**Pilvipalvelun tietoturvapolitiikka**

**Pilvipalvelu X**

v0.1

X.X.202X

# Sisällys

[Sisällys 2](#_Toc39687874)

[1. Dokumentin tarkoitus 3](#_Toc39687875)

[2. Omistajuus ja hallinta 3](#_Toc39687876)

[3. Vastuut ja organisointi 3](#_Toc39687877)

[3.1. Johdon rooli ja vastuut 3](#_Toc39687878)

[3.2. Palvelun omistajan rooli ja vastuut 3](#_Toc39687879)

[3.3. Tietohallinnon rooli ja vastuut 3](#_Toc39687880)

[3.4. Tietoturvapäällikön rooli ja vastuut 3](#_Toc39687881)

[4. Pilvipalvelun toteuttaminen 3](#_Toc39687882)

[4.1. Riskien hallinta ja vaatimuksenmukaisuus 3](#_Toc39687883)

[4.2. Palvelun vaatimusten määrittäminen 3](#_Toc39687884)

[4.2.1. Käyttäjä- ja pääsyoikeushallinta 3](#_Toc39687885)

[4.2.2. Tiedon suojaaminen 3](#_Toc39687886)

[4.2.3. Liiketoiminnan jatkuvuus ja saatavuus 4](#_Toc39687887)

[4.3. Hankinta 4](#_Toc39687888)

[4.4. Sopimuksen laatiminen 4](#_Toc39687889)

[4.5. Palvelun toteutus ja laadun seuranta 4](#_Toc39687890)

[4.6. Sopimuksen päättyminen 4](#_Toc39687891)

[5. Poikkeusten käsittely 4](#_Toc39687892)

# Dokumentin tarkoitus

Tämä dokumentti kuvaa <organisaation> pilvipalvelun <pilvipalvelu> tietoturvapolitiikan keskeiset piirteet

# Omistajuus ja hallinta

<kuvatkaa tähän, kuka omistaa tämän tietoturvapolitiikan ja miten sen elinkaarta hallitaan. Miten sen muutokset käsitellään ja hyväksytään>

# Vastuut ja organisointi

## Johdon rooli ja vastuut

<kuvatkaa tähän, mitkä ovat organisaation johdon roolit ja vastuu tämän tietoturvapolitiikan suhteen>

## Palvelun omistajan rooli ja vastuut

<kuvatkaa, kuka omistaa palvelun, jota pilvipalvelu tukee. Kuvatkaa, mitkä ovat palvelun omistajan vastuut pilvipalvelun suhteen>

## Tietohallinnon rooli ja vastuut

<kuvatkaa, mikä on tietohallinnon rooli ja vastuut kyseisen pilvipalvelun suhteen>

## Tietoturvapäällikön rooli ja vastuut

<kuvatkaa, mikä on tietoturvapäällikön tai ICT-tietoturvapäällikön rooli ja vastuut kyseisen pilvipalvelun suhteen>

# Pilvipalvelun toteuttaminen

## Riskien hallinta ja vaatimuksenmukaisuus

<kuvatkaa pilvipalveluun liittyvät riskit ja niihin liittyvät päävaatimukset sekä kontrollit. Kuvatkaa, miten vaatimusten mukaisuus varmistetaan. Pilvipalvelujen riskien tunnistamiseen voi hyödyntää Pilvipalvelujen soveltamisohjeen liitettä 4, Pilvipalvelujen yleiset riskit ja niiden kontrollit sekä Liitettä 5, Pilvipalvelujen riskienhallinnan vaatimusten tunnistamispohja>

## Palvelun vaatimusten määrittäminen

<kuvatkaa, miten palvelun vaatimukset on määritetty, nostakaa esiin keskeiset tietoturvaan ja jatkuvuuteen sekä varautumiseen liittyvät vaatimukset. Viitatkaa tarvittaessa tarkempaan vaatimusdokumentaatioon>

### Käyttäjä- ja pääsyoikeushallinta

<kuvatkaa pilvipalvelun käyttäjä- ja pääsyoikeuksienhallinnan periaatteet, ratkaisut ja toimintamallit>

### Tiedon suojaaminen

<kuvatkaa, miten palvelussa huolehditaan tietojen ja aineistojen suojaamisesta>

### Liiketoiminnan jatkuvuus ja saatavuus

<kuvatkaa liiketoiminnan jatkuvuuden ja saatavuuden keskeisimmät tarpeet ja vaatimukset sekä näiden varmistamisen pääkeinot>

## Hankinta

<kuvatkaa keskeiset hankintaa koskevat ehdot ja vaatimukset tietoturva- ja varautumisnäkökulmasta. Ks. myös Pilvipalvelun soveltamisohjeen luku 7 sekä Liite 6, Pilvipalvelujen soveltuvuuden tarkistuslista>

## Sopimuksen laatiminen

<kuvatkaa keskeiset sopimusta ja sopimuksen laatimista koskevat ehdot ja vaatimukset tietoturva- ja varautumisnäkökulmasta. Ks. myös Pilvipalvelun soveltamisohjeen luku 7 sekä Liite 6, Pilvipalvelujen soveltuvuuden tarkistuslista>

## Palvelun toteutus ja laadun seuranta

<kuvatkaa palvelun ja pilvipalvelun toteutukseen ja laadun seurantaan liittyvät keskeiset periaatteet ja mallit. Ks. myös Pilvipalvelun soveltamisohjeen luku 8>

## Sopimuksen päättyminen

<kuvatkaa pilvipalvelun sopimuksen päättymiseen liittyvät keskeiset periaatteet ja toimintamallit. Ks. myös Pilvipalvelun soveltamisohjeen luku 9.>

# Poikkeusten käsittely

<kuvatkaa, miten mahdolliset poikkeukset käsitellään – vastuut ja päätöksenteko>