					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P20					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/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	Päätelaitesuojaus ja haittaohjelmien torjuntaa koskevat kontrollit ovat tarpeen ISMS:n tavoitteiden saavuttamiseksi
ISO/IEC 27002:2022	Kontrollit 8.7, 8	Tarjoaa tekniset kontrollit ja ohjeistuksen haittaohjelmien torjuntaan, päätelaitesuojaukseen ja poikkeamien hallintaan
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Määrittää haitallisen koodin suojauksen, keskitetyn valvonnan ja peruskonfiguraatiovaatimukset
EU:n GDPR	Artikla 32	Edellyttää asianmukaisia teknisiä toimenpiteitä henkilötietojen suojaamiseksi, mukaan lukien suojaus haittaohjelmia vastaan
EU:n NIS2-direktiivi	Artikla 21(2)(d)	Edellyttää päätelaitetason uhkien havaitsemisen ja ennaltaehkäisevien toimenpiteiden käyttöönottoa
EU:n DORA-asetus	Artikla 9	Edellyttää ICT-riskien hallintaa haittaohjelmien ja päätelaitteiden kautta leviävien uhkien torjumiseksi
COBIT 2019	DSS05.01, DSS01.04, MEA	Edellyttää päätelaitekontrollien suojaamista, valvontaa ja arviointia

1. Tarkoitus

1.1 Tässä politiikassa määritellään pakolliset kontrollit ja operatiiviset vaatimukset organisaation päätelaitteiden, mukaan lukien työasemat, kannettavat tietokoneet, mobiililaitteet ja palvelimet, suojaamiseksi haittaohjelmilta ja niihin liittyviltä uhilta.

1.2 Tässä politiikassa määritellään päätelaitesuojauksen, haittaohjelmien havaitsemisen, rajaamistoimenpiteiden ja käyttäytymiseen perustuvan valvonnan vähimmäisvaatimukset, jotta järjestelmien häiriönsietokyky säilyy sekä tavanomaisia että kehittyneitä haittaohjelmia vastaan.

1.3 Tämä politiikka tukee suoraan ISO/IEC 27001:2022 -standardin kohdan 8.1 ja liitteen A kontrollin 8.7 vaatimusten noudattamista, ja se on yhdenmukainen GDPR:n, NIS2:n ja DORA:n mukaisten alueellisten kyberturvallisuusvelvoitteiden kanssa.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia päätelaitteita, mukaan lukien:

2.1.1 Organisaation omistamat tai hallinnoimat työasemat, kannettavat tietokoneet, mobiililaitteet ja virtuaali-instanssit

2.1.2 Henkilökohtaiset laitteet, jotka on hyväksytty käyttöön BYOD-politiikan mukaisesti, edellyttäen MDM-ratkaisun tai päätelaiteagentin asentamista

2.1.3 Palvelimet ja infrastruktuuriomaisuuserät, mukaan lukien pilvessä toimivat virtuaalikoneet ja reunalaitteet

2.1.4 Käyttöjärjestelmät, ajurit, paikalliset palvelut, päätelaiteagentit ja kuhunkin solmuun asennetut tietoturvakontrollit

2.2 Tämä politiikka koskee kaikkia henkilöitä, joilla on hallinnollinen, tekninen tai operatiivinen vastuu jostakin päätelaitteesta, mukaan lukien:

2.2.1 Sisäiset työntekijät ja sopimuskumppanit

2.2.2 Hallinnoidut palveluntarjoajat (MSP), ulkoistetun työasematuen henkilöstö ja kolmansien osapuolten IT-järjestelmänvalvojat

2.2.3 Käyttäjät, joilla on valtuutus käyttää kannettavia järjestelmiä, VPN-yhteydellä varustettuja kannettavia tietokoneita tai mobiilikäyttöä organisaation verkkoihin

2.3 Tämän politiikan kattamiin uhkiin kuuluvat muun muassa:

2.3.1 Virukset, madot, troijalaiset, kiristyshaittaohjelmat, vakoiluohjelmat, rootkitit, mainosohjelmat, näppäilyntallentimet ja bottiverkot

2.3.2 Tiedostottomat haittaohjelmat, nollapäivähyötykuormat, käyttöoikeuksien korotukseen tarkoitetut haittaohjelmat ja selainpohjaiset hyväksikäyttöpaketit

2.3.3 Haitallinen koodi, joka toimitetaan siirrettävien tallennusvälineiden, tietojenkalasteluvektorien, drive-by-latausten tai USB-pohjaisten hyökkäysten kautta

3. Tavoitteet

3.1 Suojata päätelaitejärjestelmien ja niiden käsittelemien tietojen eheys, saatavuus ja luottamuksellisuus tehokkaalla haittaohjelmien estämisellä, havaitsemisella ja reagoinnilla.

