauksen havaitsemisen jälkeen rekisterinpitäjä raportoi tapahtuman 72 tunnin kuluessa tietosuojavaltuutetulle ja ilmoittaa asiasta myös rekisteröidylle henkilölle, mikäli hänen tietonsa ovat vaarantuneet. Tiedot ilmoitetaan kirjallisesti ja ne sisältävät loukkauksen luonteen, vaikuttavat henkilötiedot sekä toimenpiteet, joilla riskejä minimoidaan.
    - Jokainen organisaation työntekijä on velvollinen ilmoittamaan omalle esihenkilölleen tai ketjun tietosuojavastaavalle havaitessaan tietoturvaloukkauksen tai epäillessään sellaisen tapahtuneen.

- Jos sosiaalihuollon asiakastietoja tai potilastietoja tai muita suojattavia tietoja käsittelevät tietojärjestelmät toimivat selvästi väärin suhteessa niille asetettuihin kansallisiin vaatimuksiin, ilmoitamme välittömästi tietojärjestelmäpalvelun tuottajalle sekä valvontaviranomaisille asiasta. Tietojärjestelmä on luokiteltu A-luokan järjestelmäksi.
- Jos asiakastietoja tai potilastietoja käsittelevät tietojärjestelmät aiheuttavat riskin potilasturvallisuudelle asiasta ilmoitetaan valvontaviranomaisille sekä henkilölle, jota asia koskee. Ilmoitus tehdään Valviralle, mikäli poikkeama aiheuttaa merkittävän riskin potilasturvallisuudelle tai tietoturvalle.
- Tietosuojapoikkeamissa tehdään aina ilmoitus tietosuojavaltuutetulle ja rekisteröidyille

4.1 Tietoturvariskin hallinta

Tietoturvariskien hallinta on keskeinen osa organisaation tietoturvastrategiaa. Riskienhallinnassa tunnistetaan ja arvioidaan keskeiset uhat, kuten tietovuodot, kyberhyökkäykset, inhimilliset virheet, sisäiset uhkat sekä kolmansien osapuolten alihankkijoiden aiheuttamat riskit. Riskianalyysi auttaa organisaatiota arvioimaan todennäköisyydet ja vaikutukset kullekin riskille ja suunnittelemaan asianmukaiset torjuntatoimenpiteet.

Riskianalyysin avulla organisaatio laatii myös sosiaali- ja terveyspalveluiden yrityskohtaisen varautumissuunnitelman, jatkuvuudenhallinta- ja toipumissuunnitelman, jotka varmistavat toiminnan nopean palautumisen ja tietoturvan ylläpidon riskien toteutuessa. Tietoturvariskien hallinta on jatkuva prosessi, ja riskianalyysiä tulee päivittää säännöllisesti sekä aina merkittävien lainsäädännöllisten, teknologisten tai organisatoristen muutosten yhteydessä. Näin varmistetaan, että organisaation riskienhallinta vastaa muuttuvia uhkakuvia ja tietoturvavaatimuksia.

Kaikki riskienhallintaan liittyvät analyysit ja toimenpiteet dokumentoidaan tietoturvaraportointijärjestelmään, ja niiden toteutumista seurataan säännöllisesti sisäisten ja ulkoisten auditointien kautta. Tietosuojavaltuutetun ohjeita tietosuojasta ja tietoturvasta käytetään Alina hoivatiimin tietoturvasuunnitelman toteutuksessa Tietosuojavaltuutetun ohjeet

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

Alina hoivatiimin tietoturvasuunnitelmassa noudatetaan Euroopan unionin tietosuoja-asetuksia GDPR-info

5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

Asiakastietojen käsittelyn, tietojärjestelmien käytön sekä tietosuojan ja tietoturvan toteuttamisen koulutuksissa, ohjeistuksissa ja seurannassa toimitaan seuraavasti:

- Tietoturvallisuuden toimintamallien ja -tapojen perehdytyksestä vastaa yrityksen vastaava johtaja. Työntekijät perehdytetään aina työsuhteen alkaessa yrityksen tietoturvallisuuden periaatteisiin ja tietoturva koulutukset huomioidaan vuosittaisia koulutuksia suunniteltaessa. Työntekijöiden perehdytykseen sisältyy ketjun toimintamallin mukaan työntekijän oppaan sisällön läpikäynti, jossa tietoturva on yksi osa-alueista. Tietosuoja –ja tietoturva koulutuksia järjestää lisäksi Alinan IT-päällikkö yritysten johtajille. Yritysten vastaavat johtajat kouluttavat oman henkilöstön. Ketjun järjestämästä koulutuksesta on saatavilla myös tallenne jatkuvaan käyttöön.

- Käyttöjärjestelmien uusien versioiden kouluttamisesta vastaa Alinan IT-päällikkö yrityksien vastaaville johtajille, jotka jatkokouluttavat oman henkilöstönsä.
- Yrityksissä ylläpidetään kirjallista koulutussuunnitelmaa sekä raportoidaan koulutusten toteumaa vuositasolla.
- Koulutusten kustannuksista vastaa yrityksen johtaja. Ketju järjestää myös ilmaista koulutusta ja ohjausta yritysten johtajille.

5.1.1 Tietoturvakoulutuksen seuranta ja dokumentointi

Jokaisen työntekijän tulee suorittaa säännöllisesti tietoturvakoulutus, ja suoritukset tulee dokumentoida. Koulutuksen vaikuttavuutta ja työntekijöiden tietoturvaosaamisen kehittymistä arvioidaan säännöllisesti esimerkiksi tietoturva-aiheisilla testeillä, palautekyselyillä ja käytännön harjoituksilla. Arvioinnin tulokset raportoidaan ja käytetään koulutusten kehittämiseen.

Tietoturvan ja tietosuojan riskien kehittyessä nopeasti, henkilöstölle järjestetään erillisiä koulutuksia ajankohtaisista tietoturvauhista, kuten tietojenkalastelusta, kyberhyökkäyksistä ja muista uusista riskeistä. Nämä koulutukset varmistavat, että henkilöstö on valmiina tunnistamaan ja torjumaan nykyajan tietoturvauhkia.

