					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P39					Titlu tad-dokument: **Politika dwar l-Iżvelar Koordinat tal-Vulnerabbiltajiet**						
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 r-regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
GDPR tal-UE	Art. 32(1)(d)	
Direttiva NIS2 tal-UE	Art. 21(2)(e)	
DORA tal-UE	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Għan

1.1 Tistabbilixxi proċess formali għar-riċevuta, il-ġestjoni u l-iżvelar ta' informazzjoni dwar vulnerabbiltajiet li jaffettwaw is-sistemi jew is-servizzi tal-organizzazzjoni, kif meħtieġ mill-Artikolu 21(2)(e) tad-Direttiva NIS2 fir-rigward tal-ġestjoni u l-iżvelar tal-vulnerabbiltajiet.

1.2 Tħeġġeġ lir-riċerkaturi esterni tas-sigurtà, lis-sħab u lill-utenti jirrapportaw vulnerabbiltajiet b'mod responsabbli (Coordinated Vulnerability Disclosure - CVD), u tiddefinixxi kif l-organizzazzjoni tikkomunika informazzjoni dwar vulnerabbiltajiet lill-partijiet interessati.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għan-netwerks u għas-sistemi tal-informazzjoni kollha li huma proprjetà tal-organizzazzjoni jew li jitħaddmu minnha, kif ukoll għal kull vulnerabbiltà identifikata f'dawn is-sistemi.

2.2 Tkopri t-timijiet interni (sigurtà, IT, żvilupp) u kull parti esterna li tirrapporta vulnerabbiltajiet (eż. riċerkaturi, klijenti, fornituri). Tiggverna wkoll il-komunikazzjonijiet mal-fornituri tal-prodotti jew mal-fornituri tas-servizzi meta l-komponenti tagħhom ikunu involuti fil-vulnerabbiltà.

3. Objettivi

3.1 Tidentifika u tirrimedja vulnerabbiltajiet tas-sigurtà f'waqthom billi tuża kemm evalwazzjonijiet interni kif ukoll żvelar estern.

3.2 Tipprovdi gwida ċara sabiex ir-rappurtaturi esterni jissottomettu informazzjoni dwar vulnerabbiltajiet b'mod sigur u legali, u sabiex l-organizzazzjoni tirrispondi u twettaq ir-rimedjazzjoni b'mod effettiv.

3.3 Tiżgura allinjament mar-rekwiżiti tan-NIS2 u mal-aħjar prattiki tal-industrija (ISO/IEC 29147 u 30111) għall-iżvelar koordinat tal-vulnerabbiltajiet, sabiex tissaħħaħ is-sigurtà ġenerali tal-ekosistema.

4. Rwoli u responsabbiltajiet

4.1 Tim ta' Rispons għall-Vulnerabbiltajiet (VRT): Tim maħtur apposta, immexxi mis-CISO jew mir-Responsabbli għall-Ġestjoni tal-Vulnerabbiltajiet, li jirċievi u jwettaq triage tar-rapporti tal-vulnerabbiltajiet, jevalwa r-riskju u l-impatt, u jikkoordina r-rimedjazzjoni u l-iżvelar pubbliku.

4.2 Timijiet tal-IT u tal-Iżvilupp: Jaħdmu mal-VRT sabiex jivverifikaw il-vulnerabbiltajiet irrappurtati, jiżviluppaw u jittestjaw patches jew miżuri ta' mitigazzjoni, u jimplimentaw it-tiswijiet. Jipprovdu wkoll dettalji tekniċi għall-avviżi meta jkun meħtieġ.

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

9. Monitoraġġ u awditjar

9.1 Il-VRT għandu jżomm reġistru tal-iżvelar tal-vulnerabbiltajiet li jsegwi kull rapport mir-riċevuta sal-għeluq. Dan ir-reġistru għandu jiġi rieżaminat kull xahar sabiex jiġi żgurat progress f'waqtu fuq l-oġġetti miftuħa. Oġġetti li jaqbżu l-iskadenza għandhom jiġu eskalati.