3.2 Estää haitallisen koodin suorittaminen ja leviäminen organisaation verkoissa ottamalla käyttöön teknisiä suojatoimia, perustason koventamisen ja reaaliaikaisen telemetrian.

3.3 Integroida päätelaitesuojaus muihin ISMS-kontrolleihin, mukaan lukien haavoittuvuuksien hallinta, pääsynhallinta, lokitus ja valvonta sekä tietoturvapoikkeamien hallinta.

3.4 Varmistaa päätelaitteiden jatkuva näkyvyys keskitetysti hallinnoiduilla suojausalustoilla, mukaan lukien virustorjunta-/haittaohjelmantorjunta-agentit, päätelaitteiden havainnointi ja reagointi (EDR) sekä SIEM-telemetria.

3.5 Täyttää päätelaiteturvallisuutta koskevat oikeudelliset, sääntelyyn liittyvät ja standardiperusteiset vaatimukset (esim. EU:n GDPR artikla 32, EU:n NIS2-direktiivi artikla 21, EU:n DORA-asetus artikla 9).

3.6 Määrittää vastuutetut roolit, velvoittavat palvelutasot paikkaukselle ja hälytyksiin reagoinnille sekä varmistaa auditointivalmius dokumentoinnin ja raportoinnin avulla.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa sen yhdenmukaisuuden ISMS:n ja yleisen tietoturvastrategian kanssa.

4.1.2 Katselmoi päätelaitesuojauksen mittarit, poikkeamatrendit ja työkalujen tehokkuuden neljännesvuosittain.

4.1.3 Hyväksyy päätelaitesuojauksen kattavuuteen liittyvät poikkeukset ja jäännösriskin hyväksynnät.

4.2 Päätelaiteturvallisuuden vastuuhenkilö / tietoturvavalvomon (SOC) päällikkö

4.2.1 Hallinnoi päätelaitesuojausjärjestelmiä (esim. AV, EDR, MDM).

4.2.2 Vastaa politiikan toimeenpanosta, uhkien havaitsemisen virityksestä ja reagoinnin pelikirjoista.

4.2.3 Ylläpitää kattavuustilastoja, haittaohjelmapoikkeamien lokeja ja hälytysmääritysten peruskonfiguraatioita.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vuosittain tai kun:

9.1.1 Esiintyy merkittäviä haittaohjelmakampanjoita tai päätelaitteisiin liittyviä tietoturvapoikkeamia

9.1.2 Uudet uhkatyypit (esim. tiedostottomat haittaohjelmat, kiristyshaittaohjelmien variantit) edellyttävät päivitettyjä havaitsemis- tai reagointistrategioita

9.1.3 Päätelaitesuojausalustat tai agenttiarkkitehtuurit muuttuvat merkittävästi

9.1.4 Päätelaitekontrolleihin vaikuttavat oikeudelliset tai sääntelyvaatimukset päivittyvät

9.2 Katselmoinnin käynnistää päätelaiteturvallisuuden vastuuhenkilö, ja se koordinoidaan tietoturvajohtajan sekä laki-, riski- ja auditointitoimintojen kanssa.

9.3 Hyväksytyt muutokset on dokumentoitava ISMS:n asiakirjarekisteriin, niille on annettava uusi versiotunniste, ja niistä on tiedotettava kaikille vaikutuksen alaisille osapuolille.

9.4 Korvatut versiot on arkistoitava, niiden käyttöoikeudet on rajoitettava, ja ne on säilytettävä ISMS:n säilytysaikataulujen mukaisesti audit trailin eheyden varmistamiseksi.

10. Liittyvät politiikat ja yhteydet

10.1 P1 - Tietoturvapolitiikka. Määrittää perustavanlaatuiset periaatteet järjestelmien, tietojen ja verkkojen suojaamiselle. Tämä politiikka toteuttaa kyseiset periaatteet päätelaitetasolla teknisillä ja menettelyllisillä haittaohjelmakontrolleilla.

