[Yrityksen nimi]

Tietoturvasuunnitelma

Yrityksen nimi Versio [numero]

Laatija

Päivämäärä pp.kk.vvvv

|  |
| --- |
| Version historia  |
| Pvm | Muutos | Tekijä | Hyväksyjä |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Salassa pidettävä, vain yrityksen sisäiseen käyttöön ja viranomaiselle pyydettäessä annettava.

**Tämän asiakirjapohjan on valmistanut**

**Kyberturvan abc yrittäjille -hanke, jota rahoittaa**

**Hämeen ELY-keskus Euroopan sosiaalirahastosta (ESR).**

# Sisällys

[Sisällys 2](#_Toc124442288)

[1. Tietoturvasuunnitelman käyttötarkoitus 3](#_Toc124442289)

[2. Tietoturvasuunnitelman kohde ja päivityskäytännöt 4](#_Toc124442290)

[3. Yleiset tietoturvakäytännöt 5](#_Toc124442291)

[4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta 6](#_Toc124442292)

[5. Henkilöstön koulutus ja osaaminen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen 9](#_Toc124442293)

[5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen 9](#_Toc124442294)

[5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö 10](#_Toc124442295)

[6. Tietojärjestelmien tietoturvakäytännöt 11](#_Toc124442296)

[6.1.1. Kanta-palveluihin liittyvät tietojärjestelmät (luokat A2 tai A3) 12](#_Toc124442297)

[6.1.2. Muusta syystä tietoturva-auditoidut tietojärjestelmät (luokka A1) 12](#_Toc124442298)

[6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B) 12](#_Toc124442299)

[6.1.4. Muut tietojärjestelmät, jotka on otettava huomioon arkaluonteisten asiakastietojen suojaamisen kannalta 13](#_Toc124442300)

[6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen 13](#_Toc124442301)

[6.2. Tietojärjestelmien asennus, ylläpito ja päivitys 13](#_Toc124442302)

[6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt 16](#_Toc124442303)

[6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt 18](#_Toc124442304)

[7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt 20](#_Toc124442305)

[7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta 20](#_Toc124442306)

[7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta 23](#_Toc124442307)

[7.3. Alusta- ja verkkopalvelujen tietoturvallinen käyttö tietosuojan ja varautumisen kannalta 24](#_Toc124442308)

[8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt 28](#_Toc124442309)

[9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat 32](#_Toc124442310)

[9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat) 33](#_Toc124442311)

[9.2. Järjestelmät X (luokkaan A1 kuuluvat) 35](#_Toc124442312)

[9.3. Järjestelmät Y (luokkaan B kuuluvat) 37](#_Toc124442313)

[9.4. Järjestelmät Z (muut järjestelmät, jotka eivät kuulu luokkiin A tai B) 38](#_Toc124442314)

# 1. Tietoturvasuunnitelman käyttötarkoitus

Tämä mallipohja auttaa tietoturvasuunnitelman laatimisessa. Tietoturvasuunnitelman sisältö on määritelty THL:n määräyksessä 3/2021 (THL/4309/4.09.00/2021).

Mallipohjaan on laitettu täyttöä helpottavia ohjeita joidenkin kappaleiden alkuun. Ohjeet on kirjoitettu sinisellä tekstillä ja ne on tarkoitettu poistettaviksi valmiista tietoturvasuunnitelmasta. Myös taulukoissa on ohjeita siitä, mitä mihinkin kohtaan tulee kirjoittaa.

Alla näkyvän mustan tekstin on tarkoitus toimia pohjana suunnitelmaan sisällytettävälle tekstille. Tekstiä saa halutessaan muokata. Mallitekstin seassa on hakasuluissa olevia ohjeita, jotka kertovat mitä kyseiseen kohtaan tulee lisätä.

Tämä dokumentti on [yrityksen nimi]n tietoturvasuunnitelma. Tämän tietoturvasuunnitelman käyttötarkoitus on täyttää uuden asiakastietolain 784/2021 27 §:n ja THL:n määräyksen 3/2021 mukaiset velvoitteet. Suunnitelma kokoaa yhteen asiakastietolaissa vaaditut omavalvonnan kohteelta edellytettävät selvitykset ja vaatimukset.

Ennen uuden asiakastietolain 784/2021 voimaantuloa käytössä ollut vanhan asiakastietolain 159/2007 mukainen omavalvontasuunnitelma vastasi pääosin sisällöltään tietoturvasuunnitelmaa. Näin ollen kyse on THL:n määräyksen 3/2021 tultua voimaan yrityksen käytössä olevien omavalvontasuunnitelmien päivittämisestä uusiksi tietoturvasuunnitelmiksi.

Tietoturvasuunnitelman avulla osoitetaan, että yrityksessä noudatetaan EU:n tietosuoja-asetuksen mukaisia tietosuojaperiaatteita aina, kun käsitellään henkilötietoja. Tietosuojaperiaatteita tulee noudattaa tietojen koko elinkaaren ajan.

Periaatteiden mukaan henkilötietoja on:

* käsiteltävä **lainmukaisesti**, **asianmukaisesti** ja rekisteröidyn kannalta **läpinäkyvästi**
* kerättävä ja käsiteltävä **tiettyä**, **nimenomaista** ja **laillista tarkoitusta varten**
* kerättävä **vain tarpeellinen määrä** henkilötietojen käsittelyn tarkoitukseen nähden
* päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot on **poistettava tai oikaistava viipymättä**
* **säilytettävä** muodossa, josta rekisteröity on tunnistettavissa **ainoastaan niin kauan kuin on tarpeen** tietojenkäsittelyn tarkoitusten toteuttamista varten
* käsiteltävä **luottamuksellisesti** ja **turvallisesti**.

Tietoturvasuunnitelman piiriin kuuluu kaikki yrityksessä tapahtuva henkilötietojen käsittely.

Suunnitelma auttaa yrityksen tietoturvan ylläpitämisessä ja kehittämisessä. Se auttaa hahmottamaan yrityksen tietoturvan tilaa sekä tunnistamaan riskejä ja varautumaan poikkeustilanteisiin.

Yrityksen tavoitteena on liittyä Kanta-palveluiden käyttäjäksi [ajankohta] ja tietoturvasuunnitelma täydentyy prosessin edetessä.

Tietoturvasuunnitelmaa tulee päivittää säännöllisesti. Päivityskäytännöt on kuvattu seuraavassa kappaleessa. Tietoturvasuunnitelman laadinnan ja noudattamisen vastuu on yrityksen vastaavalla johtajalla.

