Päivityspolitiikka

**Luokitus**: Sisäinen

Tätä asiakirjaa ei saa jakaa [Yrityksen] ulkopuolelle ilman omistajan kirjallista lupaa.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Versio | Päivitetty | Muokkaaja | Asiakirjan muutokset | Hyväksyjä | Omistaja |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Sisällysluettelo

[Tämän asiakirjan tarkoitus 3](#_Toc200967075)

[Vastuut 3](#_Toc200967076)

[Politiikka 3](#_Toc200967077)

[Miksi päivittää? 3](#_Toc200967078)

[Päivitykset ja tietoturvapäivitykset 3](#_Toc200967079)

[Kriittiset päivitykset 4](#_Toc200967080)

[Poikkeukset 4](#_Toc200967081)

# Tämän asiakirjan tarkoitus

Tämä politiikka määrittelee päivitystenhallintakäytännöt koko organisaatiossa varmistaen, että tiedot on suojattu vanhentuneilta ohjelmistoilta ja haavoittuvuuksilta.

# Vastuut

**Tietoturvaryhmä:**

* Varmistaa tämän politiikan ylläpidon ja noudattamisen valvonnan sekä suorittaa säännöllisiä tarkastuksia politiikan tehokkuuden varmistamiseksi.

**IT-osasto:**

* Varmistaa, että kaikki laitteet skannataan säännöllisesti vaatimustenmukaisuuden ja haavoittuvuuksien osalta.
* Kaikkien toimittajien päivitykset arvioidaan kriittisyyden osalta ja asennetaan vähintään viikoittain.
* Kriittiset päivitykset tulee asentaa mahdollisimman nopeasti ja turvallisesti.

**Muutostenhallintaryhmä (tai vastaava):**

* Arvioi ja hyväksyy hätäpäivitykset *muutostenhallintapolitiikassa* määritellyn mukaisesti.
* Tarkistaa kaikki *päivityspolitiikalle* ehdotetut poikkeukset.

**Kolmannet osapuolet:**

* Kaikkien [Yritys] puolesta järjestelmiä tukevien toimittajien tulee varmistaa haavoittuvuuspäivitysten nopea toteuttaminen tai ilmoittaa [Yritys] IT-osastolle ja tietoturvaryhmälle mahdollisimman pian.

**Kaikki työntekijät:**

* Päivittävät työtehtävissä käytettävien henkilökohtaisten laitteiden sovellukset ja käyttöjärjestelmät, jotta ne ovat aina uusimmassa versiossa eivätkä aiheuta tietoturvauhkaa organisaatiolle.

# Politiikka

### Miksi päivittää?

* Ilman tehokasta päivitystenhallintaa organisaatiossa on riski tietoturvapoikkeamille, joita hakkerit, virukset ja haittaohjelmat voivat aiheuttaa hyödyntämällä tunnettuja järjestelmähaavoittuvuuksia.
* Vanhentuneet ohjelmistot ja ajurit voivat tehdä järjestelmistä epävakaita ja heikentää niiden suorituskykyä.

### Päivitykset ja tietoturvapäivitykset

|  |  |
| --- | --- |
| **Palvelu** | **Päivitystiheys** |
| Microsoft Palvelimet ja työasemat | Microsoft julkaisee päivityksiä joka kuukauden 2. tiistai.  Ei-kriittiset päivitykset tehdään 30 päivän välein (kuukauden 4. tiistai) -testauksen jälkeen. |
| Palomuurit | Päivitykset asennetaan automaattisesti toimittajajulkaisun yhteydessä työajan ulkopuolella, loppukäyttäjähäiriöiden minimoimiseksi. |
| Verkon pääsyliittymät | Asennetaan automaattisesti toimittajajulkaisun yhteydessä. |
| Tulostimet | Toimittajapäivitykset asennetaan automaattisesti aina kun mahdollista. |
| Matkapuhelimet ja mobiililaitteet | Asennetaan automaattisesti toimittajajulkaisun yhteydessä. |

### Kriittiset päivitykset

* Kaikki kriittiset päivitykset tulee tarkistaa valmistajan julkaisun yhteydessä ja toteuttaa mahdollisimman pian, viimeistään kymmenen työpäivän kuluessa julkaisusta.

### Poikkeukset

* Jos [Yritys] katsoo, että tässä politiikassa määritellyistä toimista on pakottava tarve tehdä poikkeus, pyyntö voidaan tehdä ottamalla yhteyttä IT-osastoon. Poikkeukset on eskaloitava muutostenhallintaryhmälle varmistaakseen, että mahdolliset tai poikkeavat lisätoimet toteutetaan ja liiketoiminta hyväksyy mahdolliset jäljelle jäävät riskit.