Kaikki tietoturva- ja tietosuojakoulutukset dokumentoidaan, ja koulutuksen suorittaneet henkilöt kirjataan koulutussuunnitelmaan. Koulutusten toteutumista seurataan vuosittain, ja tiedot raportoidaan yrityksen johdolle ja tietoturvavastaavalle. Koulutukset kohdennetaan eri rooleihin siten, että jokainen työntekijä saa tehtävänsä ja vastuunsa mukaisen tietoturva- ja tietosuojakoulutuksen. Esimerkiksi yritysten johtajille ja esimiesten koulutuksissa keskitytään tietoturvan valvontaan ja henkilöstön ohjeistukseen.

Yrityksen johtaja vastaa koulutusten kustannuksista, ja ketjun tarjoama ilmainen koulutus ja ohjaus täydentävät yritysten omia koulutuksia. Koulutuksen järjestämisessä varmistetaan, että resursseja on riittävästi kattavan ja ajantasaisen koulutuksen tarjoamiseen

5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

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

- Tietojärjestelmän käyttäjälle löytyy tarpeelliset käyttöohjeet eri kielillä. Ohjeet löytyvät kaikille, joilla tunnukset järjestelmään.
- Yrityksen vastaavat henkilöt jakavat käyttöohjeet organisaation kaikille käyttäjille sähköisesti intranetin kautta tai suoraan sähköpostitse. Ohjeet varmistetaan olevan ajan tasalla ja helposti saatavilla, ja työntekijöille tarjotaan tarvittaessa henkilökohtaista opastusta
- Kaikki käyttöohjeet säilytetään keskitetyssä järjestelmässä, kuten yrityksen intranetissä, johon kaikilla järjestelmän käyttäjillä on pääsy. Ohjeet päivitetään automaattisesti aina, kun ohjelmistoihin tehdään päivityksiä.
- Jokainen työntekijä perehtyy työntekijä oppaaseen ja suorittaa perehdytyksen jälkeen testin, jonka tulokset dokumentoidaan osana yrityksen koulutussuunnitelmaa. Tulosten perusteella arvioidaan tarvittavat jatkokoulutukset tai ohjeistuksen tarkennukset, jotta jokaisen työntekijän tietojärjestelmäosaaminen on vaaditulla tasolla.

- Ohjeiden mukaisen käytön noudattamista seurataan säännöllisesti, ja valvonnan tukena käytetään sisäisiä auditointeja. Tarvittaessa annetaan lisäkoulutusta varmistaen, että kaikki työntekijät käyttävät järjestelmiä ohjeiden mukaisesti.
- Eri työtehtävissä ja rooleissa toimiville työntekijöille on oppaat, jotka tukevat asiakastietojen ja potilastietojärjestelmien käyttämisessä. Jokaisen yrityksen vastaava johtaja vastaa järjestelmien käyttöön perehdytyksestä.
- Roolikohtaiset oppaat räätälöidään eri tehtävissä toimivien työntekijöiden tarpeisiin, kuten asiakastietojen ja potilastietojärjestelmien käyttöön. Oppaissa käsitellään myös roolien mukaisia tietoturva- ja tietosuojakäytännön erityispiirteitä, jotta työntekijät ymmärtävät tehtäväänsä liittyvät vastuut.
- Tietojärjestelmätuottajat päivittävät käyttöohjeita ja toteuttavat ohjelmistojen versiopäivitykset.

6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

Alina ketjun jokaisessa yrityksessä on käytössä Domacare-asiakastietojärjestelmä. Kuvaus järjestelmästä on liitteessä

1. Asiakaslaskutuksessa ja palkanmaksussa on käytössä Visma Netvisor -taloushallintojärjestelmä, jonne tietoja siirtyy asiakastietojärjestelmä Domacaren rajapinnan kautta. Netvisor palvelun tietosuojaseloste liitteessä
2. Konsernin RAI-järjestelmää tukevan ohjelmiston tarjoaa hetkellä Vitec Raisoft Oy. Vitec Raisoft Oy tietosuojaseloste: RAIsoft tietosuojaseloste

Järjestelmien välillä olevan integraation avulla asiakkaan perus-, diagnoosi-, lääke- ja palvelumäärätiedot siirtyvät Domacaresta RAIsoftiin ja arviointitulokset sekä NHG-riskiluku RAIsoftista Domacare. Domacare-, Visma Netvisor- ja Raisoft-järjestelmien tietoturva varmistetaan muun muassa monivaiheisella tunnistautumisella / pääsynhallinnalla, jossa kullekin käyttäjälle määritellään tarkat käyttöoikeudet, ja järjestelmien käytön lokitietojen seurannalla. Kaikki käyttäjien tekemät toimet kirjataan lokitietoihin, joita seurataan säännöllisesti poikkeamien havaitsemiseksi.

Järjestelmien välisessä tiedonsiirrossa, kuten Domacare ja Raisoftin välillä, käytetään salattuja yhteyksiä (esim. HTTPS, TLS), jotta potilas- ja asiakastietojen turvallinen siirto varmistetaan. Tietojen käsittelyssä noudatetaan tietosuojalainsäädäntöä, ja siirrettävät tiedot minimoidaan vain välttämättömään.

Tietojärjestelmien tietoturvariskejä seurataan säännöllisesti osana organisaation riskienhallintaprosessia. Riskit, kuten tietomurrot, tietojen väärinkäyttö ja korruptoituminen, pyritään estämään ajantasaisilla suojausmekanismeilla, kuten palomuureilla, tunkeutumisen estojärjestelmillä ja säännöllisillä tietoturva-auditoinneilla. Kaikki järjestelmiä käyttävät työntekijät koulutetaan tietoturvakäytännöistä ja heille tarjotaan säännöllisiä tietoturvakoulutuksia, jotta he ymmärtävät, miten järjestelmiä käytetään turvallisesti ja miten suojata asiakkaiden tietoja jokapäiväisessä työssä.

