					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P20S					Asiakirjan nimi: **Päätelaitesuojaus - haittaohjelmapolitiikka**							
Versio: 1.0		Voimaantulopäivä: 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	Operatiiviset kontrollit haittaohjelmasuojaukseen
ISO/IEC 27002:2022	Kontrolli 8	Päätelaitesuojauksen hallintatoimenpiteet
NIST SP 800-53 Rev.5	SI-3, SI-4	Haitallisen koodin suojaus ja tietoturvapoikkeamiin reagointi
EU:n NIS2-direktiivi	Artiklat 21(2)(d), (e)	Haittaohjelmien hallinta ja riskienhallinta keskeisille ja tärkeille toimijoille
EU:n DORA-asetus	Artiklat 10(1), 15	Operatiivinen häiriönsietokyky ja kolmansien osapuolten varmentaminen
COBIT 2019	DSS05.02, DSS05.04	Päätelaite- ja verkkosuojaus sekä seuranta
EU:n GDPR	Artiklat 32(1)(b), 33	Tekniset ja organisatoriset toimenpiteet sekä tietoturvaloukkauksista ilmoittaminen

1. Tarkoitus

1.1 Tämä politiikka määrittää vähimmäisvaatimukset teknisille, menettelyllisille ja käyttäytymiseen liittyville toimenpiteille, joilla kaikki päätelaitteet — kuten kannettavat tietokoneet, pöytäkoneet, mobiililaitteet ja siirrettävät tietovälineet — suojataan haitalliselta koodilta, mukaan lukien virukset, kiristyshaittaohjelmat, vakoiluohjelmat, rootkit-ohjelmat ja muut haittaohjelmauhat.

1.2 Tämän politiikan tarkoituksena on varmistaa, että päätelaitteet varustetaan, ylläpidetään ja niitä käytetään tavalla, joka vähentää haittaohjelmatartuntojen, niiden leviämisen ja järjestelmien vaarantumisen riskiä.

1.3 Organisaatio tunnistaa, että päätelaitteet ovat yleisiä haittaohjelmien sisääntulopisteitä, ja siksi ne on kovennettava, niitä on valvottava ja suojattava kerroksellisen puolustuksen keinoin.

1.4 Tämä politiikka tukee organisaation ISO/IEC 27001:2022 -sertifiointitavoitteita ja on yhdenmukainen EU:n GDPR:n, EU:n NIS2-direktiivin, EU:n DORA-asetuksen ja muiden soveltuvien viitekehysten kanssa.

2. Soveltamisala

2.1 Tämä politiikka koskee:

2.1.1 kaikkia organisaation päätelaitteita, mukaan lukien pöytäkoneet, kannettavat tietokoneet, tabletit, matkapuhelimet ja myyntipäätteet

2.1.2 henkilökohtaisia laitteita, joita käytetään liiketoimintasovellusten tai tietojen käyttöön (BYOD)

2.1.3 siirrettäviä tallennusvälineitä, kuten USB-muisteja ja ulkoisia kiintolevyjä

2.1.4 näillä alustoilla toimivia käyttöjärjestelmiä, päätelaiteohjelmistoja ja viestintätyökaluja

2.2 Tätä politiikkaa sovelletaan yhtä lailla seuraaviin:

2.2.1 sisäinen henkilöstö, sopimuskumppanit, harjoittelijat ja hallinnoidut palveluntarjoajat (MSP)

2.2.2 laitteet, joita käytetään toimipaikalla, etänä tai hybridityössä

2.2.3 pilveen liitetyt tai offline-tilassa olevat päätelaitteet, joihin tallennetaan liiketoimintatietoja tai henkilötietoja

3. Tavoitteet

3.1 Estää haittaohjelmatartunnat ja niiden leviäminen sisäisissä järjestelmissä, käyttäjälaitteissa ja ulkoisissa yhteyksissä

3.2 Havaita ja rajata haittaohjelmiin liittyvät uhat nopeasti automatisoitujen päätelaitesuojausteknologioiden ja määriteltyjen eskalointipolkujen avulla

3.3 Varmistaa, että liiketoimintatietojen käyttöön käytetään vain valtuutettuja, suojattuja ja valvottuja laitteita

3.4 Määrittää selkeät henkilöstön vastuut ja toimintaohjeet haittaohjelmiin liittyvien poikkeamien riskin vähentämiseksi

3.5 Ylläpitää jäljitettäviä ja todennettavissa olevia tallenteita haittaohjelmahavainnoista, vasteista ja politiikan noudattamisesta

3.6 Suojata henkilötiedot ja liiketoimintatiedot vaarantumiselta haittaohjelmia vastaan kerroksellisen puolustuksen strategioilla

4. Roolit ja vastuut

4.1 toimitusjohtaja

4.1.1 omistaa tämän politiikan ja varmistaa, että päätelaitesuojaukseen on käytettävissä riittävät resurssit

4.1.2 hyväksyy virustorjuntaohjelmistot, mobiililaitteiden hallintatyökalut (MDM) ja kolmansien osapuolten pääsyä koskevat säännöt

4.1.3 katselmoi päätelaitteisiin liittyvät haittaohjelmapoikkeamaraportit, vaikutusyhteenvedot ja tietoturvaloukkausilmoitukset

4.2 IT-tukipalveluntarjoaja / sisäinen IT-vastaava

4.2.1 valitsee ja ottaa käyttöön virustorjunta-, haittaohjelmien torjunta- sekä päätelaitteiden havainnointi- ja reagointiratkaisut (EDR)

