					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P19S					Titlu tad-dokument: **Politika dwar il-Ġestjoni tal-Vulnerabbiltajiet u tal-Patches**						
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 mal-istandards u mar-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	
ISO/IEC 27002:2022	Kontrolli 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Direttiva NIS2 tal-UE	Artikoli 21(2)(d), 21(2)(e)	
DORA tal-UE	Artikoli 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
GDPR tal-UE	Artikolu 32(1)(b)	

1. Għan

1.1 Din il-politika tiddefinixxi kif l-organizzazzjoni tidentifika, tevalwa u timmitiga l-vulnerabbiltajiet fis-sistemi, fl-applikazzjonijiet u fl-infrastruttura tagħha.

1.2 L-għan tagħha huwa li tnaqqas ir-riskju taċ-ċibersigurtà billi tirrikjedi l-applikazzjoni f'waqtha tal-patches u prattiki ta' rimedjazzjoni bbażati fuq ir-riskju, xierqa għal intrapriżi żgħar u ta' daqs medju (SMEs).

1.3 Din il-politika tappoġġa l-konformità maċ-ċertifikazzjoni ISO/IEC 27001:2022 u tgħin sabiex jintlaħqu l-obbligi regolatorji taħt il-GDPR, in-NIS2 u d-DORA billi tirrikjedi ġestjoni proattiva tal-vulnerabbiltajiet tekniċi.

1.4 L-organizzazzjoni tirrikonoxxi li sistemi mhux aġġornati bil-patches joħolqu theddida sinifikanti għas-sigurtà tal-informazzjoni u għandhom jiġu indirizzati b'mod sistematiku u mingħajr dewmien.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Is-servers, id-desktops, il-laptops, l-apparati mobbli, il-ħardwer tan-network u l-pjattaformi kollha ospitati fil-cloud użati mill-organizzazzjoni

2.1.2 Is-sistemi operattivi, is-softwer ta' partijiet terzi, il-plugins u l-applikazzjonijiet kollha użati fl-operazzjonijiet tan-negozju

2.1.3 Il-persunal intern tal-IT jew il-forniturі esterni tas-servizzi responsabbli mill-manutenzjoni, mill-aġġornamenti jew mill-monitoraġġ tas-sistemi

2.1.4 Kwalunkwe kodiċi żviluppat apposta jew softwer embedded miżmum mill-organizzazzjoni jew f'isimha

2.2 Il-politika tkopri kemm infrastruttura ġestita direttament mill-organizzazzjoni kif ukoll sistemi amministrati minn forniturі kuntrattati jew forniturі ta' hosting.

3. Objettivi

3.1 Jidentifikaw u jevalwaw vulnerabbiltajiet magħrufa fl-assi kollha tal-IT b'mod f'waqtu u konsistenti

3.2 Japplikaw patches u aġġornamenti tas-softwer skont is-severità u r-riskju għall-operazzjonijiet tal-organizzazzjoni jew għad-data personali

3.3 Jipprevjenu l-isfruttament ta' dgħufijiet tekniċi li jistgħu jwasslu għal tfixkil fis-servizz, ksur ta' data jew nuqqas ta' konformità legali

3.4 Iżommu reġistri preċiżi tal-patches applikati, kwistjonijiet pendenti u eċċezzjonijiet sabiex l-organizzazzjoni tkun lesta għall-awditjar

3.5 Jużaw għodod u proċessi xierqa għad-daqs tal-organizzazzjoni u għall-kumplessità operattiva tagħha mingħajr ma tiġi kompromessa l-effettività

3.6 Jappoġġaw il-konformità legali u regolatorja, inkluż l-Artikolu 32 tal-GDPR u l-Kontroll 8 tal-Anness A tal-ISO

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Iżomm ir-responsabbiltà ġenerali biex jiżgura li l-attivitajiet tal-ġestjoni tal-vulnerabbiltajiet u tal-applikazzjoni tal-patches jiġu implimentati

4.1.2 Japprova eċċezzjonijiet għar-riskju fejn il-patches ma jkunux jistgħu jiġu applikati u jirrieżamina l-istrateġiji ta' mitigazzjoni relatati

4.1.3 Jirrieżamina rapporti dwar l-istatus tal-patches u jiżgura li r-riżorsi jkunu disponibbli sabiex jintlaħqu l-obbligi tal-applikazzjoni tal-patches

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

4.2.1 Jimmonitorja s-sistemi għal vulnerabbiltajiet u patches disponibbli billi juża twissijiet tal-fornituri, avviżi dwar it-theddid u notifiki fil-livell tas-sistema operattiva

4.2.2 Japplika aġġornamenti għas-sistema operattiva, il-firmware u l-applikazzjonijiet fi ħdan l-iskadenzi definiti

4.2.3 Iżomm log formali tal-patches u jiddokumenta aġġornamenti mhux riżolti jew differiti

4.2.4 Jagħmel l-ittestjar u l-iskedar ta' aġġornamenti kritiċi biex jimminimizza t-tfixkil operattiv

[... 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 Rieżami annwali

9.1.1 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena mill-Maniġer Ġenerali, b'kontribut mill-Fornitur tal-IT u mill-Koordinatur tal-Privatezza

