					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P20					Titlu tad-dokument: **Politika dwar il-Protezzjoni tal-Endpoint u kontra l-Malware**						
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025			Sid tad-dokument:						
X	Politika		Standard		Proċedura		Formola		Reġistru		Oħra

Storja tar-reviżjonijiet				
Numru tar-reviżjoni	**Data tar-reviżjoni**	**Bidliet**	**Ivrevedut minn**	**Sid tal-proċess**

Approvazzjonijiet			
Isem	**Pożizzjoni**	**Data**	**Firma**

Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)

(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettwali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.

L-użu mhux awtorizzat huwa strettament ipprojbit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: info@clarysec.com

Allinjata ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Il-kontrolli għall-protezzjoni tal-endpoint u kontra l-malware huma meħtieġa biex jintlaħqu l-objettivi tal-ISMS
ISO/IEC 27002:2022	Kontrolli 8.7, 8	Tipprovdi kontrolli tekniċi u gwida għal difiża kontra l-malware, protezzjoni tal-endpoint u ġestjoni tal-inċidenti
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Jiddefinixxi r-rekwiżiti għall-protezzjoni kontra kodiċi malizzjuż, monitoraġġ ċentralizzat u konfigurazzjoni bażi
GDPR tal-UE	Artikolu 32	Jeħtieġ miżuri tekniċi xierqa biex tiġi ssalvagwardjata d-data personali, inkluża l-protezzjoni kontra l-malware
Direttiva NIS2 tal-UE	Artikolu 21(2)(d)	Teħtieġ l-implimentazzjoni ta’ sejbien tat-theddid fil-livell tal-endpoint u miżuri preventivi
DORA tal-UE	Artikolu 9	Teħtieġ ġestjoni tar-riskju tal-ICT għad-difiża kontra l-malware u t-theddid li joriġina mill-endpoints
COBIT 2019	DSS05.01, DSS01.04, MEA	Teħtieġ protezzjoni, monitoraġġ u evalwazzjoni tal-kontrolli tal-endpoint

1. Għan

1.1 Din il-politika tiddefinixxi l-kontrolli obbligatorji u r-rekwiżiti operattivi għall-protezzjoni tal-endpoints tal-organizzazzjoni — inklużi desktops, laptops, apparati mobbli u servers — kontra l-malware u theddid relatat.

1.2 Din tistabbilixxi standards minimi għall-protezzjoni tal-endpoint, sejbien tal-malware, trażżin, rispons u monitoraġġ tal-imġiba, sabiex is-sistemi jibqgħu reżiljenti kemm kontra malware komuni kif ukoll kontra varjanti avvanzati.

1.3 Din il-politika tappoġġa direttament il-konformità ma’ ISO/IEC 27001:2022 Klawżola 8.1 u l-Kontroll 8.7 tal-Anness A, u hija allinjata mal-obbligi reġjonali taċ-ċibersigurtà skont il-GDPR, in-NIS2 u d-DORA.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-endpoints kollha, inklużi:

2.1.1 desktops, laptops, apparati mobbli u istanzi virtwali proprjetà tal-organizzazzjoni jew ġestiti mill-organizzazzjoni

2.1.2 apparati personali awtorizzati taħt il-Politika tal-BYOD (soġġetti għall-installazzjoni tal-MDM jew ta’ aġent tal-endpoint)

2.1.3 servers u assi tal-infrastruttura, inklużi VMs ospitati fil-cloud u apparati tat-tarf

2.1.4 sistemi operattivi, drivers, servizzi lokali, aġenti tal-endpoint u kontrolli tas-sigurtà installati fuq kull node

2.2 Il-persunal kollu li għandu responsabbiltà amministrattiva, teknika jew operattiva għal kwalunkwe endpoint huwa kopert minn din il-politika, inklużi:

2.2.1 impjegati interni u kuntratturi

2.2.2 fornituri ta' servizzi ġestiti (MSPs), appoġġ esternalizzat għad-desktop u amministraturi tal-IT ta' partijiet terzi

2.2.3 utenti awtorizzati biex joperaw sistemi portabbli, laptops abilitati għall-VPN jew aċċess mobbli għan-netwerks tal-organizzazzjoni

2.3 Il-kopertura tat-theddid taħt din il-politika tinkludi, iżda mhix limitata għal:

2.3.1 viruses, worms, trojans, ransomware, spyware, rootkits, adware, keyloggers, botnets

2.3.2 malware fileless, payloads zero-day, malware ta' eskalazzjoni tal-privileġġi u browser exploit kits

2.3.3 kodiċi malizzjuż imwassal permezz ta' mezzi ta' ħżin rimovibbli, vetturi ta' phishing, downloads drive-by jew attakki bbażati fuq USB

3. Objettivi

3.1 Tiġi protetta l-integrità, id-disponibbiltà u l-kunfidenzjalità tas-sistemi tal-endpoint u d-data li jipproċessaw permezz ta' prevenzjoni, sejbien u rispons affidabbli kontra l-malware.