# 2. Tietoturvasuunnitelman kohde ja päivityskäytännöt

Tämän tietoturvasuunnitelman piiriin kuuluvat:

Tähän kohtaan tulevat yrityksen perustiedot, sekä alihankkijat ja kumppanit joita tämä tietoturvasuunnitelma koskee.

|  |  |
| --- | --- |
| Yrityksen nimi |  |
| Y-tunnus |  |
| Vastuuhenkilö |  |
| Toimipaikat |  |
| Alihankkijat/Kumppanit |  |

Suunnitelman toteuttamisessa ja päivittämisessä noudatetaan seuraavia käytäntöjä:

|  |  |
| --- | --- |
| Suunnitelman vastuuhenkilö |  |
| Tietosuojavastuuhenkilö |  |
| Tarkistus- ja päivityskäytännöt | * Milloin suunnitelma otetaan käyttöön
* Kuinka usein suunnitelma tarkastetaan (säännöllisesti, esim. joka vuosi heinäkuussa)
* Missä muissa tilanteessa tarkastetaan ja päivitetään suunnitelma
 |
| Suunnitelman seuranta ja seurannan dokumentointi | * Millä tavalla seurataan suunnitelman toteuttamista
* Miten dokumentoidaan seuranta (esim. henkilöstöltä pyydettävät lukukuittaukset, kun suunnitelmaan on perehtynyt)
* Kenellä (työntekijä) on minkälainen vastuu
 |
| Suunnitelman käyttö tietojärjestelmien hankinnoissa ja päivityksissä | * Miten huomioidaan tietoturvasuunnitelma työkalujen ja tietojärjestelmien hankinnoissa
 |
| Päätös suunnitelman hyväksymisestä ja käyttöönotosta | * kuka/ketkä ja milloin on päättänyt suunnitelman hyväksymisestä ja käyttöönotosta
* kuinka päätetään suunnitelman uusien versioiden hyväksymisestä ja käyttöönotosta
 |

# 3. Yleiset tietoturvakäytännöt

Tähän lukuun kuvataan tietoa yleisistä tietoturvakäytännöistä, politiikoista, tietoturvallisuustyön vastuuttamisesta ja organisoinnista, selosteet henkilötietojen käsittelytoimista, sopimuksista, keskeisistä tietoturvallisuusohjeista sekä tietosuojavastaavista.

[Yritys]:ssa noudatetaan seuraavia yleisiä tietoturvakäytäntöjä ja tehdään tietoturvallisuus-, tietosuoja-, riskienhallinta- ja asiakastietojen käsittelyn omavalvontatyötä seuraavien dokumenttien mukaisesti:

* Seloste henkilötietojen käsittelytoimista (lisätietoja saat täältä: [Seloste käsittelytoimista | Tietosuojavaltuutetun toimisto](https://tietosuoja.fi/seloste-kasittelytoimista))
* Riskienhallintasuunnitelma
* Liiketoiminnan jatkuvuussuunnitelma
* Muita tietoturvaan liittyviä asiakirjoja / suunnitelmia

Tietosuojavastaavana ja varahenkilönä toimivat: nimi ja nimi

# 4. Menettelyt virhe- ja ongelmatilanteissa sekä jatkuvuudenhallinta

Tähän kohtaan kasataan toimintaohjeet ja vastuut virhe- ja ongelmatilanteiden varalta. Yritykseltä tulee löytyä selkeät toimintatavat ja vastuut tällaisten tilanteiden havainnointiin, tiedottamiseen, korjaamiseen ja toipumiseen. Jos sinulla on jo ohjeistus jonkin alla mainitun tilanteen varalle, voit viitata siihen ohjeistukseen.

Poikkeustilanteisiin varautumisessa ja jatkuvuuden suunnittelussa noudatetaan seuraavia toimintatapoja:

|  |  |
| --- | --- |
| Aihepiiriin kuuluvat suunnitelmat | * Liiketoiminnan jatkuvuussuunnitelma
* Palautumissuunnitelma
* Muut mahdolliset jatkuvuuteen, toipumiseen ja varautumiseen liittyvät suunnitelmat
 |
| Käytännön harjoittelu ja valmiustoiminta | * Miten poikkeustilanteita harjoitellaan ja kuinka usein
* Kenen vastuulla poikkeamista ilmoittaminen on ja kuka niihin reagoi
 |
| Ohjeistukset | * Ohjeistukset poikkeustilanteiden varalle
* Mistä ohjeet löytyvät
 |
| Normaalista poikkeavat olosuhteet, lyhyt- ja pitkäkestoiset häiriöt, poikkeusolosuhteet | * Mahdolliset poikkeustilanteet ja häiriöt ja miten niissä toimitaan
 |
| Varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä ja/tai alusta- ja verkkopalveluita | * Miten toimitaan, jos tietojärjestelmät ja yrityksen toiminnalle tarpeelliset palvelut eivät toimi
 |

Virhe- ja ongelmatilanteissa noudatetaan seuraavia toimintatapoja:

|  |  |
| --- | --- |
| Verkko- tai tietoliikenneongelmat | * Menettelyt
* Yhteystiedot verkkopalveluiden tuottajille
* Mahdolliset tuottajien ohjeet
 |
| Tietojärjestelmien käyttöön liittyvät ongelmat | * Menettelyt, jos järjestelmä ei toimi, ei käynnisty tai toimii virheellisesti
* Eri järjestelmätoimittajien yhteystiedot ja tukipalvelut
 |
| Tietojärjestelmien, niiden osajärjestelmien ja komponenttien hallintatoimenpiteet | * Valvonta-, huolto- ja päivitystoimet
	+ Kenen vastuulla?
 |
| Epäiltyjen, havaittujen tai toteutuneiden tietoturva- tai tietosuojauhkien tai ongelmien hallinta | * Toimenpiteet, jos asiakastietoja tai muita suojattavia tietoja on vuotanut sivullisille
* Toimenpiteet, jos havaintaan virus- tai haittaohjelma
* Toimenpiteet, jos työntekijän tunnukset ovat vuotaneet ulkopuolisille
* Toimenpiteet, jos havaitaan tietojen kalastelua
 |
| Toimenpiteet, jos asiakastietoja käsittelevät tietojärjestelmät toimivat selvästi väärin suhteessa niille asetettuihin kansallisiin vaatimuksiin | * Eli luokan A tai luokan B järjestelmien olennaisten vaatimusten täyttymisessä havaittujen merkittävien poikkeamien ilmoittaminen tietojärjestelmäpalvelun tuottajalle
 |
| Toimenpiteet, jos asiakastietoja käsittelevät tietojärjestelmät aiheuttavat riskin potilasturvallisuudelle | * Eli luokan A tai luokan B järjestelmien merkittävien poikkeamien ilmoittaminen Valviralle, jos poikkeama aiheuttaa merkittävän riskin potilasturvallisuudelle tai tietoturvalle (esimerkiksi tilanteessa, jossa sosiaalihuollon asiakastiedot ja/tai potilastiedot ja/tai reseptitiedot ovat menneet väärälle asiakkaalle/potilaalle järjestelmävirheen vuoksi)
 |
| Toimenpiteet tietosuojapoikkeamissa | * Ilmoittaminen tietosuojavaltuutetulle ja rekisteröidyille
 |