10.2 P4 - Pääsynhallintapolitiikka. Määrittää käyttäjien käyttörajoitukset, joita toteutetaan päätelaitetasolla, mukaan lukien suojaukset käyttöoikeuksien korotusta ja arvioimattomien ohjelmistojen luvatonta asennusta vastaan.

10.3 P5 - Muutoksenhallintapolitiikka. Varmistaa, että päätelaitesuojausohjelmiston, politiikkasääntöjen tai agenttimääritysten päivityksiin sovelletaan hyväksyntää ja hallittuja käyttöönottomenettelyjä.

10.4 P12 - Omaisuudenhallintapolitiikka. Tarjoaa omaisuuserien luokittelun ja luetteloinnin perustason, jota tarvitaan päätelaitenäkyvyyteen, paikkauksen kattavuuteen ja haittaohjelmasuojauksen soveltamisalan määrittelyyn.

10.5 P22 - Lokitus- ja valvontapolitiikka. Mahdollistaa päätelaitteiden hälytysten, agenttien toimintakunnon ja uhkatiedustelun integroinnin keskitettyihin SIEM-järjestelmiin reaaliaikaista havaitsemista ja forensista jäljitettävyyttä varten.

10.6 P30 - Tietoturvapoikkeamien hallintapolitiikka. Yhdistää päätelaitteisiin liittyvät haittaohjelmapoikkeamat standardoituihin rajaamis-, poistamis-, tutkinta- ja palautumistyönkulkuihin, joille on määritetty roolit ja eskalointikynnykset.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:

11.1.1 Kohta 8.1 - Operatiivinen suunnittelu ja ohjaus: edellyttää teknisten kontrollien, mukaan lukien päätelaitteiden suojatoimien, toteuttamista ISMS:n tavoitteiden ylläpitämiseksi.

11.2 ISO/IEC 27002:2022 - Kontrollit 8.7, 8:

11.2.1 Tarjoaa yksityiskohtaista teknistä ohjeistusta haittaohjelmien torjuntatoimenpiteistä, turvallisesta ohjelmistojen käyttöönotosta, valvonnasta ja poikkeamavalmiudesta päätelaiteympäristöissä.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Haitallisen koodin suojaus: edellyttää haittaohjelmien torjuntatyökalujen käyttöä reaaliaikaisella, käytönaikaisella skannauksella ja käyttäytymisanalyysillä.

11.3.2 SI-4 - Järjestelmävalvonta: tukee telemetrian integrointia keskitettyihin havaitsemisalustoihin.

11.3.3 CM-6 - Konfiguraatioasetukset: vahvistaa päätelaitteiden perustason kontrolliasetuksia, mukaan lukien suojausagenttien pakollisen käyttöönoton.

11.4 EU:n GDPR (2016/679):

11.4.1 Artikla 32 - Käsittelyn turvallisuus: edellyttää organisaatioilta asianmukaisten teknisten toimenpiteiden toteuttamista henkilötietojen suojaamiseksi, mukaan lukien suojaus haittaohjelmauhilta.

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

11.5.1 Artikla 21(2)(d): velvoittaa yhteisöjä ottamaan käyttöön uhkien havaitsemis- ja estotoimenpiteitä, mukaan lukien päätelaitetason haittaohjelmien torjuntamekanismit.

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

11.6.1 Artikla 9 - ICT-riskien hallinnan vaatimukset: edellyttää, että finanssialan toimijat ottavat käyttöön suojatoimet haittaohjelmien ja päätelaitteiden kautta leviävien uhkien estämiseksi, havaitsemiseksi ja niihin reagoimiseksi.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Suojaudu haittaohjelmia vastaan: edellyttää haittaohjelmien havaitsemista ja lieventämistä kaikissa organisaation päätelaitteissa.

11.7.2 DSS01.04 - Hallitse saatavuutta ja kapasiteettia: varmistaa, että haittaohjelmasuojaus on tasapainossa järjestelmän suorituskyvyn ja liiketoiminnan jatkuvuuden kanssa.

11.7.3 MEA03 - Seuraa, arvioi ja arvioi vaatimustenmukaisuutta: edellyttää päätelaitekontrollien ja suojaustoimien tehokkuuden säännöllistä auditointia.