Tietojen säilytys- ja poistokäytännöt on määritelty siten, että tiedot säilytetään ainoastaan niin kauan kuin se on lakisääteisesti tarpeellista. Vanhentuneet tai tarpeettomat tiedot poistetaan järjestelmistä turvallisesti, ja tiedon poistamisesta tehdään lokimerkintä, jota valvotaan säännöllisesti.

6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokka A1)

Domacare – asiakastietojärjestelmä
invian, tuki@domacare.fi
Domacare-järjestelmä kuuluu A1-luokkaan, kriittisimpään järjestelmät, jotka käsittelevät potilastietoja ja muita henkilötietojen erityisryhmiä. Kyseisissä järjestelmissä tietosuojan ja tietoturvan vaatimukset ovat kaikkein tiukimmat. Tarkempi kuvaus kohdassa 9.1

6.1.2. Muut asiakastietoja käsittelevät järjestelmät (luokka A2)

Raisoft - ohjelmisto toimintakyvyn sekä hoidon laadun ja vaikuttavuuden arviointiin ikäihmisten koti- ja pitkäaikaishoitoon, aikuisväestön mielenterveystyöhön ja kehitysvammahuoltoon sekä ennaltaehkäisevään työhön. **Vitec Raisoft Oy** Vaasantie 6 (iPark) 67100 Kokkola, puh**.** 020 778 9567.

ISO 9001:2015-sertifiointi tarkistuslinkki: DNV Certificate Checker
Raisoft-järjestelmä kuuluu myös A2-luokkaan, sillä se käsittelee asiakastietoja, mutta ei potilastietoja. Tietoturvavaatimukset ovat korkeat, mutta joustavammat kuin A1-luokassa. Järjestelmän turvallisuuden varmistamiseksi on hyvä lisätä tietosuojatoimenpiteet ja -politiikat. Tarkempi kuvaus kohdassa 9.2

6.1.3. Muut tietojärjestelmät (luokka B)

Visma Netvisor- taloushallintojärjestelmä. Visma Netvisor käsittelee taloushallinnon tietoja, kuten yrityksen kirjanpitoa, laskutusta ja palkanlaskentaa.

Visma
Karenslyst allé 56, 0277 Oslo, Norja, puh. 47 46 40 40 00
Visman yksityisyyttä koskevat päätökset tekee yritystasolla Visman tietosuojaneuvosto, jota valvoo ja johtaa tietosuojavastaava (DPO). Henkilötietojen käsittelystä vastuussa oleva rekisterinpitäjä on Visma-konserni ja sen tytäryhtiöt. Tarkempi kuvaus kohdassa 9.4

6.1.4. Tietojärjestelmien olennaisten vaatimusten täyttyminen

- Asiakastietolain 27 § mukaan osana tietoturvasuunnitelmaansa ketju osaltaan varmistaa hankinnoissa ja sopimuksissa, että tietojärjestelmien käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön.
- Käytössä olevan ja päivitettävän asiakastietojärjestelmän vähimmäisvaatimusten voimassaolo tarkistetaan Valviran tietojärjestelmärekisteristä.
- Tietojen ylläpidosta vastaa ketjun IT päällikkö.
- Tietojärjestelmien auditoiminen säännöllisesti on tärkeää, ja mahdolliset riskiarviot tulee toteuttaa puutteiden korjaamiseksi.
- Yhteistyö tietosuojaviranomaisten ja järjestelmätoimittajien asiantuntijoiden kanssa on olennaista, jotta voidaan varmistaa, että kaikki käytössä olevat järjestelmät täyttävät vaatimukset.

6.2. Tietojärjestelmien asennus, ylläpito ja päivitys

Tietojärjestelmien asennuksissa, ylläpidossa ja päivityksissä noudatetaan seuraavia toimintatapoja:

- Yrityksen johtaja vastaa tietojärjestelmien asennusprosessin valvonnasta ja varmistaa, että kaikki toimenpiteet toteutetaan asianmukaisesti.
- Ketju toimittaa tarvittavat asennusohjeet ja tarjoaa ohjausta asennustoimenpiteiden toteuttamiseksi.
- Ulkopuolisten henkilöiden pääsy järjestelmien asentamiseen on estetty, ja laitteet sekä järjestelmät suojataan käyttäjäkohtaisilla salasanoilla sekä muilla pääsynhallintakäytännöillä.
- Järjestelmäpäivityksistä ja versiotestauksista vastaa ohjelmistotuottaja.
- Versiopäivitysten käyttöönotosta ja tiedottamisesta vastaa ohjelmistotuottaja. Isommissa versiopäivityksissä testaukseen osallistuu myös ketjun nimeämät yritykset ennen käyttöönottoa.
- Asennus-, ylläpito- ja päivitystoimenpiteitä suorittavilta henkilöiltä edellytetään riittävää ammatillista osaamista tai asianmukaista koulutusta, jotta varmistetaan järjestelmien turvallinen käsittely. Asennustoimenpiteitä saa suorittaa ketjun IT-päällikkö sekä yrityksen vastaava johtaja ketjun IT-päällikön ohjauksessa.
- Yrityksessä vastaava johtaja vastaa käytössä olevien laitteiden asennuksesta ja päivittämisestä. Laitteet ovat suojattu pääkäyttäjä-tunnuksilla, joilla asennukset suoritetaan. Asennusohjeet tulevat ketjulta.
- Asiakastietojärjestelmän osalta Myneva suorittaa järjestelmäpäivitykset. Päivityksen ajankohdasta tiedotetaan käyttäjiä.
- Asiakastietojärjestelmän uusien versioiden testauksista vastaa järjestelmätuottaja Myneva.
- Tietojärjestelmän luotettavuus arvioidaan tietojärjestelmäkuvauksen, tietosuojaselosteen, sertifikaattien ja käytännön kokemuksen perusteella.
- Järjestelmissä on määritelty tunnusten asettaminen kirjautumisessa ja tunnusten automaattinen tallennus on kielletty.
- Tietojärjestelmä tuottaja vastaa tietojärjestelmä päivityksistä ja ohjelmiston kehittämisestä vaatimusten mukaiseksi Sosiaali- ja terveysalan asiakas- ja potilastietojen käsittelyssä. Ketjun IT-päällikkö vastaa tietojärjestelmien asentavien henkilöiden perehdytyksestä ja ohjauksesta. Yrityksen johtaja vastaa tietojärjestelmien käyttäjätunnuksista ja turvallisen käytön varmistamisesta yksikössä.
- Käytössä olevaan asiakastietojärjestelmään sisältyy integraatio kantakirjaamiseen, Netvisor taloushallinnon järjestelmään, hyvinvointialueen Parasta Palvelua palvelusetelijärjestelmään sekä Raisoft järjestelmään.
- Säännölliset tarkastukset ja auditoinnit suoritetaan, jotta varmistetaan, että järjestelmien asennus, ylläpito ja päivitys toteutetaan suunnitelmien mukaisesti. Kaikki asennus-, ylläpito- ja päivitystoimenpiteet dokumentoidaan huolellisesti, jotta voidaan varmistaa jäljitettävyys ja noudattamisen toteaminen.