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

## 5.1. Henkilöstön koulutus sekä osaamisen ylläpito ja kehittäminen

Kirjoita tähän miten varmistetaan, että henkilöstölle on annettu koulutus tietojärjestelmien käyttöön, asiakastietojen käsittelyyn, sekä tietosuoja- ja tietoturva-asioihin. Lisäksi tulee kuvata, miten seurataan ja ylläpidetään henkilöstön osaamista.

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

|  |  |
| --- | --- |
| Asiakastietojen käsittelyn toimintamallien koulutus ja perehdytys | * miten huolehditaan asiakastietojen käsittelyn toimintamallien/-tapojen koulutuksesta ja perehdytyksestä (esim. asiakkaiden ja potilaiden informointi, tietopyyntöihin vastaaminen jne.)
 |
| Tietojärjestelmien käyttökoulutus ja osaamisen ylläpito | * miten huolehditaan tietojärjestelmien ja niiden uusien versioiden käyttökoulutuksesta ja perehdytyksestä sekä osaamisen säännöllisestä ylläpidosta erilaisissa työtehtävissä ja rooleissa
 |
| Tietosuoja- ja tietoturva koulutukset | * miten tietosuoja- ja tietoturva koulutukset tai kouluttautuminen toteutetaan, tarvittaessa viittaukset erillisiin koulutussuunnitelmiin
 |
| Osaamisen seuranta | * miten koulutusten osaamista seurataan (esim. todistukset tai ylläpidettävät tiedot koulutuksiin osallistumisista arkistoidaan)
 |
| Kustannukset | * mikä taho kulloinkin vastaa erilaisten koulutusten kustannuksista, tarvittaessa viittaukset asiaa koskeviin sopimuksiin
 |

## 5.2. Tietojärjestelmien käyttöohjeet ja ohjeiden mukainen käyttö

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

|  |  |
| --- | --- |
| Tietojärjestelmien käyttöohjeet | * miten on varmistettu, että tietojärjestelmän käyttäjällä on saatavilla tarpeelliset käyttöohjeet käyttäjälle ymmärrettävässä (eri kieliversiot) muodossa kirjallisesti – ohjeet tarvittaessa sekä organisaatio- että tietojärjestelmäkohtaisesti
 |
| Ohjeet asiakastietojen käsittelystä ja henkilöstön koulutuksesta tietojen käsittelyyn | * miten ohjeet asiakastietojen käsittelystä ja palvelunantajan henkilöstön koulutuksesta tietojen käsittelyyn sekä henkilöstön tietämyksen ylläpito on dokumentoitu ja todennettavissa
 |
| Ohjelmistojen käyttöohjeiden päivittäminen | * miten käyttöohjeiden päivittäminen ja jakelu toteutetaan ohjelmistojen versiopäivitysten sekä muiden muutosten yhteydessä
 |
| Tuki | * kuinka tuetaan (perehdytys, ohjaus, neuvonta) erilaisissa työtehtävissä ja rooleissa toimivia työntekijöitä tietojärjestelmien käyttämisessä.
 |

# 6. Tietojärjestelmien tietoturvakäytännöt

6.1. Tietojärjestelmien perustiedot, kuvaukset ja olennaisten vaatimusten täyttyminen
Nämä tiedot saat järjestelmätoimittajalta. Mukaan otetaan ainakin järjestelmät, joilla on vaikutusta asiakastietojen käsittelyyn, tietoturvaan ja tietosuojaan. Voit myös viitata erilliseen tietojärjestelmistä kasattuun ajantasaiseen luetteloon.

Valviran tietojärjestelmärekisterin löydät täältä: <https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat/sosiaali-ja-terveydenhuollon-tietojarjestelmarekisteri>

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

Luettelo luokkiin A2 ja A3 kuuluvista järjestelmistä (nimi, versio, toimittaja, yhteystiedot, tiedot tietoturvallisuuden arviointia koskevasta todistuksesta (todistuksen numero ja mihin asti voimassa) ja sen vastaavuus Valviran tietojärjestelmärekisterin tietoihin).

|  |  |  |  |
| --- | --- | --- | --- |
| Nimi |  | Versio |  |
| Toimittaja |  | Yhteystiedot |  |
| Todistukset |  | Valvira tietojärjestelmä-rekisteri |  |

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

Luettelo luokkaan A1 kuuluvista järjestelmistä (nimi, versio, toimittaja, yhteystiedot, tiedot tietoturvallisuuden arviointia koskevasta todistuksesta (todistuksen numero ja mihin asti voimassa) ja sen vastaavuus Valviran tietojärjestelmärekisterin tietoihin).

|  |  |  |  |
| --- | --- | --- | --- |
| Nimi |  | Versio |  |
| Toimittaja |  | Yhteystiedot |  |
| Todistukset |  | Valvira tietojärjestelmä-rekisteri |  |

### 6.1.3. Muut asiakastietoja käsittelevät järjestelmät (luokka B)

Luettelo luokkaan B kuuluvista järjestelmistä.

|  |  |  |  |
| --- | --- | --- | --- |
| Nimi |  | Versio |  |
| Toimittaja |  | Yhteystiedot |  |

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

Luettelo muista järjestelmistä, jotka tarvitsee ottaa huomioon

|  |  |  |  |
| --- | --- | --- | --- |
| Nimi |  | Versio |  |
| Toimittaja |  | Yhteystiedot |  |

### 6.1.5. Tietojärjestelmien olennaisten vaatimusten täyttyminen

|  |  |
| --- | --- |
| Hankinnat ja sopimukset | * esim. maininta siitä, että uusia sopimuksia tehdessä varmistetaan, että järjestelmät täyttävät vähimmäisvaatimukset
 |
| Tietojärjestelmien vaatimustenmukaisuuden varmistaminen | * kuinka usein tarkistetaan tietojärjestelmien tietojen ja vaatimustenmukaisuuden voimassaolo Valviran tietojärjestelmärekisteristä (esim. tietoturvasuunnitelman päivittämisen yhteydessä vuosittain)
 |
| Tietojen ylläpitomenettelyt | * maininta siitä, kuinka myös muut kohdissa 6.1.1-6.1.4 kirjatut tiedot tarkistetaan säännöllisesti (esim. suunnitelman päivittämisen yhteydessä)
 |

