| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>P30S | | | | | Asiakirjan nimi:<br>**Tietoturvapoikkeamien hallintapolitiikka** | | | | | | | |
| 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 | Kohta/artikla | Kommentti |
|---|---|---|
| ISO/IEC 27001:2022 | Kohdat 6.1, 6.3, 8 | poikkeamien hallinta, jatkuva parantaminen, operatiivinen ohjaus |
| ISO/IEC 27002:2022 | Kontrollit 5.24, 5.25 | poikkeamien havaitseminen, valmius, oppiminen |
| NIST SP 800-53 Rev.5 | IR-4, IR-5, IR-6 | poikkeamien käsittely ja seuranta, raportointi |
| EU:n GDPR | Artikla 33 | henkilötietojen tietoturvaloukkausten ilmoitusvaatimukset |
| EU:n NIS2-direktiivi | Artikla 23 | pakollinen kyberpoikkeamien ilmoittaminen |
| EU:n DORA-asetus | Artikla 17 | ICT-poikkeamien hallinta |
| COBIT 2019 | DSS02, DSS04 | palvelupyyntöjen ja poikkeamien hallinta sekä jatkuvuuden hallinta |

**1. Tarkoitus**

1.1. Tämä politiikka määrittää, miten organisaatio havaitsee, ilmoittaa ja käsittelee tietoturvapoikkeamia, jotka vaikuttavat sen digitaalisiin järjestelmiin, tietoihin tai palveluihin.

1.2. Politiikan tarkoituksena on minimoida vahingot, suojata asiakkaiden tiedot ja varmistaa sääntelyvelvoitteiden täyttäminen, kuten EU:n GDPR:n 72 tunnin ilmoitusvaatimus henkilötietojen tietoturvaloukkauksista.

1.3. Tämä politiikka varmistaa selkeät vastuut, viestintämenettelyt ja poikkeamien jälkiarvioinnin myös pienissä organisaatioissa, joilla ei ole erillistä tietoturvatiimiä.

**2. Soveltamisala**

**2.1. Tämä politiikka koskee:**

2.1.1. kaikkia työntekijöitä, toimeksisaajia ja ulkoisia IT-palveluntarjoajia

2.1.2. kaikkia yrityksen hallinnoimia järjestelmiä ja palveluja, mukaan lukien verkkosivustot, pilvialustat, mobiililaitteet, kannettavat tietokoneet ja sähköpostitilit

**2.1.3. kaikkia poikkeamatyyppejä, mukaan lukien:**

2.1.3.1. luvaton pääsy tietoihin tai järjestelmiin

2.1.3.2. haittaohjelmatartunnat tai kiristyshaittaohjelmat

2.1.3.3. tietojenkalastelu tai sosiaalisen manipuloinnin yritykset

2.1.3.4. järjestelmäkatkokset, jotka johtuvat kyberhyökkäyksestä tai väärinkäytöstä

2.1.3.5. arkaluonteisten tietojen tahaton paljastuminen tai poistaminen

2.1.3.6. liiketoiminnassa käytettävien laitteiden tai tallennusvälineiden katoaminen tai varkaus

**3. Tavoitteet**

3.1. Määrittää selkeä menettely tietoturvapoikkeamien tunnistamiseen ja eskalointiin.

3.2. Varmistaa, että tietoturvapoikkeamat ilmoitetaan, kirjataan ja käsitellään ennalta määritettyjen määräaikojen puitteissa.

3.3. Mahdollistaa vahinkojen nopea rajaaminen, tietojen palauttaminen ja palvelujen palauttaminen.

3.4. Varmistaa, että asianomaisille osapuolille, kuten asiakkaille ja viranomaisille, ilmoitetaan lain niin edellyttäessä.

