| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>P19S | | | | | Asiakirjan nimi:<br>**Haavoittuvuuksien ja korjauspäivitysten 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/säädös | Kohta/artikla | Kommentti |
|---|---|---|
| ISO/IEC 27001:2022 | Kohta 8 | |
| ISO/IEC 27002:2022 | Kontrollit 8.8, 8.9 | |
| NIST SP 800-53 Rev.5 | RA-5, SI-2, CM-2 | |
| EU:n NIS2-direktiivi | Artiklat 21(2)(d), 21(2)(e) | |
| EU:n DORA-asetus | Artiklat 8(1), 10(2) | |
| COBIT 2019 | DSS05.02, APO12 | |
| EU:n GDPR | Artikla 32(1)(b) | |

**1. Tarkoitus**

1.1 Tässä politiikassa määritetään, miten organisaatio tunnistaa, arvioi ja lieventää järjestelmiin, sovelluksiin ja infrastruktuuriin kohdistuvia haavoittuvuuksia.

1.2 Tämän politiikan tarkoituksena on vähentää kyberturvallisuusriskiä edellyttämällä oikea-aikaista paikkausta ja riskiperusteisia korjaavia toimenpiteitä, jotka soveltuvat pk-yrityksille.

1.3 Tämä politiikka tukee ISO/IEC 27001:2022 -sertifioinnin mukaista vaatimustenmukaisuutta ja auttaa täyttämään EU:n GDPR:n, EU:n NIS2-direktiivin ja EU:n DORA-asetuksen mukaiset sääntelyvelvoitteet edellyttämällä teknisten haavoittuvuuksien ennakoivaa hallintaa.

1.4 Organisaatio tunnistaa, että paikkaamattomat järjestelmät muodostavat merkittävän tietoturvauhan, ja ne on käsiteltävä järjestelmällisesti ja viipymättä.

**2. Soveltamisala**

**2.1 Tämä politiikka koskee seuraavia:**

2.1.1 Kaikkia organisaation käyttämiä palvelimia, pöytätietokoneita, kannettavia tietokoneita, mobiililaitteita, verkkolaitteita ja pilvipalvelualustoja

2.1.2 Kaikkia liiketoiminnassa käytettäviä käyttöjärjestelmiä, kolmannen osapuolen ohjelmistoja, lisäosia ja sovelluksia

2.1.3 Sisäistä IT-henkilöstöä tai ulkoisia palveluntarjoajia, jotka vastaavat järjestelmien ylläpidosta, päivityksistä tai valvonnasta

2.1.4 Kaikkea organisaation tai sen puolesta ylläpidettyä räätälöityä koodia tai sulautettua ohjelmistoa

2.2 Politiikka kattaa sekä organisaation suoraan hallinnoiman infrastruktuurin että sopimuskumppanien tai hosting-palveluntarjoajien ylläpitämät järjestelmät.

**3. Tavoitteet**

3.1 Tunnistaa ja arvioida tunnetut haavoittuvuudet kaikissa IT-omaisuuserissä oikea-aikaisesti ja yhdenmukaisesti

3.2 Toteuttaa korjauspäivitykset ja ohjelmistopäivitykset vakavuuden sekä organisaation toimintaan tai henkilötietoihin kohdistuvan riskin perusteella

3.3 Estää teknisten heikkouksien hyväksikäyttö, joka voisi johtaa palveluhäiriöön, henkilötietojen tietoturvaloukkaukseen tai sääntelyvaatimusten noudattamatta jättämiseen

3.4 Ylläpitää tarkkoja tietoja toteutetuista korjauspäivityksistä, avoimista asioista ja poikkeuksista auditointivalmiuden varmistamiseksi

3.5 Käyttää organisaation kokoon ja toiminnan monimutkaisuuteen soveltuvia työkaluja ja menettelyjä vaikuttavuutta vaarantamatta

3.6 Tukea lakiin ja sääntelyyn perustuvaa vaatimustenmukaisuutta, mukaan lukien EU:n GDPR:n artikla 32 ja ISO:n liitteen A kontrolli 8

**4. Roolit ja vastuut**

**4.1 Toimitusjohtaja**

4.1.1 Vastaa kokonaisuudessaan siitä, että paikkauksen ja haavoittuvuuksien hallinnan toimenpiteitä sovelletaan

4.1.2 Hyväksyy riskipoikkeukset tilanteissa, joissa korjauspäivityksiä ei voida toteuttaa, ja katselmoi niihin liittyvät lieventämisstrategiat

4.1.3 Katselmoi paikkauksen tilaraportit ja varmistaa, että resurssit ovat käytettävissä paikkausvelvoitteiden täyttämiseksi

**4.2 IT-tukipalveluntarjoaja / sisäinen IT-järjestelmänvalvoja**

4.2.1 Seuraa järjestelmien haavoittuvuuksia ja saatavilla olevia korjauspäivityksiä toimittajahälytysten, uhkatiedotteiden ja käyttöjärjestelmätason ilmoitusten avulla