## 6.2. Tietojärjestelmien asennus, ylläpito ja päivitys

Kirjaa tähän kohtaan tietojärjestelmien asennukseen, ylläpitoon ja päivitykseen liittyvät käytännöt. Viittaa tarvittaessa sopimuksiin tai muihin dokumentteihin joissa asioita kuvataan. Järjestelmäkohtaisia erityiskäytäntöjä voidaan kuvata luvuissa 6.1 ja 9, jos käytössä on useita järjestelmiä ja jos ne poikkeavat tässä määritellyistä käytännöistä

Tietojärjestelmien asennuksissa, ylläpidossa ja päivityksissä noudatetaan seuraavia toimintatapoja:

|  |  |
| --- | --- |
| Järjestelmien asennus | * henkilöt ja toimijat, jotka saavat suorittaa järjestelmien asennustoimenpiteitä
* kuinka estetään se, että muut eivät pääse suorittamaan järjestelmien tai ohjelmistojen asennuksia (esimerkiksi edellytetäänkö joissakin tehtävissä tai palveluissa toimivilta henkilöiltä tai palveluntuottajilta tietoturvaselvityksiä tai turvallisuusselvityksiä)
 |
| Asennus-, ylläpito- ja päivitystoimenpiteitä suorittavien henkilöiden osaaminen ja roolit | * asennus-, ylläpito- ja päivitystoimenpiteitä suorittavilta henkilöiltä vaadittava ammatillinen osaaminen tai asianmukainen koulutus
* tietojärjestelmiä asentavien, ylläpitävien ja päivittävien henkilöiden roolit ja vastuut suhteessa tietoturvallisuuden omavalvonnan kohteeseen sekä tietojärjestelmäpalvelun tuottajaan
 |
| Palvelut ja sovellukset | * mitä palveluita ja mitä sovelluksia on tietojärjestelmissä tai niiden osajärjestelmissä
 |
| Oletustunnukset ja oletusasetukset | * kuinka estetään se, ettei tietojärjestelmissä tai laiteohjelmistoissa ole aktiivisia oletustunnuksia tai muita mahdollisesti oletuksena tulevia tietoturvallisuuden kannalta huonoja asetuksia (viittaukset esimerkiksi kovennusohjeisiin)
 |
| Suojaus | * kuinka tietojärjestelmät suojataan tyypillisimmiltä tietoturvapuutteilta ja www-sovellusten haavoittuvuuksilta
 |
| Päivitykseen liittyvät toimintatavat  | * toimintatavat, jos käytössä olevaan järjestelmään tehdään päivitys
 |
| Uuden järjestelmän tai järjestelmäversion käyttöönotto | * mitä on vähintään testattava ja varmistettava ennen kuin järjestelmä tai uusi järjestelmäversio otetaan tuotantokäyttöön
* miten hyväksytään uuden järjestelmän tai järjestelmäversion käyttöönotto, hyväksymisvastuut
 |
| Tärkeät ja kriittiset tietojärjestelmät | * tärkeimpien ja kriittisimpien tietojärjestelmien sekä niiden toiminnassa tarvittavien laitteiden fyysisten ja ohjelmallisten osien sekä niihin liittyvien yksittäisten komponenttien huolto-, uusimis-, ylläpito- ja päivitysmenettelyt
* kriittisimmiksi luokiteltujen tietojärjestelmien luotettavuudesta huolehtiminen (mm. kahdennukset, tilapäisratkaisut, varaosat ja erityiskomponentit) aktiivisilla valvonta- ja huoltotoimilla
 |

## 6.3. Käyttövaltuuksien hallinnan ja tunnistautumisen käytännöt

Tarvittaessa viittaukset erillisiin omiin tai ulkoisiin ohjeisiin tai kuvauksiin.

Tietojärjestelmien ja laitteiden käyttäjiä ja käyttäjäryhmiä hallinnoidaan seuraavasti:

|  |  |
| --- | --- |
| Asiakastietojärjestelmät | * miten ja missä ylläpidetään ajantasaista luetteloa käyttäjistä ja tarvittaessa käyttäjäryhmistä, jotka käyttävät asiakastietojärjestelmiä
 |
| Laitteet | * miten ja missä ylläpidetään ajantasaista luetteloa käyttäjistä ja tarvittaessa käyttäjäryhmistä, jotka käyttävät yrityksen laitteita (työasemat, mobiililaitteet, muut laitteet)
 |
| Kanta-palvelut | * miten ja missä ylläpidetään ajantasaista luetteloa käyttöoikeuksista Kanta-palvelujen käyttöön
 |
| Muut sähköiset järjestelmät | * miten ja missä ylläpidetään ajantasaista luetteloa käyttöoikeuksista muihin sähköisiin järjestelmiin
 |

Käyttöoikeuksien ja käyttövaltuuksien osalta noudatetaan seuraavia toimintatapoja:

|  |  |
| --- | --- |
| Roolit | * käyttövaltuuksien hallintaan liittyvät erilaiset roolit ja henkilöt, jotka eri rooleissa toimivat (käyttöoikeuden hakeminen, myöntäminen, muuttaminen, peruminen, poistaminen)
 |
| Hallintamenettelyt | * käyttövaltuuksien hallintamenettelyt (mahdollisesti käytössä olevat IAM-järjestelmät)
 |
| Uuden työntekijän/sijaisen käyttöoikeudet | * kuinka uudelle työntekijälle tai sijaiselle (erilaisissa käytännön tilanteissa ja kellonajankohdissa) saadaan tunnukset ja käyttöoikeudet
* kuinka sijaisten henkilöllisyys varmistetaan ennen käyttöoikeuksien myöntämistä
 |
| Käyttöoikeuksien tai tunnusten poistaminen | * kuinka ja milloin poistuneiden työntekijöiden tunnukset ja käyttöoikeudet poistetaan
* käytännön toiminta kiireellisissä käyttöoikeuksien tai tunnusten poistamistilanteissa
 |
| Kanta-palvelujen käyttöoikeuksien hallinnointi | * kuinka Kanta-palvelujen käyttöoikeuksia hallinnoidaan
 |