3.5. Estää toistuminen juurisyyanalyysin, korjaavien toimenpiteiden ja politiikan kehittämisen avulla.

3.6. Mahdollistaa sen, että pk-yritys täyttää ISO 27001 -sertifioinnin vaatimukset ja voi auditoinneissa osoittaa vastuullisen toimintansa.

## 4. Roolit ja vastuut

### 4.1. Toimitusjohtaja

4.1.1. Omistaa tämän politiikan ja varmistaa sen toimeenpanon.

4.1.2. Valvoo tietoturvapoikkeamiin reagointia ja hyväksyy ilmoitukset viranomaisille tai asiakkaille.

4.1.3. Katselmoi poikkeamien jälkeiset raportit ja varmistaa, että politiikka päivitetään tarvittaessa.

4.1.4. Voi delegoida koordinointitehtäviä, mutta säilyttää kokonaisvastuun.

### 4.2. IT-palveluntarjoaja / järjestelmänvalvoja (sisäinen tai ulkoinen)

4.2.1. Havaitsee ja tutkii mahdolliset tietoturvapoikkeamat.

4.2.2. Toteuttaa rajaamis- ja palauttamistoimenpiteet (esim. poistaa käyttöoikeuksia käytöstä, palauttaa varmuuskopioita).

4.2.3. Ilmoittaa toimitusjohtajalle kaikista vahvistetuista tai epäillyistä tietoturvapoikkeamista yhden tunnin kuluessa niiden havaitsemisesta.

4.2.4. Ylläpitää poikkeamalokia, joka sisältää aikaleimat, vaikutusarvioinnit ja reagointitoimenpiteet.

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

## 9. Katselmointi- ja päivitysvaatimukset

### 9.1. Säännöllinen katselmointi

**9.1.1. Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran 12 kuukaudessa varmistaakseen:**

9.1.1.1. yhdenmukaisuuden ISO/IEC 27001:2022:n kontrollien kanssa

9.1.1.2. kyvyn vastata uusiin uhkiin, riskeihin ja tietoturvapoikkeamiin

9.1.1.3. lakisääteisten ja sopimusperusteisten velvoitteiden jatkuvan noudattamisen (esim. EU:n GDPR, EU:n DORA-asetus)

### 9.2. Käynnistävät tapahtumat

**9.2.1. Politiikka on katselmoitava ja päivitettävä myös seuraavien jälkeen:**

9.2.1.1. mikä tahansa vakavuudeltaan korkea tietoturvapoikkeama tai viranomaisilmoitus

9.2.1.2. uuden IT-infrastruktuurin käyttöönotto tai järjestelmämuutokset

9.2.1.3. tietoturvaloukkauksia koskevien lakisääteisten vaatimusten muutokset

### 9.3. Katselmoinnin dokumentointi ja jakelu

9.3.1. Kaikki katselmoinnit ja muutokset on dokumentoitava politiikan muutoslokiin.

9.3.2. Päivitetyt versiot on jaettava kaikille työntekijöille, toimittajille ja IT-palveluntarjoajille, jotka osallistuvat tietoturvaan tai järjestelmien operointiin.

9.3.3. Näyttö henkilöstön tietoisuudesta (esim. kokousmuistiot tai sähköpostivahvistukset) on säilytettävä auditointivalmiuden varmistamiseksi.

## 10. Liittyvät politiikat ja yhteydet

### 10.1. Tätä politiikkaa on sovellettava yhdessä seuraavien pk-yrityksen politiikkojen kanssa:

10.1.1. P1S – Tietoturvapolitiikka: määrittää yleiset vaatimukset luottamuksellisuuden, eheyden ja saatavuuden ylläpitämiselle toiminnan aikana, mukaan lukien tietoturvapoikkeamien käsittely.

10.1.2. P2S – Hallintoroolien ja -vastuiden politiikka: määrittää toimivallan ja vastuurakenteet tietoturvapoikkeamien havaitsemiselle, ilmoittamiselle ja eskaloinnille.

