| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>P15S | | | | | Asiakirjan nimi:<br>**Varmuuskopiointi- ja palautuspolitiikka** | | | | | | | |
| Versio:<br>1.0 | | Voimaantulopäivä:<br>01.01.2025 | | | Asiakirjan omistaja: | | | | | | | |
| X | Politiikka | | Standardi | | Menettely | | Lomake | | Rekisteri | | Muu | |

| **Muutoshistoria** | | | | |
|---|---|---|---|---|
| **Muutosnumero** | **Muutospäivä** | **Muutokset** | **Tarkistanut** | **Prosessin omistaja** |
| | | | | |
| | | | | |

| **Hyväksynnät** | | | |
|---|---|---|---|
| **Nimi** | **Tehtävänimike** | **Päivämäärä** | **Allekirjoitus** |
| | | | |
| | | | |

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

| Standardi/sääntely | Lauseke/artikla | Kommentti |
|---|---|---|
| ISO/IEC 27001:2022 | Lauseke 8 | Varmuuskopiointikontrollit tietoturvallisuuden hallintajärjestelmän vaatimusten mukaisesti |
| ISO/IEC 27002:2022 | Kontrollit 5.29, 8.13 | Varmuuskopioinnin parhaat käytännöt ja integrointi liiketoiminnan jatkuvuuteen |
| NIST SP 800-53 Rev. 5 | CP-9, MP-6 | Varmuuskopiointi ja tallennusvälineiden suojaus |
| EU:n NIS2-direktiivi | Artikla 21(2)(c) | Häiriönsietokyky ja jatkuvuus varmuuskopioinnin avulla |
| EU:n DORA-asetus | Artikla 10(1) | ICT-jatkuvuus – varmuuskopiointi finanssialan organisaatioille |
| COBIT 2019 | BAI04.05, DSS04 | Varmuuskopioiden dokumentointi ja testaus sekä prosessikontrollit |
| EU:n GDPR | Artiklat 5(1)(f), 32(1)(c) | Tietojen eheys, saatavuus ja oikea-aikainen palauttaminen |

**1. Tarkoitus**

1.1 Tämä politiikka määrittää, miten organisaatio toteuttaa ja hallinnoi varmuuskopiointia liiketoiminnan jatkuvuuden varmistamiseksi, tietojen menetyksen estämiseksi ja oikea-aikaisen palautumisen mahdollistamiseksi poikkeamatilanteista.

1.2 Se asettaa sitovat vaatimukset sille, miten järjestelmät ja tiedot on varmuuskopioitava, säilytettävä ja palautettava erityisesti pk-yrityksissä, joilla ei ole monimutkaista IT-infrastruktuuria.

1.3 Tämä politiikka tukee auditointivalmiutta ja ISO/IEC 27001 -sertifiointia varmistamalla, että olennaiset varmuuskopiointikontrollit on toteutettu, niitä sovelletaan johdonmukaisesti ja niitä katselmoidaan säännöllisesti.

1.4 Organisaation kyky palautua teknisistä vioista, tahattomasta poistamisesta tai kyberpoikkeamista riippuu tämän politiikan tiukasta noudattamisesta.

**2. Soveltamisala**

**2.1 Tämä politiikka koskee kaikkia liiketoimintajärjestelmiä ja tietoja, mukaan lukien:**

2.1.1 taloushallinnon tiedot, asiakastiedot ja henkilöstöhallinnon tiedot

2.1.2 pöytätietokoneet, kannettavat tietokoneet, palvelimet ja liiketoiminnassa käytettävät pilvipalvelut

2.1.3 varmuuskopiointivälineet, kuten USB-asemat, ulkoiset tallennusvälineet tai pilvipohjaiset varmuuskopiot

**2.2 Tämä politiikka koskee myös kaikkia henkilöitä, joilla on vastuu varmuuskopiointiprosessien toteuttamisesta tai hallinnoinnista, mukaan lukien:**

2.2.1 toimitusjohtaja tai muu nimetty vastuuhenkilö

2.2.2 ulkoiset IT-tukipalveluntarjoajat tai konsultit

2.2.3 kaikki työntekijät, jotka vastaavat tietojen tallentamisesta hyväksyttyihin sijainteihin

## 3. Tavoitteet

3.1 Varmistaa, että kaikki kriittiset liiketoimintatiedot ja järjestelmät varmuuskopioidaan turvallisesti asianmukaisin aikavälein riskien ja operatiivisten tarpeiden perusteella.

3.2 Varmistaa, että tiedot voidaan palauttaa häiriötilanteiden jälkeen oikea-aikaisesti ja täydellisesti.

3.3 Estää varmuuskopioitujen tietojen luvaton käyttö, muuttaminen tai menetys tehokkailla säilytyskontrolleilla.

3.4 Määrittää selkeästi roolit ja vastuut varmuuskopiointi- ja palautusmenettelyjen toteuttamiselle ja testaukselle sekä varmistaa niiden noudattaminen.

3.5 Tukea ISO/IEC 27001:n, EU:n GDPR:n ja muiden sääntelyvelvoitteiden noudattamista jäsennellyillä ja dokumentoiduilla varmuuskopiointikäytännöillä.

