

Viludent Oy

Tietoturvasuunnitelma

9.7.2026, versio 1.0

Laatija: Viludent Oy

Hyväksynyt: Vilma Sääski

Sisällys

1. Tietoturvasuunnitelman käyttötarkoitus	3
2. Tietoturvasuunnitelman kohde ja päivityskäytännöt	3
3. Yleiset tietoturvakäytännöt	4
4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta	4
5. Henkilöstön koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturallinen käyttäminen	4
5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen	5
5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö	5
6. Tietojärjestelmien tietoturvakäytännöt	5
6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen	6
6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3)	6
6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1)	6
6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)	6
6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta	6
6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen	6
6.2. Tietojärjestelmien asennus, ylläpito ja päivitys	6
6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt	7
6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt	7
7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt	8
7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta	8
7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta	8
7.3. Alusta- ja verkkopalvelujen tietoturallinen käyttö tietosuojan ja varautumisen kannalta	9
8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt	9
9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat	10
9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat)	10
9.2. Järjestelmät X (luokkaan A1 kuuluvat)	10
9.3. Järjestelmät Y (luokkaan B kuuluvat)	10
9.4. Järjestelmät Z (muut järjestelmät, jotka eivät kuulu luokkiin A tai B)	10

1. Tietoturvasuunnitelman käyttötarkoitus

Tämä dokumentti on Viludent Oy:n tietoturvasuunnitelma. Tietoturvasuunnitelman käyttötarkoitus on täyttää uuden asiakastietolain¹ 703/2023 77 §:n ja THL:n määräyksen 3/2024 mukaiset velvoitteet. Suunnitelma kokoaa yhteen palvelunantajalta, apteekilta, välittäjältä ja Kansaneläkelaitokselta edellytettävät selvitykset ja vaatimukset.

Yhtiön johto päivittää Tietoturvasuunnitelmaa Yhtiön käyttämien asiantuntijoiden avulla säännöllisesti. Tietoturvasuunnitelman laadinnan ja noudattamisen vastuu on sosiaali- ja terveydenhuollon palvelunantajan vastaavalla johtajalla asiakastietolain 78 §:n mukaisesti.

2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat:

- Nimi: Viludent Oy:
- Y-tunnus: 3586803-7
- Vastuuhenkilö/johtaja: hallituksen jäsen Vilma Sääski
- Toimipaikat/palveluyksiköt: Viludent Oy – Liikkuva hammashoidon vastaanotto
- Suunnitelman piiriin kuuluvat alihankkijat ja sopimuskumppanit: -

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

- Suunnitelman ja sen päivittämisen vastuuhenkilö: hallituksen jäsen, tietoturvavastaava Vilma Sääski.
- Suunnitelman toteuttamisen vastuuhenkilöt: Vilma Sääski.
- Tarkistus- ja päivityskäytännöt: Yhtiö huolehtii henkilöstön perehdyttämisestä tietoturvasuunnitelmaan. Yhtiö huolehtii, että mahdollisesti tulevaisuudessa työntekijöitä rekrytoitaessa sen työntekijät saavat näihin ohjeisiin ja käytäntöihin riittävän perehdytyksen. Yhtiö ja tietosuojavastaava tarkastelevat ja päivittävät tietoturvasuunnitelmaa tarvittavilta osin vähintään kerran vuodessa. Laki- ja sääntelymuutoksista johtuvat päivitykset ja muutokset tehdään sääntelymuutosten voimaantulosäädösten puitteissa. Tarvittaessa Yhtiö käyttää näissä toimissa apunaan asiantuntijoita.
- Suunnitelman seuranta ja seurannan dokumentointi: Yhtiö ja tietosuojavastaava tarkastelevat suunnitelman toteutumista säännöllisesti vähintään kerran vuodessa. Tarkastelun yhteydessä Yhtiö laatii tietosuojavastaavan johdolla tietoturvasuunnitelman toteutumista ja mahdollisia päivitystarpeita kuvaavan dokumentin.
- Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä: hankittaessa ja päivitettäessä tietojärjestelmiä otetaan huomioon tietoturvasuunnitelman sekä soveltuvan lainsäädännön asettamat vaatimukset ja ohjeet.

¹ Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä,
<https://www.finlex.fi/fi/laki/alkup/2023/20230703#Pidm46494958192992>

- Päätös suunnitelman hyväksymisestä ja käyttöönotosta: tietoturvasuunnitelman hyväksyy ja sen käyttöönotosta päättää tietosuojavastaava. Tietosuojavastaava hyväksyy myös tietoturvasuunnitelman päivitettyt versiot.