9.2 Attivaturi tar-rieżami

9.2.1 Għandhom isiru rieżamijiet interim jekk:

9.2.1.1 Vulnerabbiltà ewlenija jew exploit jaffettwaw is-sistemi fil-kamp ta' applikazzjoni

9.2.1.2 Isiru bidliet sinifikanti fis-sistema jew fis-softwer

9.2.1.3 Awditu jidentifika lakuni fil-proċessi tal-applikazzjoni tal-patches

9.2.1.4 Jiġi rreġistrat inċident jew ksur relatat mal-applikazzjoni tal-patches

9.3 Kontroll tal-verżjoni tal-politika

9.3.1 L-aġġornamenti kollha għandhom jiġu rreġistrati f'log tal-verżjonijiet b'sommarju tal-bidliet

9.3.2 Il-bidliet għandhom jiġu kkomunikati lill-persunal affettwat

9.3.3 Verżjonijiet skaduti għandhom jiġu arkivjati b'aċċess ristrett

10. Politiki relatati u rabtiet

10.1 Din il-politika tappoġġa u tiddependi fuq diversi politiki oħra tal-SME:

10.1.1 P12S – Politika tal-Ġestjoni tal-Assi: Tidentifika s-sjieda u l-klassifikazzjoni tas-sistemi, u tiżgura li l-assi kollha li jeħtieġu patches ikunu identifikati u inklużi fl-inventarju

10.1.2 P14S – Politika taż-Żamma u r-Rimi tad-Data: Tiżgura li sistemi skedati għad-dekummissjonar jiġu aġġornati b'mod sigur jew jitħassru, u b'hekk titnaqqas l-espożizzjoni għall-vulnerabbiltajiet

10.1.3 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tagħti prijorità għar-rimedjazzjoni tal-vulnerabbiltajiet f'sistemi li jipproċessaw data personali sabiex tiġi żgurata l-konformità mal-liġijiet dwar il-privatezza

10.1.4 P22S – Politika tal-Illoggjar u l-Monitoraġġ: Tappoġġa s-sejbien ta' sistemi mhux aġġornati bil-patches jew imġiba suspettuża li tista' tindika li vulnerabbiltà qed tiġi sfruttata

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi proċeduri għar-rispons għal vulnerabbiltajiet li jwasslu għal inċidenti tas-sigurtà, inklużi l-passi ta' eskalazzjoni u r-rappurtar

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1 – Tirrikjedi l-implimentazzjoni ta' kontrolli biex jiġi indirizzat ir-riskju operattiv, inkluża l-ġestjoni tal-vulnerabbiltajiet

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.8 – Jispeċifika proċessi għall-iskannjar u l-korrezzjoni ta' dgħufijiet magħrufa fis-sistemi

11.2.2 Kontroll 8.9 – Jenfasizza konfigurazzjoni sigura, verifika tal-patches u kontroll tal-bidliet biex tiġi evitata espożizzjoni ġdida matul l-aġġornamenti

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Jirrikjedi identifikazzjoni tal-vulnerabbiltajiet u rimedjazzjoni fi ħdan skadenzi definiti

11.3.2 SI-2 – Jobbliga applikazzjoni fil-pront ta' patches u aġġornamenti skont is-severità

11.3.3 CM-2 – Jirregola konfigurazzjonijiet bażi tas-sistemi u d-dokumentazzjoni tal-aġġornamenti biex jiżgura protezzjoni konsistenti

11.4 GDPR tal-UE

11.4.1 Artikolu 32(1)(b) – Jirrikjedi li l-organizzazzjonijiet jimplimentaw miżuri tekniċi xierqa, inkluża l-applikazzjoni tal-patches, biex iżommu s-sigurtà tal-ipproċessar

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(d) – Jirrikjedi l-ġestjoni tal-vulnerabbiltajiet permezz ta' skannjar sistematiku u rimedjazzjoni

11.5.2 Artikolu 21(2)(e) – Jobbliga konfigurazzjoni sigura u ġestjoni tal-patches biex tiġi żgurata r-reżiljenza tal-ICT

11.6 DORA tal-UE

11.6.1 Artikolu 8(1) – Jirrikjedi l-identifikazzjoni u l-mitigazzjoni tar-riskji tal-ICT, inklużi vulnerabbiltajiet tekniċi

11.6.2 Artikolu 10(2) – Jobbliga lill-entitajiet finanzjarji jirrimedjaw dgħufijiet li jaffettwaw is-sistemi u l-operazzjonijiet tal-ICT

11.7 COBIT 2019

11.7.1 DSS05.02 – Jirrikjedi trattament ta' vulnerabbiltajiet tekniċi magħrufa biex jinżammu operazzjonijiet siguri

11.7.2 APO12.01 – Jallinja l-ġestjoni tar-riskju mal-monitoraġġ proattiv u l-korrezzjoni ta' dgħufijiet fis-sistemi