10.1.3. P4S – Pääsynhallintapolitiikka: mahdollistaa käyttöoikeuksien välittömän peruuttamisen tietoturvapoikkeamiin reagoinnin aikana.

10.1.4. P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: varmistaa, että kaikki työntekijät osaavat tunnistaa ja ilmoittaa tietoturvapoikkeamat tehokkaasti.

10.1.5. P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: ohjaa EU:n GDPR:n mukaisia tietoturvaloukkausten ilmoitusmenettelyjä ja tukee sääntelyvaatimusten noudattamista tietoturvapoikkeamien aikana.

10.1.6. P22S – Lokitus- ja valvontapolitiikka: tarjoaa tarvittavat työkalut ja näkyvyyden tietoturvatapahtumien havaitsemiseen, analysointiin ja auditointiin.

10.1.7. P31S – Todisteiden keruun ja forensiikan politiikka: tukee tietoturvapoikkeamiin liittyvien toimien tutkintaa ja oikeudellista puolustettavuutta ohjaamalla todentamisaineiston asianmukaista käsittelyä.

10.2. Nämä politiikat muodostavat yhdessä pk-yrityksen operatiivisen viitekehyksen tietoturvapoikkeamien havaitsemiseksi, niihin reagoimiseksi ja niistä palautumiseksi.

## 11. Viitestandardit ja viitekehykset

### 11.1. ISO/IEC 27001

11.1.1. Kohta 6.1 – edellyttää riskien käsittelyn suunnittelua, mukaan lukien varautuminen tietoturvapoikkeamiin.

11.1.2. Kohta 6.3 – tukee jatkuvaa parantamista tietoturvatapahtumista saatujen oppien avulla.

11.1.3. Kohta 8.1 – korostaa operatiivista ohjausta tietoturvapoikkeamien ja häiriöiden hallinnassa.

### 11.2. ISO/IEC 27002

11.2.1. Kontrolli 5.24 – edellyttää jäsenneltyä toimintamallia tietoturvapoikkeamien ilmoittamiseen, arviointiin ja käsittelyyn.

11.2.2. Kontrolli 5.25 – painottaa tietoturvapoikkeamista oppimista tulevan valmiuden ja järjestelmien häiriönsietokyvyn parantamiseksi.

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

11.3.1. IR-4 – määrittää poikkeamien käsittelymenettelyt, mukaan lukien rajaaminen ja palautuminen.

11.3.2. IR-5 – määrittää vaatimukset poikkeamien seurantaan ja analysointiin.

11.3.3. IR-6 – edellyttää ulkoisia ja sisäisiä poikkeamien ilmoitusmenettelyjä.

### 11.4. EU:n GDPR

11.4.1. Artikla 33 – edellyttää henkilötietojen tietoturvaloukkausten ilmoittamista viranomaisille 72 tunnin kuluessa sekä tietoja niiden laajuudesta ja lieventämistoimenpiteistä.

### 11.5. EU:n NIS2-direktiivi (2022/2555)

11.5.1. Artikla 23 – edellyttää, että keskeiset ja tärkeät toimijat ilmoittavat merkittävistä poikkeamista toimivaltaisille viranomaisille standardoiduilla ilmoitusmuodoilla.

### 11.6. EU:n DORA-asetus (2022/2554)

11.6.1. Artikla 17 – edellyttää, että finanssialan toimijat luokittelevat, ilmoittavat ja seuraavat ICT:hen liittyviä poikkeamia ja häiriöitä.

### 11.7. COBIT 2019

11.7.1. DSS02 – palvelupyyntöjen ja poikkeamien hallinta: ohjaa operatiivisten ja tietoturvapoikkeamien tehokasta käsittelyä hallintatavoitteiden mukaisesti.

11.7.2. DSS04 – jatkuvuuden hallinta: yhdistää tietoturvapoikkeamiin reagoinnin laajempiin jatkuvuus- ja palautumisstrategioihin.