					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P20S					Titlu tad-dokument: **Politika dwar il-Protezzjoni tal-Endpoints 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**

Allinjata ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Kontrolli operattivi għall-protezzjoni kontra l-malware
ISO/IEC 27002:2022	Kontroll 8	Miżuri ta’ kontroll għall-protezzjoni tal-endpoints
NIST SP 800-53 Rev.5	SI-3, SI-4	Protezzjoni kontra kodiċi malizzjuż u rispons għall-inċidenti
Direttiva NIS2 tal-UE	Artikoli 21(2)(d), (e)	Ġestjoni tal-malware u tar-riskju għal entitajiet essenzjali u importanti
DORA tal-UE	Artikoli 10(1), 15	Reżiljenza operattiva u verifika ta’ partijiet terzi
COBIT 2019	DSS05.02, DSS05.04	Protezzjoni tal-endpoints u tan-network u monitoraġġ
GDPR tal-UE	Artikoli 32(1)(b), 33	Miżuri tekniċi u organizzattivi u notifika ta’ ksur

1. Għan

1.1 Din il-politika tiddefinixxi r-rekwiżiti minimi tekniċi, proċedurali u ta’ mġiba għall-protezzjoni tal-apparati kollha tal-endpoint — bħal laptops, desktops, apparati mobbli u mezzi portabbli — kontra kodiċi malizzjuż, inklużi viruses, ransomware, spyware, rootkits u theddid ieħor ta’ malware.

1.2 L-għan tagħha huwa li tiżgura li l-endpoints ikunu mgħammra, miżmuma u użati b’mod li jnaqqas ir-riskju ta’ infezzjoni minn malware, il-propagazzjoni tiegħu u l-kompromess tas-sistema.

1.3 L-organizzazzjoni tirrikonoxxi li l-endpoints huma punti komuni ta’ dħul għall-malware u għalhekk għandhom ikunu msaħħa, immonitorjati u protetti permezz ta’ difiża fuq diversi saffi.

1.4 Din il-politika tappoġġa l-objettivi taċ-ċertifikazzjoni tal-organizzazzjoni skont ISO/IEC 27001:2022 u hija allinjata mal-GDPR tal-UE, mad-Direttiva NIS2 tal-UE, mad-DORA tal-UE u ma’ oqfsa rilevanti oħra.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-endpoints kollha tal-organizzazzjoni, inklużi desktops, laptops, tablets, mobile phones u terminals tal-point-of-sale

2.1.2 Apparati personali (BYOD) użati biex jaċċessaw applikazzjonijiet jew data tan-negozju

2.1.3 Mezzi ta’ ħżin li jistgħu jitneħħew, bħal USB drives u hard disks esterni

2.1.4 Kwalunkwe sistemi operattivi, softwer tal-endpoint jew għodod tal-komunikazzjoni li joperaw fuq dawn il-pjattaformi

2.2 Tapplika bl-istess mod għal:

2.2.1 Persunal intern, kuntratturi, interns u fornituri ta’ servizzi ġestiti (MSPs)

2.2.2 Apparati użati fuq il-post, b’mod remot jew permezz ta’ arranġamenti ta’ xogħol ibridu

2.2.3 Endpoints konnessi mal-cloud jew offline li jaħżnu data tan-negozju jew data personali

3. Objettivi

3.1 Jiġi prevenut il-malware u l-propagazzjoni tiegħu fis-sistemi interni, fuq l-apparati tal-utenti u permezz ta' konnessjonijiet esterni

3.2 Jinstab u jiġi trażżan malajr it-theddid relatat mal-malware bl-użu ta' teknoloġiji awtomatizzati tas-sigurtà tal-endpoints u mogħdijiet ta' eskalazzjoni definiti

3.3 Jiġi żgurat li jintużaw biss apparati awtorizzati, siguri u mmonitorjati biex tiġi aċċessata informazzjoni tan-negozju

3.4 Tiġi stabbilita allokazzjoni ċara tar-responsabbiltajiet għall-persunal u regoli ta' mġiba għall-utenti biex jitnaqqas ir-riskju ta' inċidenti relatati mal-malware

3.5 Jinżammu reġistri traċċabbli u awditjabbli dwar sejbiet ta' malware, rispons u konformità ma' din il-politika

3.6 Tiġi protetta d-data personali u d-data tan-negozju minn kompromess ikkawżat minn malware permezz ta' strateġiji ta' difiża fuq diversi saffi

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Huwa s-sid ta' din il-politika u jiżgura li jkunu disponibbli riżorsi suffiċjenti għall-protezzjoni tal-endpoints

4.1.2 Japprova s-softwer tal-antivirus, l-għodod tal-ġestjoni ta' apparati mobbli (MDM) u r-regoli ta' aċċess minn partijiet terzi

4.1.3 Jirrevedi rapporti ta' inċidenti ta' malware, sommarji tal-impatt u notifiki ta' ksur li jinvolvu endpoints

4.2 Fornitur ta' Appoġġ tal-IT / Amministratur Intern tal-IT

4.2.1 Jagħżel u jimplimenta softwer ta' antivirus, anti-malware u skoperta u rispons tal-endpoint (EDR)

4.2.2 Jiżgura li l-aġġornamenti jiġu applikati b'mod konsistenti u li l-logs jinżammu

4.2.3 Jirrispondi għal twissijiet ta' malware, jiżola sistemi infettati u jwettaq ir-rimedjazzjoni

4.2.4 Japplika kontrolli fuq l-użu tal-USB u ta' apparati esterni

[... 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 Rekwiżit għal rieżami annwali