3. Yleiset tietoturvakäytännöt

Yhtiössä noudatetaan seuraavia yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

- tietoturvasuunnitelma;
- seloste henkilötietojen käsittelytoimista;
- lista tietoturvasuunnitelmaankuuluvista tietojenkäsittelyyn ja tietoturvallisuuteen liittyvistä sopimuskumppaneista alihankkijoihin;
- tietojärjestelmäpalvelun tuottajien tietoturvallisuusohjeet;
- Yhtiön omat tietoturvaa koskevat ohjeet.

Tietosuojavastaavana toimii: Vilma Sääski.

4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja:

- Jokainen Yhtiön palveluksessa oleva henkilö saa näihin ohjeisiin perehdytyksen.
- Käytännön harjoittelu normaaleista poikkeaviin olosuhteisiin (lyhyt- ja pitkäkestoiset häiriöt, poikkeusolosuhteet).
- Varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä ja/tai alusta- ja verkkopalveluita.
- Yhtiö varautuu esimerkiksi seuraaviin virhe- ja ongelmatilanteisiin:
 - verkko- tai tietoliikenneongelmat;
 - tietojärjestelmien käyttöön liittyvät ongelmat;
 - tietojärjestelmien, niiden osajärjestelmien ja komponenttien hallintatoimenpiteet, kuten valvonta-, huolto- ja päivitystoimet;
 - epäilytjen, havaittujen tai toteutuneiden tietoturva- tai tietosuojauhat tai -ongelmat:
 - tilanteet, joissa potilastietoja tai muita suojattavia tietoja on vuotanut sivullisille;
 - virus- tai haittaohjelman havaitseminen;
 - työntekijän tunnusten vuotaminen ulkopuolisille;
 - tietojen kalastelun havaitseminen.

Virhe- ja ongelmatilanteissa noudatetaan seuraavia toimintatapoja:

- Virhe- ja ongelmatilanteet selvitetään tarpeen vaatimalla tavalla viipymättä tietosuojavastaavan johdolla. Yhtiön tietojenkäsittelystä ja tietoturvallisuudesta vastaavien sopimuskumppanien kanssa.

- Virhe- ja ongelmatilanteista ilmoitetaan viipymättä Yhtiön tietojärjestelmäpalvelun tuottajalle.
- Tarvittaessa ilmoitus virhe- ja ongelmatilanteesta tehdään lisäksi toimivaltaiselle viranomaiselle, esimerkiksi poliisille ja/tai tietosuojavaltuutetulle.
- Yhtiö noudattaa virhe- ja ongelmatilanteissa tietojenkäsittelyä ja tietoturvallisuudesta vastaavien sopimuskumppaniensa ja/tai viranomaisten ohjeistuksia.

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

5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

Yhtiön jokaiselle henkilöstön jäsenelle annetaan rekrytointivaiheessa tietosuojavastaavan johdolla koulutus tietojärjestelmien käyttöön, potilastietojen käsittelyyn sekä tietosuoja- ja tietoturvasioihin.

Tietoturvasuunnitelmaa tarkastellaan ja tarvittaessa päivitetään säännöllisesti vuosittain. Mahdolliset laki- ja muut sääntelymuutokset päivitetään tietoturvasuunnitelmaan voimaantulosäännösten puitteissa. Henkilöstö koulutetaan tietoturvasuunnitelman päivityksiin viipymättä.

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

- Jokainen henkilöstön jäsen perehdytetään asiakastietojen ja potilastietojen käsittelyn toimintamalleihin ja -tapoihin, kuten esimerkiksi asiakkaiden ja potilaiden informointiin ja tietopyyntöihin vastaamiseen.
- Tietojärjestelmien ja niiden uusien versioiden käytöstä annetaan tarvittaessa perehdytys huomioiden perehdytettävän henkilön työtehtävät ja rooli.
- Tietojärjestelmien osaamisen ylläpidosta huolehditaan säännöllisesti tarjottavin koulutuksin ja kurssein.
- Tietosuoja- ja tietoturvakoulutuksista laaditaan henkilöstön koulutussuunnitelma.
- Todistukset ja muut tiedot koulutuksiin osallistumisista arkistoidaan.
- Koulutusten mahdollisista kustannuksista vastaa Yhtiö. Yhtiön mahdollisesti käyttämät alihankkijat vastaavat koulutuskustannuksistaan itse.

5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

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

- Yhtiö varmistaa, että jokaisella Yhtiön tietojärjestelmän käyttäjällä on saatavilla tarpeelliset kirjalliset käyttöohjeet. Käyttöohjeita säilytetään digitaalisena versiona.
- Käyttöohjeet ovat saatavilla suomen kielellä.