6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

Tietojärjestelmien ja laitteiden käyttäjiä ja käyttäjäryhmiä hallinnoidaan seuraavasti:

- Asiakastietojärjestelmien käyttäjäryhmät löytyvät ketjun oppaista. Käyttäjäluetteloa hallinnoidaan yrityksittäin. Yrityksen vastaava johtaja pitää yllä ajantasaista luetteloa käyttäjistä. Käyttäjäluetteloa tarkistetaan ja päivitetään säännöllisesti, vähintään kerran kuukaudessa.
- Yrityksessä pidetään yllä ajantasaista luetteloa laitteiden käyttäjistä. Luettelon ylläpitämisestä vastaa yrityksen vastaava johtaja. Luettelo pidetään turvallisessa ympäristössä, jotta käyttäjätiedot eivät ole alttiita tietovuodoille.
- Käyttöoikeuksista Kanta-palveluiden käyttöön pidetään ajantasaista luetteloa sähköisesti. Tämän luettelon ylläpidosta vastaa yrityksen vastaava johtaja.
- Käyttäjäluetteloita Ketjun sähköpostitileihin ja Intran käyttöön ylläpitää Alina ketjun IT-päällikkö. IT-päällikkö varmistaa, että luetteloiden tietoturva ja saatavuus ovat kunnossa.
- Käyttäjäluettelot ovat yrityksen vastaavan johtajan sekä Alinan ketjun IT-päällikön vastuualueella. Molemmat osapuolet tekevät yhteistyötä varmistaakseen käyttäjäluetteloiden ajantasaisuuden.

6.3.1 Käyttöoikeuksien ja käyttövaltuuksien osalta noudatetaan seuraavia toimintatapoja

- Käyttövaltuuksien hallintaan liittyvät erilaiset roolit ja henkilöt, jotka eri rooleissa toimivat (käyttöoikeuden hakeminen, myöntäminen, muuttaminen, peruminen, poistaminen) on määritelty selkeästi. Roolit sisältävät käyttöoikeuden hakijan, myöntäjän ja valvojan.
- Käyttöoikeuksien ajantasaisesta hallinnasta vastaa yrityksen vastaava johtaja. Johtaja saa ohjausta asiakastietojärjestelmän käyttöoikeuksien hallintaan Alina ketjun omalta IT-päälliköltä.
- Käyttövaltuuksien hakemisen, myöntämisen, seurannan, muuttamisen, tarkistamisen/varmistamisen ja poistamisen käytännöt:
    - Yrityksen vastaava johtaja vastaa käyttäjätunnusten luomisesta ja poistamisesta. Tämä varmistaa, että käyttäjätunnukset ovat aina ajan tasalla ja oikein määritettyjä.
    - Sijaisten henkilöllisyystodistus sekä ammattipätevyys tarkistetaan ennen työsuhteen muodostamista ja käyttäjätunnusten luomista. Tarkistukset dokumentoidaan ja säilytetään turvallisesti.
    - Käyttäjätunnukset passivoidaan ketjun ohjeistuksen mukaisesti siinä vaiheessa, kun henkilön työsuhde on päättynyt. Tätä prosessia valvotaan säännöllisesti.
    - Käyttöoikeuksia myöntää yrityksen vastaava johtaja ja ketjutasolla Alinan IT-päällikkö. Molemmat varmistavat, että käyttöoikeudet myönnetään vain tarpeen mukaan ja että niitä tarkistetaan säännöllisesti.
    - Kiireellisissä käyttäjätunnusten poistamistilanteissa ensisijaisesti poistot tehdään vastaavan johtajan toimesta. Tarvittaessa Alina ketjun IT-päällikkö avustaa poistoissa. Poistoja dokumentoidaan, ja tarvittaessa tehdään raportointi asianomaisille tahoille.
    - Käyttöoikeuksia myöntää yrityksen vastaava johtaja. Kantapalveluihin käyttöoikeuksia myöntää ketjun Alinan IT. Kantapalveluiden käyttöoikeudet tarkistetaan säännöllisesti, ja niiden ajantasaisuus varmistetaan.