Käyttäjien tunnistautumisessa ja todentamisessa noudatetaan seuraavia käytäntöjä:

|  |  |
| --- | --- |
| Kirjautumis- ja tunnistamisvälineiden hallinta | * toimikorttien ja salasanojen sekä muiden kirjautumis- ja tunnistamisvälineiden hallinta
* nämä asiat on hyvä kirjata erilliseen suunnitelmaan (näkökulmina ainakin kulunvalvonta, työasemien ja järjestelmien kirjautumiset, mobiililaitteiden kirjautumis- ja tunnistautumiskäytännöt)
 |
| Käyttäjätunnus- ja salasanatunnistautuminen | * käyttäjätunnus- ja salasanatunnistautumiseen liittyvät käytännöt
 |
| Yhteiskäyttöiset tunnukset | * yhteiskäyttöisten tunnusten käyttäminen rajatuissa ja välttämättömissä kohteissa (ei-tunnisteelliset) ja estäminen muissa kohteissa
 |
| Monivaiheinen tunnistautuminen | * monivaiheisen tunnistautumisen (MFA) mahdollinen hyödyntäminen
 |
| Toiminta ja tunnistautuminen virhetilanneselvityksissä  | * pääkäyttäjien ja tietojärjestelmäasiantuntijoiden toiminta ja tunnistautuminen virhetilanneselvityksissä
 |
| Kulunvalvonta | * tietoteknisten turvakäytäntöjen mahdollinen hyödyntäminen kulunvalvonnassa
 |

## 6.4. Asiakas- ja potilastietojärjestelmien pääsynhallinnan ja käytön seurannan käytännöt

Tarvittaessa viittaukset erillisiin omiin tai ulkoisiin ohjeisiin tai kuvauksiin.

Asiakastietoja käsittelevien järjestelmien pääsynhallintaa ja käytön seurantaa toteutetaan seuraavasti:

|  |  |
| --- | --- |
| Tarkistukset | * millaisia pääsynhallinnan tarkistuksia tehdään laitteisiin kirjautumisessa, tietojärjestelmien käynnistämisessä ja mahdollisesti muissa tilanteissa, kuten kulunvalvonnassa
 |
| Tekniset käytännöt ei-sallitun käytön estämiseen | * pääsynhallinnan tekniset käytännöt ei-sallitun käytön estämiseen asiakastietoja käsittelevissä tietojärjestelmissä sekä omavalvonnan kohteen omat ohjeet ja toimintatavat oikeisiin toimintatapoihin ja tietojenkäsittelyyn
 |
| Lokit | * luettelot tai vastaavat koonnit tietojärjestelmien tuottamista ja asiakastietojen käytön seurantaan koottavista lokeista (mm. lokitiedostot, lokienhallintajärjestelmät, …)
 |
| Lokienhallinnan ja käytön seurannan käytännöt valvonnassa ja tietopyyntöihin vastaamisessa | * keskeiset roolit, kuvattava mm. tietosuojavastaavan, tietohallinnon ja rekisterinpidosta vastaavien roolit asiakastiedon käytön seurannassa
* käytössä olevat lokienhallintajärjestelmät ja/tai muut raportointimenettelyt
* asiakkaiden tietopyyntöihin vastaaminen, kuka/ketkä kokoavat lokiraportit ja kuinka usein
* kuka/ketkä seuraavat lokiraportteja tai lokitietoja ja kuinka usein
 |
| Toimintamalli epäiltäessä tai havaittaessa säädösten vastaista asiakastietojen käsittelyä | * kuvaus sisäisen valvonnan toimintatavoista liittyen mahdollisiin epäilyihin rikkomuksista
* kuvaus siitä kuinka toimitaan, jos lokitiedoista paljastuu virhetilanteita tai epäilyjä rikkomuksista tai epäasianmukaisesta käytöstä
 |
| Kelan lokitietojen saanti ja hankinta seurannan ja valvonnan toteuttamiseksi | * Kela voi luovuttaa luovutuslokirekisterin tietoja ko. rekisterin rekisterinpitäjälle ja reseptikeskuksen lokitietoja palvelunantajalle tai apteekille seurannan ja valvonnan toteuttamiseksi
* kuvaus toimintamallista ja käytännön menettelyistä
 |
| Muut seuranta- ja raportointimenettelyt | * listaa tähän muita mahdollisia menettelyjä, kuten esim. tietotilinpäätöksen hyödyntäminen rekisterinpitäjän osoitusvelvollisuuden täyttämisessä
 |

# 7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

## 7.1. Fyysinen turvallisuus osana tietojärjestelmien käyttöympäristön turvallisuutta

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

|  |  |
| --- | --- |
| Kulunvalvonta | * Miten huolehditaan toimitilojen lukitseminen ulkopuolisilta
* Kulunvalvonnan järjestelyt
 |
| Näyttöpäätteiden sijoittuminen ja suojaus | * Miten varmistetaan, ettei sivullisilla ole näköyhteyttä ruuduille (sijoittelu, näytönsuojakalvot, ym.)
* Näytön lukitsemiskäytännöt (käyttämättömän laitteen lukkiutumisaika, näytön lukitseminen työpisteeltä poistuttaessa)
* Muut suojaukseen liittyvät käytännöt, kuten salasanat
 |
| Aikarajat | * Kuinka ja millaisilla aikarajoilla määritellään istunnon aikakatkaisu tai käyttöliittymän lukittumisen aikaraja järjestelmissä, joissa käyttöliittymän käyttö on estettävä/lukittava
 |
| Ohjelmien ja sovellusten asentaminen | * Kenellä on oikeus asentaa ohjelmistoja ja sovelluksia yrityksen laitteille
* Kuinka varmistetaan, että vain nämä henkilöt pääsevät asentamaan ohjelmia ja sovelluksia
 |
| Ulkoiset kovalevyt ja muistitikut | * Sallitaanko ulkoisten kovalevyjen ja muistitikkujen käyttö
* Jos sallitaan, mitkä ovat niiden suojauskäytännöt, esim. vain yrityksen itse hankkimat tallennusvälineet, suojaus salasanalla ym.
* Kuinka estetään se, että ulkopuoliset toimijat eivät voi tuoda muistivälineitä työasemille tai sisäverkkoon (liittyy mm. haittaohjelmilta suojautumiseen)
 |
| Tulostin | * Sijaintipaikat
* Kuinka estetään ulkopuolisten pääsy tulostimille, mahdolliset turvatulostusratkaisut
 |
| Paperitulosteiden säilyttäminen | * Miten asiakastietoja sisältäviä paperitulosteita säilytetään paloturvallisesti lukittuna ja suojassa sivullisilta
 |
| Paperitulosteiden hävittäminen | * Niiden hävittäminen siten, etteivät sivulliset pääse tietoihin
* Hävittämisen käytännön ratkaisut, esim. lukittavat säilytysastiat ja paperisilppurit
* Tulostajan ja tulosteiden käyttäjän vastuut tulosteiden turvallisuudesta
 |
| Tietoteknisten turvakäytäntöjen mahdollinen hyödyntäminen kulunvalvonnassa | * Voi olla kuvattuna mallipohjan kohdassa 6.3
 |

## 7.2. Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden hallinta

Kirjoita suunnitelmaan, mitkä kohdat ovat yrityksen omaa toimintaa ja mistä asioista on sovittu sopimuskumppaneiden ja mahdollisten alihankkijoiden kanssa.