4.2.2 Toteuttaa käyttöjärjestelmä-, laiteohjelmisto- ja sovelluspäivitykset määritettyjen määräaikojen puitteissa

4.2.3 Ylläpitää muodollista korjauspäivityslokia ja dokumentoi ratkaisemattomat tai lykätyt päivitykset

4.2.4 Suorittaa kriittisten päivitysten testauksen ja aikataulutuksen toimintahäiriöiden minimoimiseksi

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

**9. Katselmointi- ja päivitysvaatimukset**

**9.1 Vuosittainen katselmointi**

9.1.1 Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa IT-palveluntarjoajan ja tietosuojakoordinaattorin antaman palautteen perusteella

**9.2 Katselmoinnin käynnistävät tapahtumat**

**9.2.1 Välikatselmointi on tehtävä, jos:**

9.2.1.1 Merkittävä haavoittuvuus tai hyväksikäyttömenetelmä vaikuttaa soveltamisalaan kuuluviin järjestelmiin

9.2.1.2 Järjestelmiin tai ohjelmistoihin tehdään merkittäviä muutoksia

9.2.1.3 Auditoinnissa tunnistetaan puutteita korjauspäivitysprosesseissa

9.2.1.4 Korjauspäivityksiin liittyvä poikkeama tai tietoturvaloukkaus kirjataan

**9.3 Politiikan versionhallinta**

9.3.1 Kaikki päivitykset on kirjattava versiolokiin yhdessä muutosten yhteenvedon kanssa

9.3.2 Muutoksista on tiedotettava niille henkilöille, joita ne koskevat

9.3.3 Vanhentuneet versiot on arkistoitava rajoitetuin käyttöoikeuksin

**10. Liittyvät politiikat ja yhteydet**

**10.1 Tämä politiikka tukee useita muita pk-yrityksen politiikkoja ja on riippuvainen niistä:**

10.1.1 P12S – Omaisuudenhallintapolitiikka: tunnistaa järjestelmäomistajuuden ja luokittelun sekä varmistaa, että kaikki paikkausta edellyttävät omaisuuserät on tunnistettu ja sisällytetty omaisuusluetteloon

10.1.2 P14S – Tietojen säilytys- ja hävityspolitiikka: varmistaa, että käytöstä poistettaviksi suunnitellut järjestelmät päivitetään turvallisesti tai tyhjennetään, mikä vähentää haavoittuvuusaltistusta

10.1.3 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: priorisoi haavoittuvuuksien korjaavat toimenpiteet henkilötietoja käsitteleville järjestelmille tietosuojalainsäädännön noudattamiseksi

10.1.4 P22S – Lokitus- ja valvontapolitiikka: tukee paikkaamattomien järjestelmien tai epäilyttävän toiminnan havaitsemista, mikä voi viitata haavoittuvuuden hyväksikäyttöön

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää menettelyt haavoittuvuuksiin reagoimiseksi silloin, kun ne johtavat tietoturvapoikkeamiin, mukaan lukien eskalointi- ja raportointivaiheet

## 11. Viitestandardit ja viitekehykset

### 11.1 ISO/IEC 27001

11.1.1 Kohta 8.1 – edellyttää kontrollien toteuttamista operatiivisten riskien, mukaan lukien haavoittuvuuksien hallinnan, käsittelemiseksi

### 11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.8 – määrittää menettelyt järjestelmien tunnettujen heikkouksien skannaamiseksi ja korjaamiseksi

11.2.2 Kontrolli 8.9 – korostaa turvallista konfigurointia, korjauspäivitysten validointia ja muutoksenhallintaa uusien altistusten välttämiseksi päivitysten aikana

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

11.3.1 RA-5 – edellyttää haavoittuvuuksien tunnistamista ja korjaavia toimenpiteitä määritettyjen määräaikojen puitteissa

11.3.2 SI-2 – edellyttää korjauspäivitysten ja päivitysten viivytyksetöntä toteutusta vakavuuden perusteella

11.3.3 CM-2 – ohjaa järjestelmien peruskonfiguraatioita ja päivitysdokumentaatiota yhdenmukaisen suojaustason varmistamiseksi

### 11.4 EU:n GDPR

11.4.1 Artikla 32(1)(b) – edellyttää organisaatioilta asianmukaisten teknisten toimenpiteiden toteuttamista, mukaan lukien paikkauksen, käsittelyn turvallisuuden ylläpitämiseksi

### 11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(d) – edellyttää haavoittuvuuksien käsittelyä järjestelmällisen skannauksen ja korjaavien toimenpiteiden avulla

11.5.2 Artikla 21(2)(e) – velvoittaa turvalliseen konfigurointiin ja korjauspäivitysten hallintaan ICT:n häiriönsietokyvyn varmistamiseksi

### 11.6 EU:n DORA-asetus

11.6.1 Artikla 8(1) – edellyttää ICT-riskien, mukaan lukien teknisten haavoittuvuuksien, havaitsemista ja lieventämistä

11.6.2 Artikla 10(2) – velvoittaa finanssialan toimijat korjaamaan ICT-järjestelmiin ja -toimintoihin vaikuttavat heikkoudet

### 11.7 COBIT 2019

11.7.1 DSS05.02 – edellyttää tunnettujen teknisten haavoittuvuuksien käsittelyä turvallisen toiminnan ylläpitämiseksi

11.7.2 APO12.01 – yhdenmukaistaa riskienhallinnan järjestelmien heikkouksien ennakoivan seurannan ja korjaamisen kanssa