4.2.2 varmistaa, että päivitykset otetaan käyttöön johdonmukaisesti ja että lokit säilytetään

4.2.3 reagoi haittaohjelmahälytyksiin, eristää tartunnan saaneet järjestelmät ja toteuttaa korjaavat toimenpiteet

4.2.4 toteuttaa kontrollit USB-laitteiden ja ulkoisten laitteiden käytölle

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vuosittainen katselmointivaatimus

9.1.1 toimitusjohtajan on katselmoitava tämä politiikka muodollisesti vähintään kerran vuodessa yhteistyössä IT-tukipalveluntarjoajan ja tietosuojakoordinaattorin kanssa

9.2 Heräteperusteiset päivitykset

9.2.1 politiikka on päivitettävä myös silloin, kun:

9.2.1.1 uusi merkittävä haittaohjelmauhka tai laajamittainen haittaohjelmaesiintyminen kohdistuu organisaation käyttämiin päätelaitteisiin

9.2.1.2 virustorjunta- tai EDR-työkaluja muutetaan, päivitetään tai vaihdetaan

9.2.1.3 haittaohjelmapoikkeama paljastaa puutteita tämän politiikan soveltamisalassa tai toimeenpanossa

9.2.1.4 lainsäädännöllisiä tai sääntelyyn liittyviä vaatimuksia (esim. EU:n GDPR, EU:n DORA-asetus, EU:n NIS2-direktiivi) päivitetään

9.3 Versionhallinta ja viestintä

9.3.1 kaikki politiikkamuutokset on dokumentoitava versionumerolla, päivämäärällä ja muutosten yhteenvedolla

9.3.2 henkilöstölle on tiedotettava päivityksistä, erityisesti jos ne muuttavat toiminnallisia tai käyttäytymiseen liittyviä vaatimuksia

9.3.3 aiemmat versiot on säilytettävä politiikka-arkistossa vähintään kolme vuotta auditointien tukemiseksi

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka on toimeenpantava yhdessä seuraavien pk-yrityksen politiikkojen kanssa:

10.1.1 P9S – Etätyöpolitiikka: varmistaa, että päätelaitesuojauksen vaatimuksia sovelletaan laitteisiin, joita käytetään toimipaikan ulkopuolella tai hybridityössä

10.1.2 P12S – Omaisuudenhallintapolitiikka: tukee kaikkien päätelaitteiden seurantaa ja hallintaa sekä varmistaa, että käytössä ovat vain valtuutetut ja suojatut laitteet

10.1.3 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: vahvistaa haittaohjelmien torjunnan keskeiseksi tietosuojakontrolliksi henkilötietojen ja arkaluonteisten tietojen suojaamiseksi vaarantumiselta

10.1.4 P22S – Lokitus- ja valvontapolitiikka: määrittää vaatimukset haittaohjelmatapahtumien lokitukselle ja hälytysten näkyvyyden ylläpitämiselle varhaista reagointia varten

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää eskaloinnin, rajaamisen ja ulkoisten ilmoitusten vaiheet, jos haittaohjelma johtaa tietojen vaarantumiseen tai operatiiviseen häiriöön

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 8.1 – edellyttää operatiivisten kontrollien toteutusta haittaohjelmahyökkäysten kaltaisten riskien vähentämiseksi

11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.7 – kuvaa haittaohjelmien hallintakäytännöt, mukaan lukien virustorjunta, reaaliaikainen tarkistus, päivitykset ja käyttäjäkoulutus

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – edellyttää haitallisen koodin suojausmekanismien käyttöönottoa kaikissa päätelaitteissa

11.3.2 SI-4 – edellyttää päätelaitetasolla tapahtuvien uhkien ja hälytysten seurantaa, havaitsemista, analysointia ja niihin reagointia

11.4 EU:n GDPR

11.4.1 Artikla 32(1)(b) – edellyttää teknisiä ja organisatorisia kontrollitoimenpiteitä (kuten virustorjuntaa) henkilötietojen suojaamiseksi

11.4.2 Artikla 33 – velvoittaa ilmoittamaan tietoturvaloukkauksesta, kun haittaohjelma vaarantaa tietojen eheyden, luottamuksellisuuden tai saatavuuden

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(d) – edellyttää toimenpiteitä haittaohjelmauhkiin ehkäisemiseksi ja niihin reagoimiseksi keskeisissä ja tärkeissä toimijoissa

11.5.2 Artikla 21(2)(e) – edellyttää kerroksellisia kyberturvallisuuden riskienhallintastrategioita, mukaan lukien päätelaitteiden haittaohjelmasuojaus

11.6 EU:n DORA-asetus

11.6.1 Artikla 10(1) – edellyttää ICT-järjestelmien suojaamista haittaohjelmilta ja muilta uhkilta osana operatiivista häiriönsietokykyä

11.6.2 Artikla 15 – velvoittaa finanssialan organisaatioita varmentamaan haittaohjelmasuojauksen kolmannen osapuolen palveluntarjoajilla

11.7 COBIT 2019

11.7.1 DSS05.02 – korostaa suojaavia toimenpiteitä päätelaitteiden ja verkkojen puolustamiseksi haittaohjelmauhkilta

11.7.2 DSS05.04 – tukee haittaohjelmiin liittyvien tietoturvatapahtumien seurantaa ja hälytyksiä osana jatkuvaa toimintaa