Työasemien, mobiililaitteiden ja käyttöympäristön tukipalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

Työasemat ja mobiililaitteet

|  |  |
| --- | --- |
| Virusturva | * Miten virusturvan toimivuus ja päivitykset on käytännössä varmistettu työasemilla (onko laitteissa virusturva, ovatko tarkistukset ajastettuja, kiinnitetäänkö raportteihin huomiota, ym.)
 |
| Mobiililaitteiden suojauskäytännöt | * Koskee puhelimia, tabletteja, kannettavia tietokoneita
* Esim. käyttäjätunnukset, salasanat, PIN-koodit, SIM-korttien hallinta ja laitteiden virusturvaohjelmat, kadonneiden mobiililaitteiden etälukitseminen ja/tai tyhjentäminen
 |

Käyttöympäristön tukipalvelut

|  |  |
| --- | --- |
| Käyttöjärjestelmä | * Kuinka tietokoneen päivityksistä huolehditaan
 |
| Huolto | * Kuka vastaa laitteiden huollosta
 |
| Muut ohjelmistot | * Esim. MS Office-päivitykset
* (Mahdolliset koventamiset, yhteentoimivuuden varmistaminen ja tilanteen seuranta sote-tietojärjestelmien kanssa)
 |

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

Kirjoita suunnitelmaan, mitkä palvelut ovat yrityksen omalla vastuulla ja mistä övastaa tietojärjestelmäpalvelun tuottaja tai kolmas osapuoli.

Alusta- ja verkkopalveluiden tietoturvallisuudesta huolehditaan seuraavasti:

Yleistä

|  |  |
| --- | --- |
| Luettelot käytössä olevista alusta- ja verkkopalveluista sekä niiden hallinnan vastuukysymykset ja lainmukaisuuden osoittaminen | * Luettelo palveluista tai maininta siitä, kuinka palvelut on listattu jossain muussa dokumentissa tai aiemmin tässä suunnitelmassa
* Maininta siitä, että vastuukysymykset on määritelty sopimuksissa
 |
| Varautuminen toimintaan poikkeustilanteissa ilman tietojärjestelmiä | * Kuvattuna mallipohjan kappaleessa 4
 |

Palvelimet ja palvelinympäristöt

Tähän kohtaan kasattavat tiedot löytyvät palvelinten ylläpitäjiltä. Tiedot saattavat olla kerrottuna sopimuksissa tai ne voi kysyä toimittajalta.

|  |  |
| --- | --- |
| Palvelut ja sovellukset | * mitä palveluita ja mitä sovelluksia palvelimilla on ja kuka vastaa niiden asentamisesta ja ylläpidosta
 |
| Haittaohjelmilta suojautuminen | * kuinka ne palvelimet, joilla tietojärjestelmät toimivat suojataan haittaohjelmilta
* millainen on haittaohjelmien torjunnassa olevien ohjelmien päivityskäytäntö
 |
| Oletustunnukset | * kuinka estetään se, ettei palvelinympäristössä ole aktiivisia oletustunnuksia tai muita oletuksena tulevia tietoturvallisuuden kannalta huonoja asetuksia
 |
| Päivittäminen | * kuinka palvelinten tietoturvapäivitysten asentaminen on kuvattu ja järjestetty
* miten päivitysten kriittisyys ja tarve arvioidaan
* miten päivitykset testataan ja hyväksytään erillisessä testausympäristössä ennen tuotantoympäristöön asentamista
 |

Tietoverkkojen hallinta, verkkolaitteet, langattomat verkot ja reitittimet

|  |  |
| --- | --- |
| Tietoliikenne | * Onko sopimuksissa otettu kantaa tietoturvaan liittyvistä vastuista
* Menettelyt häiriötilanteessa (esim. asiakaspalvelun yhteystiedot)
 |
| Verkon tietoturvallisuuskäytänteet | * Onko verkossa palomuuri
* Onko reitittimen päivityksistä ja suojauksesta huolehdittu
* Kenen vastuulla reitittimien ja muiden mahdollisten verkkolaitteiden päivitykset ja suojaus on
 |
| Langaton verkko | * Salasanakäytännöt (onko langattomassa verkossa salasana, kuinka usein sitä vaihdetaan, kenelle se annetaan)
* Tarjotaanko asiakkaille langaton verkko (jos tarjotaan, tulee sen olla erillinen yrityksen omasta verkosta)
 |

Etäyhteydet ja niiden tietoturva

Tässä voidaan viitata organisaation mahdollisiin etätyöohjeistuksiin, jossa vastaavia tietoturvaan ja tietosuojaan liittyviä asioita on käsitelty.

|  |  |
| --- | --- |
| Etätyökäytäntö | * Tehdäänkö yrityksessä etätöitä
* Ketkä yrityksessä tekevät etätöitä
 |
| Palvelut ja järjestelmät | * Mitä on sallittua käyttää etänä
* Miten muiden palveluiden käyttö on estetty
* Millaisilla yhteyksillä ja tietoturvaratkaisuilla etänä käytettyjä palveluja voi ja saa käyttää(esim. VPN-yhteydet)
* Mihin internettiä on sallittua käyttää työpaikan koneella (esim. työnteko ja koulutukset)
 |
| Huolto | * Miten laitteiden ja ohjelmistojen huollosta on huolehdittu etätyössä
 |
| Ohjeistus | * Miten henkilökuntaa on ohjeistettu etätyön käytännöistä
 |