6.3.2 Käyttäjien tunnistautumisessa ja todentamisessa noudatetaan seuraavia käytäntöjä

- Työasemien kirjautumista valvoo yrityksen vastaava johtaja. Työntekijät käyttävät työasemia vain toimipisteessä heille annetuilla tunnuksilla. Työasemille asennettuihin järjestelmiin on pääsy henkilökohtaisten tunnusten avulla. Kirjautumistietoja seurataan ja auditoidaan säännöllisesti yrityksen vastaavan johtajan toimesta. Työasemat sijaitsevat lukituissa tiloissa, joihin pääsy on vain työntekijöillä. Työntekijöille luovutetuista toimipisteen avaimista pidetään yllä ajantasaista ja tarkkaa luetteloa, ja avaimet säilytetään turvallisessa paikassa.
- Mobiililaitteisiin asennettuihin järjestelmiin annetaan henkilökohtaiset käyttäjätunnukset. Työntekijä on vastuussa ilmoittamisesta, mikäli käyttäjätunnuksiin liittyy tietovuotoriski. Yrityksen vastaava johtaja voi tiedon saatuaan välittömästi muuttaa tunnusten salasanoja, ja kaikki muutokset dokumentoidaan asianmukaisesti.
- Vahvaa sähköistä tunnistautumista käyttää yrityksen allekirjoitusoikeudellinen vastaava johtaja, joka vastaa myönnetyistä Suomi.fi-oikeuksien antamisesta yritysasioiden hallintaan sähköisen tunnistautumisen avulla. Tämä käytäntö varmistaa, että allekirjoitusoikeudet myönnetään vain valtuutetuille henkilöille ja että niiden käyttö on jäljitettävissä.
- Yrityksen vastaava johtaja pitää yllä ajantasaista luetteloa myönnetyistä käyttäjätunnuksista ja salasanoista. Tämä luettelo tarkistetaan ja päivitetään säännöllisesti, ja sen tiedot suojataan asianmukaisesti.
- Yhteiskäyttöisiä tunnuksia on käytössä toimipisteen työasemilla. Näiden tunnusten käyttöön liittyvät säännöt ja käytännöt on dokumentoitu, ja tunnuksia vaihdetaan säännöllisin väliajoin, vähintään kolmen kuukauden välein. Yhteiskäyttöisten tunnusten käyttöä valvotaan tiukasti, jotta estetään niiden väärinkäyttö.
- Pääkäyttäjäoikeuksia hallinnoi yrityksen vastaava johtaja sekä tarvittaessa ketjun IT-päällikkö. Virhetilanteissa otetaan välittömästi yhteyttä ketjun IT-päällikköön. Kaikki virhetilanteet dokumentoidaan ja niiden käsittelyyn liittyvät toimenpiteet kirjataan ylös analysoitavaksi myöhemmin.

6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Asiakastietoja käsittelevien järjestelmien pääsynhallintaa ja käytön seurantaa toteutetaan seuraavasti:

- Yrityksen vastaava johtaja tekee säännöllisin väliajoin lokiseurantaa omasta henkilöstöstä Domacare-järjestelmän osalta. Seurantaprosessi sisältää lokitietojen analysoinnin, jossa tarkastellaan käyttäjien kirjautumisia, tietojen muokkauksia ja muita olennaisia tapahtumia. Jokainen suoritetun seurannan tulokset dokumentoidaan ja arkistoidaan, mikä mahdollistaa myöhemmän tarkastelun ja mahdollisten poikkeamien selvittämisen.
- Lokitiedostojen koonti tietojärjestelmästä tehdään säännöllisin väliajoin asiakastietojen käytön seurantaa varten. Tämä prosessi kattaa lokitietojen keräämisen ja analysoinnin, johon sisältyy mahdollisten poikkeamien, kuten luvattomien pääsyjen tai epäilyttävän toiminnan, tunnistaminen. Käyttöön liittyvät poikkeamat raportoidaan ja käsitellään henkilöstön kanssa tiimipalaverien yhteydessä, jossa keskustellaan myös toimenpiteistä ongelmien ratkaisemiseksi ja ennaltaehkäisemiseksi.
- Yrityksen tietosuojavastaava vastaa lokitietojen seurannasta ja raportoinnista sekä asiakkaiden tietopyyntöihin vastaamisesta. Lokitietoja seurataan jatkuvasti, koonti tarkastetaan vähintään joka kuukausi. Lokitietoja seuraa yrityksen vastaava johtaja ja muut nimetyt operatiivisen toiminnan vastuutehtävissä toimivat työntekijät.

6.4.1 Yrityksen lokitietojen seurannan ja tietopyyntöihin vastaamisen vastuut

Tietosuojavastaava, yrityksen vastaava johtaja, nimetty yksikön johtaja: Lokiraporttien seuraaminen ja koonti kuukausittain. Henkilöstön ohjeistus ja poikkeamien korjaus. Tietopyyntöihin vastaaminen.

Tiimiesihenkilöt, palvelukoordinaattorit, sihteerit: Jatkuva viikoittainen lokitietojen seuraaminen. Raportointi yrittäjille mahdollisista poikkeamista. Tietopyyntöjen välittäminen yrityksen vastaavalle johtajalle. Mainitut henkilöt osallistuvat tarvittaessa lokitietojen analysointiin ja poikkeamien käsittelyyn tiimipalavereissa.

- Virhetilannetta epäiltäessä tai epäillyn rikkomuksen sattuessa tietosuojavastaava arvioi minkä tasoinen riski on. Tietosuojavaltuutettu dokumentoi tietoturvallisuuteen liittyvän poikkeaman sekä ilmoittaa sekä valvontaviranomaiselle sekä myös mahdolliselle asianomaiselle, jota mahdollinen tietoturva riski koskee. Poikkeamat virhetilanteissa, epäillyissä rikkomuksissa ja epäasianmukaisessa käytöksessä käsitellään henkilöstön kanssa. Poikkeamien juurisyyt, korjaavat toimenpiteet sekä ohjeistukset kirjataan tiimipalaverin muistioon. Raportointi virhetilanteista ja niiden käsittelytavoista tapahtuu säännöllisesti tiimipalavereissa, jotta kaikki osapuolet ovat tietoisia mahdollisista ongelmista.
- Uudet työntekijät perehtyvät työntekijän käsikirjaan, jossa ohjeistetaan tietoturvaan liittyvistä ohjeista ja toimintavoista. Perehdytysprosessissa korostuu myös käytännön esimerkit ja mahdolliset riskit. Yrityksen vastaavan johtajan vastuulla on perehdyttää asiakastietojärjestelmien tekniset käytännöt ei-sallitun käytön ehkäisemiseksi.

6.5 Tietojen anonymisointi ja pseudonymisointi

Tietojen anonymisointi ja pseudonymisointi ovat keskeisiä tapoja varmistaa, että potilastietoja käsitellään tietosuojalainsäädännön mukaisesti. Pseudonymisointi tarkoittaa tietojen käsittelyä siten, ettei tietoja voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Anonymisointi puolestaan tarkoittaa, että tiedot muutetaan siten, ettei niistä voi tunnistaa henkilöä edes epäsuorasti. Molemmat menetelmät ovat tärkeitä tietoturvatoimenpiteitä, ja niiden käyttöä säädellään tarkasti tietosuojalakien mukaisesti.