- Yhtiö säilyttää kohdassa 3 kuvatut ohjeet, suunnitelmat ja selosteet potilastietojen käsittelystä.
- Yhtiö säilyttää kohdassa 5.1 tarkoitettua koulutussuunnitelman ja päivittää sitä tarvittaessa.
- Yhtiön tietosuojavastaava säilyttää kohdassa 5.1 tarkoitettujen henkilöstön tietoturvakoulutuksia koskevat todistukset ja muut tiedot.
- Mahdolliset käyttöjärjestelmäpäivitykset huomioidaan ja potilastietojen käsittelyä koskevat ohjeet päivitetään vastaavasti viipymättä.
- Jokainen henkilöstön jäsen perehdytetään potilastietojärjestelmien käyttämiseen huolellisesti työtehtävät ja roolit huomioiden.

6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen

Kuvaukset käytössä olevista tietojärjestelmistä ja siitä, millaisia käytäntöjä asiakastietojen käsittelyn, tietosuojan ja tietoturvallisuuden toteuttamisessa ja seurannassa noudatetaan näitä tietojärjestelmiä käytettäessä.

6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3)

AssisDent (potilastietojärjestelmä)

Tietojärjestelmäpalvelun tuottaja: Entteri Professional Software Oy

Tietoturvallisuustodistuksen numero: FI210702-83

Käyttökonteksti: Yksityiset terveydenhuollon palvelut

AssisDent on Entteri Professional Software Oy:n tuottama SaaS-mallin mukainen suun terveydenhuollon potilastietojärjestelmä yksityisille suun terveydenhuollon organisaatioille. Yksityinen suun terveydenhuollon palvelunantaja käyttää AssisDentia kokonaisvaltaiseen potilas- ja asiakastietojen hallintaan. AssisDent on Kanta-palveluihin yhteensopiva A3-luokkaan kuuluva korkean riskitason järjestelmä. AssisDent-järjestelmään sisältyy myös Kanta-välityspalvelu, jota pelkästään AssisDent käyttää (ei muita tietojärjestelmiä).

6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1)

Yhtiöllä ei ole käytössään muita tietoturva-auditoituja tietojärjestelmiä (A1).

6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)

Planmeca Romexis

Tietojärjestelmäpalvelun tuottaja: Planmeca Oy

Planmeca Romexis on hammaslääketieteellisen kuvantamisen modulaarinen ohjelmisto, joka mahdollistaa kaikenlaisien kuvien ottamisen (yleisesti röntgen- ja valokuvat), katselun ja käsittelyn yhdessä järjestelmässä ja tallentaa kaikki 2D- ja 3D-tutkimukset ja CAD/CAM-tiedostot samaan tietokantaan.

Fennoa taloushallintojärjestelmä. Järjestelmää voidaan käyttää asiakkaiden laskutukseen tai asiakassuhteiden hallintaan.

6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta

Yhtiöllä ei ole käytössään muita arkaluonteisten asiakastietojen suojaamisen kannalta huomioitavia järjestelmiä.

6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen

Tietojärjestelmät täyttävät yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Vaatimukset täyttyvät käytettäessä tietojärjestelmää sekä itsenäisesti että yhdessä mahdollisten muiden siihen liitettäviksi tarkoitettujen tietojärjestelmien kanssa.

Yhtiön käyttämät tietojärjestelmät vastaavat käyttötarkoitukseltaan Yhtiön toimintaa ja täyttävät Yhtiön toimintaan liittyvät olennaiset vaatimukset. Yhtiö varmistaa tietojärjestelmäpalvelun tuottajan avulla sen, että tietojärjestelmä on suunniteltu, valmistettu ja toimii tietoturvaa ja tietosuojaa koskevien lakien ja niiden nojalla annettujen säännösten sekä yhteentoimivuutta koskevien kansallisten määrittelyjen mukaisesti.

Yhtiö varmistaa tietojärjestelmäpalvelun tuottajan avulla sen, että tietojärjestelmällä pystytään suorittamaan käyttötarkoituksen mukaisessa asiakas- ja potilastietojen käsittelyssä lakien ja niiden nojalla annettujen säännösten edellyttämät toiminnot.

Yhtiö seuraa ja noudattaa Terveiden ja hyvinvoinnin laitoksen antamia tarkempia määräyksiä ja ohjeita olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä.

6.2. Tietojärjestelmien asennus, ylläpito ja päivitys

Tietojärjestelmiä ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti. Tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus.