Pilvipalvelut ja pilvipohjaiset ratkaisut

|  |  |
| --- | --- |
| Henkilötietojen käsittelyyn liittyvien riskien arviointi | * EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi
 |
| Henkilötietojen kolmansiin maihin siirtojen riskitason arviointi | * Kuvaus arvioinnista
* Organisatoriset, sopimuspohjaiset ja tekniset suojatoimet
* Tapaus- ja maakohtaisesti
 |
| Käytössä olevat pilvipalvelut | * Kuvaus palveluista
* Viittaukset sopimuksiin
 |
| Sopimusten ajantasaisuus | * Sopimusten tulee vastata voimassa olevia säädöksiä (mm. EU:n yleinen tietosuoja-asetus, tarvittaessa henkilötietojen siirtämisen perusteet ETA-alueen ulkopuolelle)
 |
| Seuranta | * Kuvaus alusta-, verkko- ja pilvipalveluiden tilanteen jatkuvasta ja säännöllisestä seurannasta
* Muun muassa toimivuuden, tietoturvallisuusriskien, häiriötilanteiden ja palveluiden käyttöehtojen näkökulmasta (sopimusten ja käytäntöjen päivittäminen muuttunutta tilannetta vastaavaksi)
 |
| Huolto-, päivitys- ja uusimissuunnitelmat | * Tietojärjestelmien, osajärjestelmien, laitekomponenttien, verkkojen sekä huolto- ja päivitystoimenpiteiden osalta
* Toimintamalli huoltotoimenpiteisiin liittyvään päätöksentekoon
 |
| Varautuminen | * Miten toimitaan, kun tiedon pitää olla käytettävissä myös poikkeusolosuhteissa
* Suunnitelmassa on kuvattava muun muassa, kuinka tiedon hallinnointi järjestetään mahdollisessa tilanteessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle
 |

# 8. Kanta-palvelujen liittymisen ja käytön tietoturvakäytännöt

Tämä kohta täydentyy, kun yritys liittyy käyttämään Kanta-palveluita. Osa tähän kohtaan kirjatuista tiedoista saattaa olla mainittuna jo aiemmin tässä suunnitelmassa, mutta ne on kuitenkin hyvä mainita uudelleen tässä (tai ainakin mainita, mistä suunnitelman kohdasta kyseinen tieto löytyy). Näin Kanta-palveluihin liittyvät käytännöt löytyvät kootusti tästä kappaleesta.

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

|  |  |
| --- | --- |
| Käyttäjien koulutus ja perehdytys | * kuinka käyttäjät koulutetaan tai perehdytetään tuntemaan Kanta-palvelut ja varmistetaan niiden tietoturvallinen käyttö
* esim. perehdytysmateriaali, verkkokoulut/kyselyt jne., ja kuinka varmistetaan, että perehdyttäminen on tehty, henkilöstön ohjeistukset (mm. tietojen lähettäminen viivytyksettä Kanta-palveluihin), asiakkaiden informointi
 |
| Kanta-palvelujen käytön seuranta | * toimintamalli Kanta-palvelujen käytön aktiivisesta seurannasta
 |
| Kanta-palvelujen edellyttämien tunnistamis- ja todentamisratkaisujen toteuttaminen | * Kanta-palveluja käyttävien järjestelmien kirjautumiskäytännöt
 |
| Sote-organisaatiorekisteritietojentai IAH-koodiston tietojen tarkastaminen | * organisaatio tarkastaa tiedot kansallisen koodistopalvelun Sote-organisaatiorekisteristä
* itsenäinen ammatinharjoittaja tarkastaa tiedot IAH-koodistosta
* 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
 |
| Käyttöoikeuksien/-valtuuksien hallinta ja kytkentä työntekijöiden työrooleihin | * myös seuraaviin rooleihin liittyvät oikeudet ja tehtävät: pääkäyttäjä(t), arkistonhoitaja(t), tietosuojavastaava(t)
 |
| Kanta-palvelujen ja niihin liittyvien järjestelmien käytön seuranta | * mukaan lukien asiakastietojen käyttölokin ja luovutuslokin seuranta (kuka/ketkä seuraavat, millä tavoin, kuinka usein)
 |
| Pääsynhallinta | * Kanta-palvelujen pääsynhallinnan toteuttaminen käytetyissä tietojärjestelmissä
 |
| Rekisterien erottaminen | * kuinka on toteutettu sosiaalihuollon ja terveydenhuollon dokumenttien ja eri rekisterien erottaminen
 |
| Kanta-palveluihin liittyvien tietojärjestelmien ja välityspalveluiden todistusten voimassaolon varmistaminen | * miten ja kuinka usein varmistetaan, että Kanta-palveluihin liittyvillä tietojärjestelmillä (erityisesti A2 tai A3-luokan järjestelmät) ja muilla sertifiointia edellyttävillä tietojärjestelmillä ja välityspalveluilla (luokan A1 järjestelmät) on voimassa oleva todistus tietoturvallisuuden arvioinnista, ja tiedot Valviran tietojärjestelmärekisterissä (A1, A2 tai A3-luokan järjestelmä)
 |
| Luokan A tietojärjestelmien vaatimustenmukaisuuden voimassaolon varmistaminen | * miten ja kuinka usein varmistetaan luokan A tietojärjestelmien vaatimustenmukaisuuden voimassaolo Valviran tietojärjestelmärekisteriä ja tietojärjestelmäpalvelun tuottajilta saatavia tietoja hyödyntäen (mm. tietoturvallisuustodistuksen voimassaolo, järjestelmään toteutetut olennaisten vaatimusten profiilit ja Kanta-palveluihin liittyneille järjestelmille tehtyjen yhteistestausten vastaavuus Kanta-palveluissa edellytettyihin määrittelyihin)
 |
| B-luokan järjestelmien tietojen ajantasaisuuden tarkistaminen | * miten ja kuinka usein varmistetaan, että muut sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitetut tietojärjestelmät on ilmoitettu Valviralle ja niiden tiedot ovat ajan tasalla Valviran tietojärjestelmärekisterissä (B-luokan järjestelmä)
 |
| Vaatimusten täyttymisen huomiointi uusia järjestelmiä hankittaessa | * kuinka varmistetaan, että hankittava tai päivitettävä järjestelmä täyttää sitä koskevat olennaiset vaatimukset
* (kuinka asia kuvataan sopimuksissa, mitä tarkistuksia tehdään esim. THL:n määräyksistä, järjestelmäprofiileista ja järjestelmältä vaadittavasta todistuksesta tietoturvallisuuden arvioinnista, Valviran tietojärjestelmärekisteristä ja Kelan yhteistestauksen tuloksista)
 |
| Menettelyt silloin, kun järjestelmän todistus tietoturvallisuuden arvioinnista perutaan tai rajoitetaan tai jos sen käyttö kielletään | * toiminta ja vastuut tilanteessa, jossa käytössä olevalta järjestelmältä peruutetaan todistus tietoturvallisuuden arvioinnista määräajaksi tai kokonaan, jossa todistusta rajoitetaan tai tilanteessa, jossa tietojärjestelmän käyttö kielletään
* kuvaus siitä kuinka asia huomioidaan sopimuksissa
 |

# 9. Tietojärjestelmäkohtaiset tarkemmat kuvakset, ohjeet ja suunnitelmat

Tämä kappale toimii yhteenvetona, jotta tärkeimmät tiedot löytyvät nopeasti. Jotkut kohdat voivat olla jo mainittuina kappaleessa 6. Siinä tapauksessa voit kirjoittaa niihin kohtiin mistä kohdasta kyseinen tieto löytyy.