3.2 Tiġi evitata l-eżekuzzjoni jew il-propagazzjoni ta' kodiċi malizzjuż fuq in-netwerks tal-organizzazzjoni billi jiġu infurzati salvagwardji tekniċi, hardening bażi u telemetrija f'ħin reali.

3.3 Tiġi integrata l-protezzjoni tal-endpoint ma' kontrolli oħra tal-ISMS, inklużi l-ġestjoni tal-vulnerabbiltajiet, il-kontroll tal-aċċess, il-Politika tal-Illoggjar u l-Monitoraġġ u r-rispons għall-inċidenti.

3.4 Tiġi żgurata viżibbiltà kontinwa tal-endpoints permezz ta' pjattaformi ta' protezzjoni ġestiti ċentralment, inklużi aġenti antivirus/anti-malware, skoperta u rispons tal-endpoint (EDR) u telemetrija tas-SIEM.

3.5 Tiġi żgurata l-konformità mar-rekwiżiti legali, regolatorji u bbażati fuq standards li jimponu sigurtà tal-endpoint (eż. Artikolu 32 tal-GDPR, Artikolu 21 tan-NIS2, Artikolu 9 tad-DORA).

3.6 Jiġu ddefiniti rwoli responsabbli, jiġu infurzati SLAs għall-applikazzjoni ta' patches u għar-rispons għat-twissijiet, u tiġi żgurata l-kapaċità li tintwera l-konformità permezz ta' dokumentazzjoni u rappurtar.

4. Rwoli u responsabbiltajiet

4.1 Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO)

4.1.1 Huwa s-sid ta' din il-politika u jiżgura l-allinjament tagħha mal-ISMS u mal-istrateġija ġenerali tas-sigurtà.

4.1.2 Jirrieżamina kull tliet xhur il-metriċi tal-protezzjoni tal-endpoint, ix-xejriet tal-inċidenti u l-effettività tal-għodod.

4.1.3 Japprova eċċezzjonijiet u aċċettazzjonijiet ta' riskju residwu relatati mal-kopertura tal-endpoint.

4.2 Responsabbli għas-Sigurtà tal-Endpoint / Maniġer tas-SOC

4.2.1 Jiġġestixxi s-sistemi ta' protezzjoni tal-endpoint (eż. AV, EDR, MDM).

4.2.2 Jissorvelja l-applikazzjoni tal-politika, l-irfinar tas-sejbien tat-theddid u l-playbooks tar-rispons.

4.2.3 Iżomm statistika tal-kopertura, logs tal-inċidenti tal-malware u konfigurazzjonijiet bażi tat-twissijiet.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti għar-rieżami u l-aġġornament

9.1 Din il-politika għandha tiġi rieżaminata kull sena jew meta:

9.1.1 iseħħu kampanji kbar ta' malware jew inċidenti tas-sigurtà tal-endpoint

9.1.2 tipi ġodda ta' theddid (eż. malware fileless, varjanti ta' ransomware) jeħtieġu strateġiji aġġornati ta' sejbien jew rispons

9.1.3 pjattaformi ta' protezzjoni tal-endpoint jew arkitetturi tal-aġenti jinbidlu b'mod sinifikanti

9.1.4 jiġu aġġornati rekwiżiti legali jew regolatorji li jaffettwaw il-kontrolli tal-endpoint

9.2 Ir-rieżami għandu jinbeda mir-Responsabbli għas-Sigurtà tal-Endpoint u jiġi kkoordinat mas-CISO, il-funzjonijiet Legali, tar-Riskju u tal-Awditjar.

9.3 Ir-reviżjonijiet approvati għandhom jiġu dokumentati fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS, jingħataw identifikatur ġdid tal-verżjoni, u jiġu kkomunikati lill-partijiet affettwati kollha.

9.4 Verżjonijiet sostitwiti għandhom jiġu arkivjati, b'aċċess ristrett, u miżmuma għall-integrità tat-traċċa tal-awditjar skont l-iskedi taż-żamma tal-ISMS.

10. Politiki relatati u rabtiet

10.1 P1 - Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-prinċipji bażiċi għall-protezzjoni tas-sistemi, tad-data u tan-netwerks. Din il-politika tapplika dawk il-prinċipji fil-livell tal-endpoint permezz ta' kontrolli tekniċi u proċedurali kontra l-malware.