9.1.1 Din il-politika għandha tiġi riveduta formalment mill-inqas darba fis-sena mill-Maniġer Ġenerali, f'koordinazzjoni mal-Fornitur ta' Appoġġ tal-IT u l-Koordinatur tal-Privatezza

9.2 Aġġornamenti bbażati fuq attivaturi

9.2.1 Il-politika għandha tiġi aġġornata wkoll meta:

9.2.1.1 Theddida jew tifqigħa kbira ġdida ta' malware timmira endpoints użati mill-organizzazzjoni

9.2.1.2 L-għodod tal-antivirus jew tal-EDR jinbidlu, jiġu aġġornati jew sostitwiti

9.2.1.3 Inċident ta' malware jikxef dgħufijiet fil-kamp ta' applikazzjoni jew fl-infurzar ta' din il-politika

9.2.1.4 Ir-rekwiżiti legali jew regolatorji (eż. GDPR, DORA, NIS2) jiġu aġġornati

9.3 Kontroll tal-verżjoni u komunikazzjoni

9.3.1 Il-bidliet kollha fil-politika għandhom jiġu dokumentati b'numru tal-verżjoni, data u sommarju tal-bidliet

9.3.2 Il-persunal għandu jiġi nnotifikat bl-aġġornamenti, b'mod partikolari jekk dawn ibiddlu rekwiżiti operattivi jew ta' mġiba

9.3.3 Verżjonijiet preċedenti għandhom jinżammu fl-arkivju tal-politika għal mill-inqas 3 snin biex jappoġġaw l-awditi

10. Politiki relatati u rabtiet

10.1 Din il-politika għandha tiġi implimentata flimkien mal-politiki SME li ġejjin:

10.1.1 P9S – Politika dwar ix-Xogħol Remot: Tiżgura li r-rekwiżiti tal-protezzjoni tal-endpoints jiġu applikati fuq apparati użati barra mis-sit jew f'ambjenti ibridi

10.1.2 P12S – Politika dwar il-Ġestjoni tal-Assi: Tappoġġa t-traċċar u l-kontroll tal-endpoints kollha, filwaqt li tiżgura li jintużaw biss apparati awtorizzati u protetti

10.1.3 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Issaħħaħ il-prevenzjoni tal-malware bħala kontroll ewlieni tal-privatezza biex tipproteġi data personali u sensittiva minn kompromess

10.1.4 P22S – Politika dwar l-Illoggjar u l-Monitoraġġ: Tistabbilixxi r-rekwiżiti għal logging ta' avvenimenti ta' malware u għaż-żamma tal-viżibbiltà tat-twissijiet għal rispons bikri

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi l-passi ta' eskalazzjoni, trażżin u notifika esterna jekk il-malware jwassal għal kompromess tad-data jew tfixkil operattiv

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Teħtieġ l-implimentazzjoni ta' kontrolli operattivi biex jitnaqqsu riskji bħal attakki ta' malware

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.7 – Jagħti dettalji dwar prattiki ta' kontroll tal-malware, inkluži antivirus, skannjar f'ħin reali, aġġornamenti u taħriġ tal-utenti

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Jeħtieġ l-implimentazzjoni ta' mekkaniżmi ta' protezzjoni kontra kodiċi malizzjuż fuq l-endpoints

11.3.2 SI-4 – Jobbliga monitoraġġ, skoperta, analiżi u azzjonijiet ta' rispons għal theddid u twissijiet fil-livell tal-endpoint

11.4 GDPR tal-UE

11.4.1 Artikolu 32(1)(b) – Jeħtieġ kontrolli tekniċi u organizzattivi (bħall-antivirus) biex tiġi protetta d-data personali

11.4.2 Artikolu 33 – Jobbliga n-notifika ta' ksur meta l-malware jikkompromett l-integrità, il-kunfidenzjalità jew id-disponibbiltà tad-data

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(d) – Jeħtieġ miżuri biex jiġi evitat u indirizzat it-theddid ta' malware fi ħdan entitajiet essenzjali u importanti

11.5.2 Artikolu 21(2)(e) – Jobbliga strateġiji ta' ġestjoni tar-riskju taċ-ċibersigurtà fuq diversi saffi, inkluża l-protezzjoni tal-endpoints kontra l-malware

11.6 DORA tal-UE

11.6.1 Artikolu 10(1) – Jeħtieġ li s-sistemi tal-ICT ikunu protetti kontra l-malware u theddid ieħor bħala parti mir-reżiljenza operattiva

11.6.2 Artikolu 15 – Jobbliga lill-organizzazzjonijiet finanzjarji jivverifikaw il-protezzjoni kontra l-malware fost fornituri ta' servizzi ta' partijiet terzi

11.7 COBIT 2019

11.7.1 DSS05.02 – Jenfasizza miżuri protettivi biex jiddefendu l-endpoints u n-networks kontra theddid ta' malware

11.7.2 DSS05.04 – Jappoġġa l-monitoraġġ u t-twissijiet dwar avvenimenti tas-sigurtà relatati mal-malware bħala parti mill-operazzjonijiet kontinwi