					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P40					Titlu tad-dokument: **Politika dwar l-Ittestjar tas-Sigurtà u r-Red Teaming**						
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	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
GDPR tal-UE	Art. 32(1)(d)	
Direttiva NIS2 tal-UE	Art. 21(2)(f)	
DORA tal-UE	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Għan

1 Jiġi stabbilit programm strutturat għall-ittestjar regolari tas-sigurtà tan-netwerks, is-sistemi u l-applikazzjonijiet tal-organizzazzjoni, inklużi valutazzjonijiet tal-vulnerabbiltajiet, testijiet ta' penetrazzjoni u eżerċizzji ta' red team, sabiex jiġu ssodisfati r-rekwiżiti tal-Artikolu 21(2)(f) tad-Direttiva NIS2 dwar l-evalwazzjoni tal-effettività tal-kontrolli taċ-ċibersigurtà.

1.1 Jiġi żgurat li d-dgħufijiet fil-miżuri tekniċi u organizzattivi jiġu identifikati u rrimedjati b'mod proattiv permezz ta' ttestjar ikkontrollat, sabiex tittejjeb b'mod kontinwu l-pożizzjoni tas-sigurtà tal-organizzazzjoni.

2. Kamp ta' applikazzjoni

2 Din il-politika tkopri s-sistemi kollha kritiċi tal-informazzjoni, l-applikazzjonijiet u l-infrastruttura ta' appoġġ li huma proprjetà tal-organizzazzjoni jew operati minnha. Tinkludi wkoll l-ittestjar tas-sigurtà fiżika tal-faċilitajiet fejn dan ikun rilevanti għaċ-ċibersigurtà, pereżempju l-inġinerija soċjali jew testijiet ta' penetrazzjoni fiżika, jekk dawn jaqgħu fil-kamp ta' applikazzjoni tar-red team.

2.1 Din il-politika tapplika għat-timijiet interni tal-IT u tas-Sigurtà tal-Informazzjoni, għal kwalunkwe fornitur estern ikkuntrattat għall-ittestjar tas-sigurtà, u għas-sidien rilevanti tas-sistemi u tal-applikazzjonijiet. L-attivitajiet kollha ta' ttestjar għandhom ikunu awtorizzati u għandhom isegwu l-proċeduri stabbiliti hawnhekk sabiex jiġi evitat tfixkil mhux intenzjonat.

3. Objettivi

3 Tiġi vverifikata l-effettività tal-kontrolli taċ-ċibersigurtà implimentati, tekniċi, operattivi u organizzattivi, permezz ta' ttestjar perjodiku u simulazzjonijiet, f'konformità mar-rekwiżit tan-NIS2 għall-kejl tal-effettività.

3.1 Jinkixfu vulnerabbiltajiet jew lakuni li l-proċessi operattivi regolari jistgħu ma jidentifikawx, inklużi vulnerabbiltajiet zero-day jew kwistjonijiet ta' konfigurazzjoni, taħt xenarji realistiċi ta' attakk (red teaming) qabel ma jiġu sfruttati minn atturi ta' theddid.

3.2 Tingħata assigurazzjoni lill-maniġment u rakkomandazzjonijiet azzjonabbli permezz tar-rapportar tas-sejbiet tat-testijiet, sabiex ikunu jistgħu jittieħdu deċiżjonijiet infurmati dwar it-trattament tar-riskju u t-titjib kontinwu tal-programm tas-sigurtà.

4. Rwoli u responsabbiltajiet

4 Koordinatur tal-Ittestjar tas-Sigurtà (STC): maħtur mill-Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO), responsabbli mill-ippjanar u s-sorveljanza tal-attivitajiet kollha tal-ittestjar tas-sigurtà.

Jiżgura li t-testijiet ikunu definiti fil-kamp ta' applikazzjoni tagħhom, awtorizzati, u li r-riżultati jiġu rrappurtati u segwiti.

4.1 Tim Intern tas-Sigurtà (Blue Team): jikkollabora fit-testijiet, pereżempju billi jipprovdi informazzjoni għad-definizzjoni tal-kamp ta' applikazzjoni u jimmonitorja s-sistemi waqt it-testijiet. Fl-eżerċizzji ta' red team, il-Blue Team jirreaġixxi għal attakki simulati u jiġu evalwati l-kapaċitajiet tiegħu ta' sejbien u rispons.

4.2 Red Team / Testers tal-Penetrazzjoni: jista' jkun tim intern ta' sigurtà offensiva jew konsulenti esterni. Dawn iwettqu t-testijiet skont ir-regoli ta' impenn maqbula, jiddokumentaw il-vulnerabbiltajiet kollha skoperti u l-mogħdijiet ta' sfruttament, u jżommu l-kunfidenzjalità.

[... 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 L-STC għandu jżomm kalendarju u log tal-attivitajiet kollha tal-ittestjar tas-sigurtà li jkunu saru. Dan il-log għandu jinkludi d-data, il-kamp ta' applikazzjoni, min wettaq it-test, u sommarju tar-riżultati. Dan għandu jiġi rieżaminat biex tiġi żgurata l-konformità mal-iskeda meħtieġa, pereżempju sabiex l-ebda sistema kritika ma tibqa' mingħajr test lil hinn miċ-ċiklu annwali.