10.2 P4 - Politika dwar il-Kontroll tal-Aċċess. Tiddefinixxi restrizzjonijiet fuq l-aċċess tal-utenti li jiġu infurzati fil-livell tal-endpoint, inklużi protezzjonijiet kontra eskalazzjoni tal-privileġġi u installazzjonijiet mhux awtorizzati ta' software mhux ivverifikat.

10.3 P5 - Politika tal-Ġestjoni tat-Tibdil. Tiżgura li aġġornamenti tas-software ta' protezzjoni tal-endpoint, regoli tal-politika jew konfigurazzjonijiet tal-aġenti jkunu soġġetti għal approvazzjoni u proċessi kkontrollati ta' tqegħid fis-servizz.

10.4 P12 - Politika tal-Ġestjoni tal-Assi. Tipprovdi l-linja bażi għall-klassifikazzjoni u l-inventarju tal-assi meħtieġa għall-viżibbiltà tal-endpoint, il-kopertura tal-patching u d-definizzjoni tal-kamp ta' applikazzjoni tal-protezzjoni kontra l-malware.

10.5 P22 - Politika tal-Illoggjar u l-Monitoraġġ. Tippermetti l-integrazzjoni tat-twissijiet tal-endpoint, l-istatus tas-saħħa tal-aġenti u l-intelligence dwar it-theddid f'sistemi SIEM ċentralizzati għal sejbien f'ħin reali u traċċabbiltà forensika.

10.6 P30 - Politika dwar ir-Rispons għall-Inċidenti. Torbot inċidenti ta' malware ibbażati fuq endpoints ma' flussi tax-xogħol standardizzati għal trażżin, eradikazzjoni, investigazzjoni u rkupru, b'rwoli assenjati u limiti ta' eskalazzjoni.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:

11.1.1 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Teħtieġ l-implimentazzjoni ta' kontrolli tekniċi, inklużi salvagwardji tal-endpoint, biex jinżammu l-objettivi tal-ISMS.

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

11.2.1 Tipprovdi gwida teknika dettaljata dwar miżuri kontra l-malware, tqegħid fis-servizz sigur tas-software, monitoraġġ u tħejjija għall-inċidenti f'ambjenti tal-endpoint.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Protezzjoni kontra Kodiċi Malizzjuż: Teħtieġ l-użu ta' għodod kontra l-malware bi skannjar f'ħin reali, mal-aċċess u b'analiżi tal-imġiba.

11.3.2 SI-4 - Monitoraġġ tas-Sistema: Jappoġġa l-integrazzjoni tat-telemetrija ma' pjattaformi ta' sejbien ċentralizzat.

11.3.3 CM-6 - Impostazzjonijiet tal-Konfigurazzjoni: Isaħħaħ l-impostazzjonijiet tal-kontroll tal-linja bażi fuq l-endpoints, inkluża l-applikazzjoni tal-aġenti ta' protezzjoni.

11.4 GDPR tal-UE (2016/679):

11.4.1 Artikolu 32 - Sigurtà tal-Ipproċessar: Jeħtieġ li l-organizzazzjonijiet jimplimentaw miżuri tekniċi xierqa biex jissalvagwardjaw id-data personali, inkluża protezzjoni kontra theddid tal-malware.

11.5 Direttiva NIS2 tal-UE (2022/2555):

11.5.1 Artikolu 21(2)(d): Tobbliga lill-entitajiet jimplimentaw miżuri ta' sejbien u prevenzjoni tat-theddid, inklużi mekkaniżmi ta' difiża kontra l-malware fil-livell tal-endpoint.

11.6 DORA tal-UE (2022/2554):

11.6.1 Artikolu 9 - Rekwiżiti tal-Ġestjoni tar-Riskju tal-ICT: Teħtieġ li entitajiet finanzjarji jadottaw miżuri protettivi biex jipprevjenu, jiskopru u jirrispondu għal malware u theddid li joriġina mill-endpoints.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Protezzjoni kontra l-Malware: Teħtieġ sejbien u mitigazzjoni tal-malware fl-endpoints kollha tal-organizzazzjoni.

11.7.2 DSS01.04 - Ġestjoni tad-Disponibbiltà u l-Kapaċità: Tiżgura li l-protezzjoni kontra l-malware tkun ibbilanċjata mal-prestazzjoni tas-sistema u l-kontinwità tan-negozju.

11.7.3 MEA03 - Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità: Teħtieġ awditu perjodiku tal-kontrolli tal-endpoint u tal-effettività tal-protezzjoni.