6.5.1 Käytännön esimerkkejä tietojen anonymisoinnista ja pseudonymisoinnista

6.5.1.1. Pseudonymisointi

- Tilanne: Terveydenhuollon organisaatio käyttää potilasrekisteriä, jossa on paljon henkilökohtaisia tietoja, kuten nimiä ja osoitteita.
- Esimerkki: Potilaan tiedot tallennetaan järjestelmään pseudonymisoituna (esim. "Potilas001"). Kaikki viestit, laskut ja muistutukset lähetetään tämän koodin avulla, jolloin varsinaisia henkilötietoja ei paljasteta. Vain valtuutetut työntekijät voivat yhdistää koodin alkuperäisiin potilastietoihin erillisessä tietokannassa, jossa on rekisteröidyt nimet ja tiedot.

6.5.1.2. Anonymisointi

- Tilanne: Terveydenhuollon yksikkö haluaa kerätä palautetta potilailta hoidon laadusta.
- Esimerkki: Potilaille lähetetään kysely, jossa kysytään heidän kokemuksiaan hoidosta. Kyselyssä ei kysytä nimiä tai muita tunnistettavia tietoja, ja vastaukset analysoidaan täysin anonymisoituna. Tulokset esitetään raporttina, jossa näkyy vain yleiset suuntaukset ja keskiarvot, ilman että yksittäisten potilaiden tietoja voidaan jäljittää.

6.5.1.3. Tietopyynnöt ja lokiseuranta

- Tilanne: Potilastietojen lokitietoja tarkastellaan tietosuojan varmistamiseksi.
- Esimerkki: Kun potilastietoja tarkastellaan tietopyyntöjen yhteydessä, tietosuojavastaava voi käyttää pseudonymisoituja lokitietoja arvioidakseen, kuka on käyttänyt järjestelmää ja milloin. Tällöin henkilötietoja ei paljasteta, mutta lokitiedot auttavat varmistamaan, että tietosuojakäytännöistä pidetään kiinni.

6.5.1.4. Koulutus ja perehdytys

- Tilanne: Uudet työntekijät perehdytetään potilastietojen käsittelyyn.
- Esimerkki: Työntekijöille annetaan koulutusta, jossa he oppivat käyttämään potilastietojärjestelmiä pseudonymisoitujen esimerkkitietojen avulla. Näin he voivat harjoitella tietojen syöttämistä ja käsittelyä ilman, että he joutuvat käsittelemään todellisia potilastietoja.

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

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

- Toimitilat ovat lukollisia, ja niihin pääsee vain avaimella. Asiakkaiden avaimet ovat lukitussa avainkaapissa toimitiloissa.
- Laitteet ovat salasanasuojattuja ja niissä on aikaraja istunnolle. Näytöt on sijoitettu niin, ettei ulkopuolisilla ole näköyhteyttä. Näytönsuojakalvoja käytetään tarpeen mukaan.
- Laitteissa ja järjestelmissä on omat aikakatkaisu määritykset, joita käyttäjät voivat muokata itse.
- Yrityksen vastaava johtaja vastaa laite- ja ohjelmistoasennuksista. Ohjelmistoihin ja asennusohjeisiin pääsy on rajattu henkilökohtaisilla käyttäjätunnuksilla.
- Käytössä olevat ulkoiset kovalevyt ja muistitikut ovat vain yrityksen hankkimia. Laitteet ovat salasanasuojattuja, mikä estää ulkopuolisten laitteiden pääsyn.
- Tulostimet sijaitsevat toimipisteessä, joihin ulkopuolisilla ei ole pääsyä. Vain työntekijät pääsevät toimitiloihin toimipaikan avaimen avulla. Työntekijöille on annettu ohjeistusta siitä, ettei ulkopuolisia saa päästää toimitiloihin.
- Paperiset asiakastiedot säilytetään toimitiloissa lukituissa kaapeissa suojassa ulkopuolisilta. Tiedot tallennetaan paloturvallisesti myös liitteeksi asiakastietojärjestelmään asiakkaan omiin tietoihin.
- Paperitulosteet hävitetään säilytysajan päättymisen jälkeen paperisilppurilla, ja suurten määrien hävitykset hoidetaan lukittavalla säilytysastialla ulkopuolisen tahon maksullisen tietoturvallisen kierrätyksen avulla. Yrityksessä ohjeistetaan työntekijöitä tulosteiden käsittelystä ja tulostamisen turvallisuuden periaatteista.

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

7.2.1 Työasemat ja mobiililaitteet

Yrityksen vastaava johtaja vastaa virustorjunnan toimivuudesta ja päivityksistä käytössä olevilla työasemilla. Virustorjunnan toimivuuden varmistamiseksi yritykset saavat tarvittaessa tukea ketjun IT-päälliköltä.

Virustorjunnan toimivuuden varmistamiseksi:

- **Säännöllinen tarkastus:** IT-päällikkö suorittaa säännöllisiä tarkastuksia virustorjuntaohjelmiston toiminnasta ja päivityksistä.
- **Raportointi:** Virustorjuntaohjelmasta saadaan kuukausittaiset raportit, jotka tarkastetaan ja dokumentoidaan.
- **Käyttäjätuki:** Tarvittaessa työntekijät voivat ottaa yhteyttä IT-tukeen virustorjuntaan liittyvissä kysymyksissä.

Mobiillilaitteet ovat suojattu PIN-koodilla tai salasanalla. Käytössä olevista SIM-korteista pidetään listaa yrityksessä.

Mobiililaitteiden suojaus varmistetaan seuraavasti:

- **PIN-koodit ja salasanat:** Kaikilla mobiililaitteilla on oltava PIN-koodi tai salasana. Salasanat vaihdetaan säännöllisesti.
- **Laitehallintaohjelmisto:** Käytössä on laitehallintaohjelmisto, joka mahdollistaa laitteen etäpuhelun ja tietojen tyhjennyksen, jos laite katoaa tai varastetaan.
- **Käyttöehdot:** Työntekijöitä ohjeistetaan säännöistä ja käytännöistä, jotka liittyvät mobiililaitteiden käyttöön.