## 4. Roolit ja vastuut

### 4.1 Toimitusjohtaja

4.1.1 hyväksyy tämän politiikan ja varmistaa sen toimeenpanon

4.1.2 osoittaa resurssit ja nimeää vastuut varmuuskopiointi- ja palautustoiminnoille

4.1.3 katselmoi varmuuskopioinnin epäonnistumiset, poikkeamat ja politiikasta poikkeamiset

4.1.4 johtaa politiikan vuosittaista katselmointia ja varmistaa auditointivalmiuden

### 4.2 IT-tukipalveluntarjoaja (tarvittaessa)

4.2.1 toteuttaa ja hallinnoi varmuuskopiointiratkaisuja (paikallisia tai pilvipohjaisia)

4.2.2 seuraa varmuuskopiointien onnistumista ja aikatauluttaa palautustestit

4.2.3 raportoi epäonnistumiset ja poikkeamat suoraan toimitusjohtajalle

4.2.4 varmistaa salauksen, käyttöoikeusrajoitukset ja varmuuskopiointivälineiden asianmukaisen käsittelyn

[ ... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ... ]

## 9. Katselmointi- ja päivitysvaatimukset

### 9.1 Tämä politiikka on katselmoitava vähintään kerran vuodessa toimitusjohtajan toimesta. Katselmoinnin välittömiä käynnistäviä tekijöitä ovat:

9.1.1 merkittävät muutokset järjestelmissä tai säilytysmenetelmissä

9.1.2 uusien pilvi- tai IT-alustojen käyttöönotto

9.1.3 tietojen palauttamiseen vaikuttavat oikeudelliset tai sääntelyyn liittyvät muutokset

9.1.4 auditointien tai poikkeamien havainnot

9.2 Toimitusjohtaja vastaa katselmoinnin käynnistämisestä, muutosten hyväksymisestä ja päivityksistä tiedottamisesta.

9.3 Politiikan versioita on hallittava ja arkistoitava. Korvatut versiot on rajattava käyttöoikeuksin sekaannuksen välttämiseksi auditointien tai liiketoiminnan palautumistilanteiden aikana.

## 10. Liittyvät politiikat ja yhteydet

### 10.1 Tämä politiikka on yhdenmukainen seuraavien SME-politiikkojen kanssa ja riippuu niistä:

10.1.1 P14S – Tietojen säilytys- ja hävityspolitiikka: Määrittää, kuinka kauan varmuuskopioituja tietoja on säilytettävä ja miten ne poistetaan turvallisesti.

10.1.2 P13S – Tiedon luokittelu- ja merkintäpolitiikka: Auttaa priorisoimaan, mitkä tiedot on varmuuskopioitava tiedon luokittelutasojen perusteella.

10.1.3 P30S – Tietoturvapoikkeamien hallintapolitiikka: Kattaa menettelyt tilanteissa, joissa varmuuskopiointi epäonnistuu tai tietojen palauttaminen on tarpeen tietomurron tai palvelukatkoksen jälkeen.

10.1.4 P2S – Hallinnointirooleja ja vastuita koskeva politiikka: Määrittää selkeän toimivallan varmuuskopioinnin valvonnalle ja politiikan toimeenpanolle.

10.1.5 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Varmistaa, että henkilötietojen käsittely varmuuskopioinnin yhteydessä on oikeudellisten ja tietosuojavaatimusten mukaista.

## 11. Viitestandardit ja viitekehykset

### 11.1 ISO/IEC 27001

11.1.1 Lauseke 8.1: Varmuuskopiointijärjestelmien operatiivinen suunnittelu ja hallinta osana tietoturvallisuuden hallintajärjestelmää

### 11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.13: Määrittää parhaat käytännöt varmuuskopioinnin aikataulutukselle, seurannalle ja palauttamiselle

11.2.2 Liite A, kontrolli 5.29: Varmuuskopioinnin integrointi liiketoiminnan jatkuvuuteen ja palautumisvalmiuteen

### 11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (Varautumissuunnittelu): Määrittää jäsennetyt varmuuskopiointistrategiat liiketoiminnan häiriönsietokyvyn tueksi

11.3.2 MP-6 (Tallennusvälineiden suojaus): Edellyttää varmuuskopiointivälineiden turvallista käsittelyä ja hävittämistä

### 11.4 EU:n GDPR

11.4.1 Artikla 5(1)(f): Edellyttää henkilötietojen eheyttä ja saatavuutta

11.4.2 Artikla 32(1)(c): Edellyttää kykyä palauttaa henkilötietojen saatavuus oikea-aikaisesti

### 11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(c): Edellyttää varmuuskopiointia ja palautumista osana häiriönsietokyvyn ja jatkuvuuden suunnittelua

### 11.6 EU:n DORA-asetus

11.6.1 Artikla 10(1): Finanssialan organisaatioiden on varmistettava varmuuskopiointi osana ICT-jatkuvuustoimenpiteitä

### 11.7 COBIT 2019

11.7.1 BAI04.05: Edellyttää dokumentoituja varmuuskopiointistrategioita

11.7.2 DSS04.07: Korostaa rutiininomaista testausta sekä varmuuskopiointi- ja palautusprosessien hallintaa