9.1 Il-progress fir-rimedjazzjoni tas-sejbiet tat-testijiet għandu jiġi mmonitorjat u rrappurtat kull xahar. Kwistjonijiet pendenti ta' severità għolja għandhom jiġu rieżaminati fil-laqgħat tal-maniġment sakemm jingħalqu.

9.2 L-Awditjar Intern jew awditur indipendenti għandu jirrieżamina kull sena l-programm tal-ittestjar tas-sigurtà biex jivverifika li t-testijiet huma awtorizzati, imwettqa u rrappurtati kif suppost; li s-sejbiet kritiċi ġew indirizzati; u li l-programm jissodisfa l-aspettattivi regolatorji. Pereżempju, l-awdituri jistgħu jivverifikaw li sar test ta' penetrazzjoni qabel it-tnedija ta' servizz online ġdid, kif meħtieġ. Kwalunkwe devjazzjoni għandha twassal għal Pjanijiet ta' Trattament.

10. Rieżami u manutenzjoni

10 Din il-politika u l-pjan ġenerali tal-ittestjar għandhom jiġu rieżaminati mill-inqas darba fis-sena. Ir-rieżami għandu jqis bidliet fil-pajsaġġ tat-theddid, pereżempju l-emerġenza ta' tekniki ġodda ta' attakk li l-ittestjar attwali tagħna jista' ma jkoprix, u jadatta l-kamp ta' applikazzjoni jew il-frekwenzi kif xieraq.

10.1 Wara kwalunkwe inċident ewlieni taċ-ċibersigurtà jew ksur, din il-politika għandha terġa' tiġi eżaminata biex jiġi ddeterminat jekk ittestjar addizzjonali jew aktar frekwenti setax jipprevjeni jew jiskopri l-kwistjoni. Il-politika għandha mbagħad tiġi aġġornata biex tinkorpora dawn l-aġġustamenti, pereżempju billi jiżdied xenarju ġdid mal-eżerċizzji ta' red team ibbażat fuq mudelli ta' attakk osservati.

10.2 Aġġornamenti għal din il-politika għandhom jiġu approvati mill-Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO) u nnotati mill-Bord tad-Diretturi. Il-persunal rilevanti kollu għandu jiġi informat bil-bidliet, u s-sħab esterni tal-ittestjar għandhom jiġu nnotifikati jekk kwalunkwe bidla taffettwa t-termini tal-impenn tagħhom.

11. Politiki relatati u rabtiet

11.1 P06 – Politika tal-Ġestjoni tar-Riskju. Ir-riżultati tat-testijiet jappoġġjaw il-valutazzjoni u t-trattament tar-riskju.

11.2 P22 – Politika tal-Illoggjar u l-Monitoraġġ. Tivverifika l-kopertura tas-sejbien waqt l-eżerċizzji.

11.3 P24 – Politika dwar l-Iżvilupp Sigur. Tintegra s-sejbiet tat-testijiet fil-kontrolli tal-SDLC.

11.4 P25 – Politika dwar ir-Rekwiżiti tas-Sigurtà tal-Applikazzjonijiet. Tiżgura li r-rekwiżiti jirriflettu t-tagħlim miksub mit-testijiet.

11.5 P30 – Politika dwar ir-Rispons għall-Inċidenti. Ix-xenarji tar-red team jirfinaw il-playbooks u r-rispons.

11.6 P31 – Politika dwar il-Ġbir tal-Evidenza u l-Forensika. Tiġbor artefatti waqt l-ittestjar b'mod sigur.

11.7 P32 – Politika dwar il-Kontinwità tan-Negozju u l-Irkupru minn Diżastru. L-eżerċizzji jivverifikaw ir-reżiljenza taħt attakk.

11.8 P33 – Politika ta' Monitoraġġ tal-Awditjar u l-Konformità. Tipprovdi sorveljanza indipendenti tal-effettività tal-programm tal-ittestjar.

12. Referenzi

12.1 Direttiva NIS2 (UE 2022/2555), Artikolu 21(2), punt (f) (politiki u proċeduri biex tiġi evalwata l-effettività tal-miżuri tal-ġestjoni tar-riskju taċ-ċibersigurtà)

12.2 Regolament ta' Implimentazzjoni tal-Kummissjoni (UE) 2024/2690, Taqsima 7 tal-Anness (rekwiżiti għall-monitoraġġ, l-ittestjar u l-evalwazzjoni tal-effettività tal-miżuri taċ-ċibersigurtà)

12.3 Gwida Teknika tal-ENISA (2025) – Anness dwar l-ittestjar tas-sigurtà u l-awditjar (linji gwida dwar it-twettiq ta' eżerċizzji taċ-ċibersigurtà u testijiet tekniċi)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Prattiki Tajba tal-Industrija: OWASP Testing Guide, NIST SP 800-115 (Gwida Teknika għall-Ittestjar tas-Sigurtà), CBEST/GREEN Team (oqfsa ta' red teaming għas-settur finanzjarju għal referenza)