7.2.2 Käyttöympäristön tukipalvelut

Yrityksen vastaava johtaja huolehtii käyttöympäristön tukipalveluista, kuten käyttöjärjestelmien päivityksistä.

Käyttöjärjestelmien päivitykset hallitaan seuraavasti:

- **Automaattiset päivitykset:** Kaikissa työasemissa on käytössä automaattiset päivitykset, jotka varmistavat uusimpien tietoturvapäivitysten asentamisen.
- **Päivityssuunnitelma:** IT-päällikkö laatii ja ylläpitää päivityssuunnitelmaa, jossa on aikataulu ja vastuuhenkilöt päivityksille.
- **Seuranta:** Päivitysten toimivuutta seurataan, ja käyttäjiltä kerätään palautetta mahdollisista ongelmista.

7.2.3 Käyttöympäristön kokonaisuuden kuvaus

Yrityksen vastaava johtaja saa perehdytyksen ja ohjausta ketjun IT-päälliköltä käyttöympäristön tukipalveluihin.

Käyttöympäristön tukipalveluissa tapahtuva ohjaus varmistetaan seuraavasti:

- **Säännölliset kokoukset:** IT-päällikkö ja yrityksen vastaava johtaja järjestävät säännöllisiä kokouksia, joissa käsitellään käyttöympäristön kehittämistä ja tukipalveluiden toimivuutta.
- **Perehdytysmateriaalit:** Uusille työntekijöille annetaan perehdytysmateriaalit, jotka sisältävät ohjeet ja toimintatavat tukipalveluista.

- **Palautejärjestelmä:** Työntekijöiltä kerätään palautetta tukipalveluista, ja tarvittaessa palveluja kehitetään saadun palautteen perusteella.

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

Alusta- ja verkkopalveluiden tietoturvallisuudesta huolehditaan seuraavasti

7.3.1 Yleistä

- Luettelot käytössä olevista alusta- ja verkkopalveluista sekä niiden hallinnan vastuukysymykset: Organisaatio listaa käytössä olevat alusta- ja verkkopalvelut. Listan ylläpitämisestä vastaa ketjun IT-päällikkö, ja siinä määritellään myös hallintaan liittyvät vastuukysymykset tuottajan ja tilaajan välillä.
- Tietosuojasäädösten lainmukaisuus osoitetaan omassa toiminnassa käytettäessä ulkoisten palveluntuottajien alusta- ja verkkopalveluita. Tämä huomioidaan sopimuksissa ilmaistavien tietoturvallisuusvaatimusten lisäksi myös tarkistamalla kaikki tietoturvallisuuden todistavat asiakirjat.
- Varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä on kirjattu valmiussuunnitelmaan. Tässä suunnitelmassa määritellään toimenpiteet, vastuut ja viestintäkanavat poikkeustilanteissa.

7.3.2 Palvelimet ja palvelinympäristöt

- Alina Hoivatiimin yrityksissä ei ole omia palvelimia. Kaikki palvelut hankitaan ulkoisilta palveluntuottajilta, ja niiden tietoturvastandardeja arvioidaan säännöllisesti.

7.3.3 Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet

- Yrityksen vastaava johtaja sopii tietoliikenneoperaattorin ja tietoliikenneturvaan liittyvät vastuut, yhteydenotot ja menettelyt häiriötilanteisiin.

Yrityksen toimintamalli:

- Langattomat verkot ovat salasanasuojattuja ja niiden käyttöoikeudet rajoitetaan vain tarvittaville henkilöille. Verkkojen tietoturvaa valvotaan säännöllisesti ja niiden suojausasetuksia päivitetään tarpeen mukaan.

7.3.4 Etäyhteydet ja niiden tietoturva

- Etätyöskentelyssä on luvallista käyttää samoja tietojärjestelmiä kuin toimistotiloissa, mutta on huomioitava oman työhuoneen rauhoittaminen. Työntekijöiden on myös varmistettava, että heidän laitteensa ovat ajantasaisia ja suojattuja.
- Työasemilla saa käyttää internetin kautta sellaisia palveluita, jotka liittyvät työntekijän työskentelyyn. Internetin käyttöä valvotaan ja käytön ohjeet annetaan selkeästi.

7.3.5 Pilvipalvelut, pilvipohjaiset ratkaisut

- Yrityksellä on käytössään Teams videokokouksia varten, lisäksi ketjun toimittama materiaali tallennetaan Teams-järjestelmän pilvipalveluun. OneDrive kuuluu jokaiseen Alina-sähköpostitiliin, johon sisältyy käyttäjäkohtainen pilvipalvelu.
- Tiedot eivät siirry kolmansiin maihin. Noudatamme sopimuksissa EU:n yleistä tietosuoja-asetusta.

7.3.6 Tietolähteet:

- 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

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

- Kanta-palveluiden käyttöönoton yhteydessä järjestelmätoimittaja perehdyttää ja kouluttaa käyttäjät tuntemaan Kanta-palvelut. Tämä varmistaa tietoturvallisen käytön, ja lisäksi ketjujohtoa perehdytetään antamaan säännöllistä ohjausta palveluiden käyttöön. Yrityksen johtaja vastaa kantapalveluiden käyttäjien koulutuksesta ennen työskentelyn aloittamista. Perehdytysohjelman osa-alueena on Kanta-palveluiden käyttö ja tietoturvallisuus.
- Toimintamalli Kanta-palvelujen käytön aktiivisesta seurannasta tulee tarkentamaan sosiaalihuollon kantapalveluiden käyttöönottovaiheessa.
- Kanta-palveluja käyttävien järjestelmien kirjautumiseen on käytettävä henkilökohtaisia tunnuksia.
- Sote-organisaatiorekisteritietojen tai IAH-koodiston tietojen tarkastaminen:
    - organisaatio tarkastaa tiedot kansallisen koodistopalvelun Sote-organisaatiorekisteristä
    - 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 seurataan lokitietojen avulla. Lokitietoja seuraa yrityksen johtaja kuukausittain ja mahdolliset muut nimetyt operatiivisen toiminnan vastuuhenkilöt jatkuvasti.
- Kanta-palvelut otetaan käyttöön integroituna asiakastietojärjestelmään ja järjestelmän käyttöoikeuksien myöntämisestä yrityksen johtaja pitää yllä ajantasaista listaa.
- Sosiaalihuollon ja terveydenhuollon kirjaukset eriytetään toisistaan. Työntekijät koulutetaan rakenteelliseen kirjaamiseen ja rekisterien erottamiseen.
- Vuosittain tarkistetaan A-luokan tietojärjestelmän vaatimustenmukaisuus rekisteristä ja todistus tietoturvallisuuden arvioinnista pyydetään ajankohtina, jolloin rekisteriin on merkitty seuraava arvioajankohta.
- Kanta-palveluissa edellytettyihin määrittelyihin liittyvät käytännöt on vahvistettava.
- Vuosittain tarkistetaan B-luokan tietojärjestelmän vaatimustenmukaisuus rekisteristä ja todistus tietoturvallisuuden arvioinnista pyydetään ajankohtina, jolloin rekisteriin on merkitty seuraava arvioajankohta.