9.2 L-Awditjar Intern jew valutatur tas-sigurtà indipendenti għandu, kull sena, jirrieżamina l-effettività tal-proċess tal-ġestjoni tal-vulnerabbiltajiet, pereżempju billi jiċċekkja li kampjuni ta' każijiet ta' vulnerabbiltà ġew immaniġġjati skont il-politika (rikonoxxuti, irrimedjati u żvelati fi żmien xieraq). Għandu jivverifika wkoll li l-kanal ta' żvelar pubbliku għal sistemi aċċessibbli pubblikament huwa funzjonali (eż. li emails ta' test jiġu riċevuti u tittieħed azzjoni fuqhom).

9.3 Il-metriċi dwar il-vulnerabbiltajiet (volum skont is-severità, ħinijiet ta' rimedjazzjoni, eċċ.) għandhom jinġabru kull tliet xhur u jiġu ppreżentati lill-Kumitat ta' Governanza taċ-Ċibersigurtà sabiex jappoġġjaw l-aġġornamenti tal-valutazzjonijiet tar-riskju.

10. Rieżami u manutenzjoni

10.1 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena. Barra minn hekk, kull bidla sinifikanti fl-ambjent tal-IT tagħna (eż. it-tnedija ta' servizz ġdid aċċessibbli mill-internet) jew żvilupp regolatorju rilevanti (eż. liġijiet ġodda tal-UE dwar l-iżvelar tal-vulnerabbiltajiet tal-prodotti) għandu jattiva rieżami barra miċ-ċiklu normali.

10.2 L-aġġornamenti għall-politika għandhom jinkorporaw feedback minn rapportaturi esterni u lessons learned minn analiżijiet interni wara l-inċident. Bidliet maġġuri għandhom jiġu approvati mis-CISO, ikkomunikati lill-impjegati kollha u ppubblikati fir-repożitorju online tal-politiki tas-sigurtà tagħna għal finijiet ta' trasparenza.

11. Politiki relatati u rabtiet

11.1 P01 – Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-mandat ta' ġestjoni għall-ġestjoni u l-iżvelar tal-vulnerabbiltajiet.

11.2 P19 – Politika dwar il-Ġestjoni tal-Vulnerabbiltajiet u l-Patches. Tkopri l-pipeline intern ta' rimedjazzjoni marbut mar-riċevuta tas-CVD.

11.3 P24 – Politika dwar l-Iżvilupp Sigur. Tindirizza t-tiswijiet u l-hardening tal-SDLC li jirriżultaw minn kwistjonijiet irrappurtati.

11.4 P25 – Politika dwar ir-Rekwiżiti tas-Sigurtà tal-Applikazzjonijiet. Tiżgura li l-prodotti jkollhom rekwiżiti tas-sigurtà adattati għall-iżvelar.

11.5 P30 – Politika dwar ir-Rispons għall-Inċidenti. Tindirizza sfruttament attiv ta' vulnerabbiltajiet żvelati.

11.6 P31 – Politika dwar il-Ġbir tal-Evidenza u l-Forensika. Tiżgura ż-żamma ta' artifacts minn difetti rrappurtati u/jew sfruttati.

11.7 P26 – Politika tas-Sigurtà ta' Partijiet Terzi u tal-Forniturі. Tikkoordina żvelar li jinvolvi komponenti ta' forniturі.

11.8 P37 – Politika dwar il-Konformità Legali u Regolatorja. Tiggverna n-notifika, il-formulazzjoni tas-safe harbor u l-pubblikazzjoni.

12. Referenzi

12.1 Direttiva NIS2 (UE 2022/2555), Artikolu 21(2), punt (e) (sigurtà fl-iżvilupp u ġestjoni u żvelar tal-vulnerabbiltajiet)

12.2 Regolament ta' Implimentazzjoni tal-Kummissjoni (UE) 2024/2690, Anness Taqsima 6.10 (rekwiżiti tekniċi dwar il-proċessi ta' ġestjoni u żvelar tal-vulnerabbiltajiet)

12.3 Gwida Teknika tal-ENISA dwar Miżuri ta' Ġestjoni tar-Riskju taċ-Ċibersigurtà – Taqsima dwar il-Ġestjoni u l-Iżvelar tal-Vulnerabbiltajiet

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontroll A.5.7 dwar threat intelligence u l-iżvelar tal-vulnerabbiltajiet; kontroll A.8.28 dwar żvilupp sigur)

12.5 ISO/IEC 29147:2018 (Linji gwida għall-iżvelar tal-vulnerabbiltajiet) u ISO/IEC 30111:2019 (Linji gwida għall-proċessi tal-ġestjoni tal-vulnerabbiltajiet)