6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

Tietojärjestelmien ja laitteiden käyttäjiä ja käyttäjäryhmiä hallinnoidaan seuraavasti:

Yhtiön johto ylläpitää ajantasaista luetteloa seuraavista käyttäjistä:

- käyttäjät, jotka käyttävät terveydenhuollon asiakastieto- ja/tai potilastietojärjestelmiä;
- käyttäjät, jotka käyttävät Yhtiön laitteita (työasemat, mobiililaitteet, muut laitteet);
- käyttäjät, joilla on käyttöoikeudet Kanta-palvelujen käyttöön.

Käyttöoikeuksien ja käyttövaltuuksien osalta noudatetaan seuraavia toimintatapoja:

- käyttöoikeuksia hallinnoi Yhtiön tietoturvavastaava.

Käyttäjien tunnistautumisessa ja todentamisessa noudatetaan seuraavia käytäntöjä:

- Yhtiön johto hallinnoi toimikortteja, kulunvalvontaa ja muita tunnistamisvälineitä.
- Työasemiin ja järjestelmiin kirjaudutaan omilla henkilökohtaisilla käyttäjätunnuksilla ja salasanoilla.
- Yhteiskäyttöisiä tunnuksia käytetään vain silloin, kun se on välttämätöntä.
- Virhetilanneselvityksissä pääkäyttäjä ja tietojärjestelmäasiantuntija voivat tunnistautua kaikkiin järjestelmiin ja laitteisiin.

6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Asiakastietoja käsittelevien järjestelmien pääsynhallintaa ja käytön seurantaan toteutetaan seuraavasti:

- Laitteisiin ja tietojärjestelmiin kirjaudutaan joko terveydenhuollon ammattihenkilön toimikortilla tai omalla henkilökohtaisella käyttäjätunnuksella ja salasanalla.
- Mikäli epäillään tai havaitaan säädösten vastaista terveydenhuollon asiakastietojen tai potilastietojen käsittelyä, rikkomukseen puututaan välittömästi ja otetaan tarvittaessa välittömästi yhteys toimivaltaiseen viranomaiseen.

7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

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

- Näyttöpäätteet sijoitetaan ja suojataan siten, että sivullisilla ei ole näköyhteyttä ruuduille.
- Käyttämättömän päätteen lukittumisaika asetetaan niin, että sivulliset eivät pääse käyttämään päätteitä.
- Tietokoneille, tietojärjestelmille ja muille laitteille pääsee vain henkilökohtaisella käyttäjätunnuksella ja salasanalla kirjautumalla.
- Työtä tehdään pääsääntöisesti potilaan luona tämän kotona taikka hoitolaitoksessa.
- Yhtiön johdolla ja johdon nimeämillä henkilöillä on oikeus asentaa ohjelmistoja ja sovelluksia organisaation laitteille. Yhtiö huolehtii siitä, että vain nämä henkilöt pääsevät tekemään asennuksia.
- Yhtiössä ei lähtökohtaisesti sallita ulkoisten kovalevyjen ja muistitikkujen käyttöä. Jos ulkoisia kovalevyjä ja muistitikkuja on tarpeen käyttää, Yhtiön johto harkitsee tarvittavat suojaustoimenpiteet.
- Tulostinten sijainti ratkaistaan siten, että ulkopuolisilla ei ole pääsyä tulostimille.
- Lähtökohtaisesti paperisia potilastietoja sisältäviä asiakirjoja ei synny. Mikäli näitä syntyy ja niitä säilytetään Yhtiön tiloissa, asiakirjoja säilytetään paloturvallisesti lukittuna ja suojassa sivullisilta.
- Paperiset potilastietoja sisältävät asiakirjat hävitetään tarvittaessa paperisilppurilla tai vastaavalla tietoturvallisella tavalla.

7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

- Virusturvan toimivuus ja päivitykset työasemilla varmistetaan ulkopuolisten tietoturva-asiantuntijoiden avulla.
- Mobiililaitteiden (tabletit ja älypuhelimet, mahdolliset kannettavat työasemat) osalta käyttäjätunnukset, salasana, PIN-koodit, SIM-korttien hallinta ja laitteiden virusturvaohjelmat, kadonneiden mobiililaitteiden etälukitseminen ja/tai tyhjentäminen järjestetään tietoturva huomioiden. Yhtiö käyttää näissä toimissa tarvittaessa apunaan asiantuntijoita.