- Varmistetaan rekisteristä, että järjestelmä täyttää THL:n määräyksen mukaiset tietoturvallisuuden olennaiset vaatimukset ja on sertifioitu.
- Hyväksytystä tietoturvallisuuden arvioinnista myönnetään tietoturvallisuustodistus, jonka organisaatio tarkistaa. Luokan A2 ja A3 tietojärjestelmien sertifiointiin kuuluu yhteistestaus Kelan kanssa. Yhteistestauksessa varmistetaan, että järjestelmä toimii yhdessä Kanta-palvelujen ja muiden niihin liittyneiden järjestelmien kanssa ja täyttää yhteentoimivuusvaatimukset.
- Sopimuksissa huomioidaan, että järjestelmän tuottajan tulee korjata järjestelmän puutteet, jos käytössä olevalta järjestelmältä peruutetaan todistus tietoturvallisuuden arvioinnista. Organisaatio vaatii järjestelmän tilaajana, että järjestelmä täyttää vaaditut ominaisuudet ja korjaa välittömästi puutteet.

9. Tietojärjestelmäkohtaiset tarkemmat kuvaukset, ohjeet ja suunnitelmat

Tietojärjestelmäkohtaiset tarkemmat kuvaukset, ohjeet ja suunnitelmat on laadittu Valviran Sosiaali- ja terveydenhuollon tietojärjestelmien luokittelun mukaisesti. Luokittelun perusteet ja tarkemmat tiedot ovat saatavilla osoitteessa Valviran sivu.

Tämä viittaus varmistaa, että suunnitelma pohjautuu ajantasaisiin ja virallisiin tietojärjestelmien luokittelustandardeihin.

9.1 Järjestelmät A1-luokka

Luokkaan A1 kuuluu kaikkein kriittisimmät järjestelmät, jotka käsittelevät potilastietoja ja muita henkilötietojen erityisryhmiä. Kyseisissä järjestelmissä tietosuojan ja tietoturvan vaatimukset ovat kaikkein tiukimmat. Esimerkkinä käytettävä järjestelmä Domacare. Tässä luokassa vaatimustenmukaisuuden varmistamiseksi käytetään säännöllisiä auditointeja ja koulutuksia käyttäjille.

9.2 Järjestelmät A2-luokka

Luokkaan A2 kuuluu järjestelmät, mitkä ovat vähemmän kriittisiä kuin A1 mutta jotka edelleen käsittelevät luottamuksellisia tietoja, kuten asiakastietoja tai muita henkilötietoja. Tietoturvavaatimukset ovat korkeat, mutta hieman joustavammat kuin A1-luokassa. Esimerkkinä käytettävä järjestelmä Raisoft. Tässä luokassa järjestelmien käyttäjien on myös osallistuttava säännöllisiin tietoturvakoulutuksiin.

9.3 Järjestelmät A3-luokka

Näihin kuuluvat järjestelmät, jotka käsittelevät henkilötietoja, mutta tiedot eivät ole yhtä arkaluonteisia kuin A1- tai A2-luokassa. Tietoturva- ja tietosuoja-asetukset ovat silti tärkeitä, mutta ne voivat olla joustavampia. Käyttäjien on kuitenkin varmistettava, että henkilötietojen käsittelyssä noudatetaan voimassa olevia säädöksiä ja ohjeistuksia.

9.4 Järjestelmät B-luokka

Kyseessä järjestelmät, jossa vähemmän arkaluonteisia tietoja käsittelevät järjestelmät (esim. organisaation sisäiset tiedot). Esimerkkinä käytettävä järjestelmä Visma Netvisor käsittelee taloushallinnon tietoja, kuten yrityksen kirjanpitoa, laskutusta ja palkanlaskentaa. Vaikka tämä järjestelmä käsittelee henkilötietoja (palkanlaskennassa) ja muita liiketoiminnan kannalta tärkeitä

tietoja, se ei sisällä arkaluonteisia potilas- tai terveystietoja. Näin ollen se kuuluu B-luokkaan, jossa tietosuoja- ja tietoturvavaatimukset ovat edelleen merkittävät, mutta eivät yhtä tiukat kuin A-luokan järjestelmissä.

9.5 Järjestelmät luokittelemattomat ohjelmistot ja sovellukset

Järjestelmät, jotka eivät sisällä arkaluonteisia tietoja, mutta tukevat toimintaa. Microsoft Office365 on yleinen toimistosovelluspaketti, jota käytetään sähköpostiin, dokumenttien hallintaan, ja viestintään. Se ei sisällä itsessään arkaluonteisia tietoja, mutta se voi toimia alustana, jolla arkaluonteisia tietoja käsitellään (esim. sähköpostin kautta). Tämä järjestelmä kuuluu luokittelemattomat ohjelmistot ja sovellukset kategoriaan, koska se ei itsessään ole kriittinen tai arkaluonteisia tietoja käsittelevä järjestelmä, mutta sen turvallinen käyttö on silti tärkeää.