Valviran sivustolta voit ladata Excel-taulukon josta voit tarkistaa, mihin luokkaan järjestelmä kuuluu:

<https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat/sosiaali-ja-terveydenhuollon-tietojarjestelmarekisteri>

Järjestelmä X = Luokka A2 ja A3, Kanta-palveluihin liittyvät järjestelmät

Järjestelmä X = Luokka A1, muusta syystä tietoturva-auditoidut järjestelmä

Järjestelmä Y = Luokka B, muut sosiaalihuollon asiakastietojen tai potilastietojen käsittelyyn tarkoitettu järjestelmät

Järjestelmä Z = Järjestelmät, jotka on muista syistä otettu huomioon tietoturvasuunnitelmassa

## 9.1. Järjestelmät X (luokkiin A2 ja A3 kuuluvat)

Järjestelmä

|  |  |
| --- | --- |
| Versio |  |
| Toimittaja |  |
| Yhteystiedot |  |
| Käyttötarkoitus |  |
| Käyttäjäryhmät |  |

|  |  |
| --- | --- |
| Käyttöohjeet |  |
| Ohjeiden päivittäminen ja jakelu |  |
| Menettelyt virhe- ja ongelmatilanteissa |  |
| Järjestelmäkohtaiset tukipalvelut |  |
| Asennus- ja ylläpitovastuut ja -vaatimukset |  |
| Menettelytavat ja vastuut virhe- ja poikkeustilanteissa |  |
| Käyttövaltuushallinta järjestelmässä |  |
| Tunnistautuminen järjestelmässä |  |
| Lokit |  |
| Järjestelmän lukittuminen |  |
| Kantaan liittyvän järjestelmän tietoturvallisuuden arviointia koskevan todistuksen tietojen varmistaminen (luokka A) |  |
| Järjestelmän tiedot Kelan testaustulokset sivulla (luokka A) |  |
| Järjestelmän tiedot Valviran tietojärjestelmärekisterissä | * + tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
	+ tietojärjestelmän tietoturvallisuustodistuksen voimassaolon päättymispäivä
	+ tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
	+ tietojärjestelmälle hyväksytysti suoritetut Kelan Kanta-palvelujen yhteistestaukset (Valviran tietojärjestelmärekisteristä ja/tai Kelan testaustulokset sivulta)
	+ Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat
 |

## 9.2. Järjestelmät X (luokkaan A1 kuuluvat)

Järjestelmä

|  |  |
| --- | --- |
| Versio |  |
| Toimittaja |  |
| Yhteystiedot |  |
| Käyttötarkoitus |  |
| Käyttäjäryhmät |  |
| Käyttöohjeet |  |
| Ohjeiden päivittäminen ja jakelu |  |
| Menettelyt virhe- ja ongelmatilanteissa |  |
| Järjestelmäkohtaiset tukipalvelut |  |
| Asennus- ja ylläpitovastuut ja -vaatimukset |  |
| Menettelytavat ja vastuut virhe- ja poikkeustilanteissa |  |
| Käyttövaltuushallinta järjestelmässä |  |
| Tunnistautuminen järjestelmässä |  |
| Lokit |  |
| Järjestelmän lukittuminen |  |
| Kantaan liittyvän järjestelmän tietoturvallisuuden arviointia koskevan todistuksen tietojen varmistaminen (luokka A) |  |
| Järjestelmän tiedot Kelan testaustulokset sivulla (luokka A) |  |
| Järjestelmän tiedot Valviran tietojärjestelmärekisterissä | * + tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
	+ tietojärjestelmän tietoturvallisuustodistuksen voimassaolon päättymispäivä
	+ tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
	+ mahdolliset maininnat järjestelmän osallistumisesta yhteistestaukseen osana laajempaa tietojärjestelmäkokonaisuutta (Valviran tietojärjestelmärekisteristä ja/tai Kelan testaustulokset sivulta)
	+ Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat
 |

## 9.3. Järjestelmät Y (luokkaan B kuuluvat)

Järjestelmä

|  |  |
| --- | --- |
| Versio |  |
| Toimittaja |  |
| Yhteystiedot |  |
| Käyttötarkoitus |  |
| Käyttäjäryhmät |  |

|  |  |
| --- | --- |
| Käyttöohjeet |  |
| Ohjeiden päivittäminen ja jakelu |  |
| Menettelyt virhe- ja ongelmatilanteissa |  |
| Järjestelmäkohtaiset tukipalvelut |  |
| Asennus- ja ylläpitovastuut ja -vaatimukset |  |
| Menettelytavat ja vastuut virhe- ja poikkeustilanteissa |  |
| Käyttövaltuushallinta järjestelmässä |  |
| Tunnistautuminen järjestelmässä |  |
| Lokit |  |
| Järjestelmän lukittuminen |  |
| Järjestelmän tiedot Valviran tietojärjestelmärekisterissä | * + Tietojärjestelmän tietojen tarkastusajankohta Valviran tietojärjestelmärekisteristä
	+ Tietojärjestelmään toteutetut olennaisten vaatimusten profiilit
	+ Valviran tietojärjestelmärekisteristä mahdollisesti löytyvät tietojärjestelmien käytössä tai käyttöönotossa huomioitavat asiat
 |

## 9.4. Järjestelmät Z (muut järjestelmät, jotka eivät kuulu luokkiin A tai B)

Järjestelmä

|  |  |
| --- | --- |
| Versio |  |
| Toimittaja |  |
| Yhteystiedot |  |
| Käyttötarkoitus |  |
| Käyttäjäryhmät |  |

|  |  |
| --- | --- |
| Käyttöohjeet |  |
| Ohjeiden päivittäminen ja jakelu |  |
| Menettelyt virhe- ja ongelmatilanteissa |  |
| Järjestelmäkohtaiset tukipalvelut |  |
| Asennus- ja ylläpitovastuut ja -vaatimukset |  |
| Menettelytavat ja vastuut virhe- ja poikkeustilanteissa |  |
| Käyttövaltuushallinta järjestelmässä |  |
| Tunnistautuminen järjestelmässä |  |
| Lokit |  |
| Järjestelmän lukittuminen |  |