Käyttöympäristön tukipalvelut:

- Käyttöjärjestelmiä päivitetään säännöllisesti.
- Järjestelmät kovennetaan säännöllisesti.
- Järjestelmien yhteentoimivuus sote-tietojärjestelmien kanssa varmistetaan säännöllisesti.

Yhtiö käyttää näissä toimissa tarvittaessa apunaan asiantuntijoita.

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

Alusta- ja verkkopalveluiden tietoturallisuudesta huolehditaan seuraavasti:

Yleistä:

- Yhtiö varmistaa sopimusehdoilla ja tietoturvaselosteet tarkistamalla tietosuojasäännösten noudattamisen sen käyttäessä ulkoisia alusta- ja verkkopalveluita.
- Yhtiö varautuu toimimaan poikkeustilanteissa ilman tietojärjestelmiä.

Palvelimet ja palvelinympäristöt:

- Ulkopuolinen asiantuntija vastaa Yhtiön palvelinten ja palvelinympäristöjen asentamisesta ja ylläpidosta.
- Palvelimet, joilla tietojärjestelmät toimivat, suojataan asianmukaisesti haittaohjelmilta.
- Haittaohjelmien torjunnassa olevat ohjelmat päivitetään aina tarvittaessa.
- Palvelinympäristöön ei asenneta aktiivisia oletustunnuksia tai muita oletuksena tulevia tietoturallisuuden kannalta ongelmallisia asetuksia.

Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet:

- Yhtiön tietoliikenneoperaattoreista ja tietoliikenteen tietoturvaan liittyvistä vastuista vastaa ulkopuolinen asiantuntija.
- Yhtiö ottaa tietoverkkojen häiriötilanteissa yhteyttä ulkopuoliseen asiantuntijaan.
- Segmentoinnit, palomuurit ja reititykset asennetaan asianmukaisella tavalla tietoturvan varmistamiseksi.

- Langattoman verkon käyttö vaatii salasanan.
- Yhtiön langaton verkko suojataan asianmukaisesti ulkoisilta käyttäjiltä.
- Reitittimet ja muut verkkolaitteet sekä näiden komponentit ja laite- ja laiteohjelmistot päivitetään aina tarvittaessa.

Pilvipalvelut, pilvipohjaiset ratkaisut, etähallintapalvelut, palvelinvuokraus, palvelinhallinta, varmistus- ja konesalipalvelut:

- Sopimukset päivitetään ulkopuolisten asiantuntijoiden avulla tarvittaessa vastaamaan voimassa olevia säädöksiä (mm. EU:n yleinen tietosuoja-asetus, tarvittaessa henkilötietojen siirtämisen perusteet ETA-alueen ulkopuolelle).
- Käytössä olevia alusta- ja verkkopalveluita (mukaan lukien pilvipalvelut) seurataan jatkuvasti ja säännöllisesti ulkopuolisten asiantuntijoiden avulla muun muassa toimivuuden, tietoturvaluksuusriskien, häiriötilanteiden ja palveluiden käyttöehtojen näkökulmasta (sopimusten ja käytäntöjen päivittäminen muuttunutta tilannetta vastaavaksi).
- Tietojärjestelmien, osajärjestelmien, laitekomponenttien, verkkojen sekä huolto- ja päivitystoimenpiteiden huolto- päivitys- ja uusimissuunnitelmat sekä toimintamallit huoltotoimenpiteisiin liittyvään päätöksentekoon laatii ulkopuolinen asiantuntija.

8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

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

- käyttäjät koulutetaan tai perehdytetään tuntemaan Kanta-palvelut. Koulutuksessa ja perehdytyksessä hyödynnetään Kanta-palvelujen perehdytysmateriaali ja verkkokoulut/kyselyt.
- Yhtiön johto seuraa aktiivisesti ja säännöllisesti Kanta-palvelujen käyttöä.
- Kanta-palvelujen edellyttämien tunnistamis- ja todentamisratkaisujen toteuttaminen: Kanta-palveluja käyttäviin järjestelmiin kirjaudutaan henkilökohtaisilla tunnuksilla.
- Yhtiön johto hallinnoi Kanta-palvelujen edellyttämien käyttöoikeuksia ja käyttövaltuuksia.
- Yhtiön johto seuraa Kanta-palvelujen ja niihin liittyvien järjestelmien käyttöä.
- Yhtiön johto varmistaa, että hankittava tai päivitettävä järjestelmä täyttää sitä koskevat olennaiset vaatimukset.
- Palvelunantaja varmistaa ja todentaa asiakkaan informoinnin Kanta-palveluista ja asiakastietojen käytöstä aina hoitosuhteen alussa tai asioinnin yhteydessä.