					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P19					Titlu tad-dokument: **Politika dwar il-Ġestjoni tal-Vulnerabbiltajiet u l-Applikazzjoni 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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	Trattament sistematiku tal-vulnerabbiltajiet tekniċi; effettività kontinwa tal-kontrolli tas-sigurtà.
ISO/IEC 27002:2022	Kontrolli 8.8, 8.9, 5	Gwida għall-implimentazzjoni tal-applikazzjoni tal-patches, skannjar tal-vulnerabbiltajiet, integrità tas-softwer, konfigurazzjoni sigura u inventarji tal-assi.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Skannjar frekwenti, rimedjazzjoni tad-difetti u ġestjoni tal-konfigurazzjoni kif meħtieġ.
GDPR tal-UE	Artikolu 32, Premessa 49	Miżuri tekniċi għall-applikazzjoni fil-pront tal-patches, trattament tal-vulnerabbiltajiet u kontinwità tas-sigurtà.
Direttiva NIS2 tal-UE	Artikolu 21(2)(d)	Sejbien, rispons u mitigazzjoni tal-vulnerabbiltajiet biex tinżamm iġjene ċibernetika għolja.
DORA tal-UE	Artikoli 8, 10(2)(f)	Rimedjazzjoni f’waqtha tal-vulnerabbiltajiet tal-ICT; valutazzjonijiet kontinwi mmexxija mit-theddid.
COBIT 2019	DSS05.02, DSS01.03, MEA	Skannjar, traċċar u mitigazzjoni tad-dgħufijiet tekniċi; monitoraġġ għal sfruttament; awditjar tal-effettività inkluż l-istatus tal-patches.

1. Għan

1.1 Din il-politika tiddefinixxi r-rekwiżiti obbligatorji tal-organizzazzjoni għall-identifikazzjoni, il-klassifikazzjoni, ir-rimedjazzjoni u l-monitoraġġ tal-vulnerabbiltajiet tekniċi u tad-difetti tas-softwer fis-sistemi tal-informazzjoni u fl-assi kollha li jaqgħu fil-kamp ta’ applikazzjoni tas-Sistema ta’ Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS).

1.2 Tiżgura li l-vulnerabbiltajiet magħrufa kollha jiġu evalwati u indirizzati fil-ħin u b’mod ibbażat fuq ir-riskju permezz ta’ applikazzjoni kkoordinata tal-patches, aġġustamenti fil-konfigurazzjoni jew kontrolli kumpensatorji, f’allinjament mal-ħtiġijiet tan-negozju u mal-obbligi ta’ konformità.

1.3 Din il-politika tappoġġa l-konformità mal-Kontroll 8.8 tal-Anness A ta’ ISO/IEC 27001 u mal-gwida ta’ ISO/IEC 27002, u tindirizza r-rekwiżiti regolatorji skont l-Artikolu 8 tad-DORA, l-Artikolu 21 tan-NIS2, l-Artikolu 32 tal-GDPR, u d-dominji DSS u APO ta’ COBIT 2019.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għas-sistemi tal-informazzjoni, l-assi u l-ambjenti kollha li jaħżnu, jipproċessaw jew jittrasmettu data soġġetta għall-governanza tal-ISMS, inklużi:

2.1.1 Sistemi operattivi, applikazzjonijiet, apparat tan-network, firmware, pjattaformi cloud, interfaces tal-ipprogrammar tal-applikazzjonijiet u softwer ta’ partijiet terzi.

2.1.2 Sistemi f'ambjenti ta' żvilupp, staging, produzzjoni, backup u rkupru minn diżastru.

2.1.3 Endpoints, servers, apparat IoT, infrastruttura ta' virtwalizzazzjoni u containers.

2.2 Hija vinkolanti għal:

2.2.1 Persunal intern: amministraturi tal-IT, inġiniera tas-sistemi, żviluppaturi tal-applikazzjonijiet, analisti tas-sigurtà u timijiet tal-infrastruttura.

2.2.2 Partijiet esterni: kuntratturi, fornituri ta' servizzi ġestiti (MSPs), fornituri tas-softwer u integraturi tas-sistemi b'responsabbiltajiet tekniċi fuq assi fil-kamp ta' applikazzjoni.

2.3 Il-politika tkopri ċ-ċiklu tal-ħajja kollu tal-vulnerabbiltajiet u tal-patches, inkluż:

2.3.1 Skannjar u sejbien

2.3.2 Klassifikazzjoni u prijoritizzazzjoni tar-riskju

2.3.3 Akkwist, ittestjar, implimentazzjoni u treġġigħ lura tal-patches

2.3.4 Ġestjoni tal-eċċezzjonijiet u ppjanar ta' kontrolli kumpensatorji

2.3.5 Logging, rappurtar u traċċabbiltà għall-awditjar

3. Objettivi

3.1 Jiġi żgurat li l-vulnerabbiltajiet magħrufa kollha jiġu identifikati, evalwati u rrimedjati b'mod li jimminimizza l-espożizzjoni għar-riskju u jallinja mal-prijoritajiet operattivi.

3.2 Jiġu stabbiliti proċessi konsistenti fuq livell organizzattiv għall-iskannjar tal-vulnerabbiltajiet, il-klassifikazzjoni tas-severità (eż. CVSS), u l-ġestjoni tal-patches, inkluži l-immaniġġjar ta' emerġenza u l-ippjanar tat-treġġigħ lura.

3.3 Tissaħħaħ il-ġestjoni sigura tal-konfigurazzjoni permezz ta' allinjament mal-linji bażi tal-hardening, il-prattiki tal-kontroll tat-tibdil, u intelligence dwar it-theddid f'ħin reali.

3.4 Tiġi żgurata konformità li tista' titkejjel ma' kontrolli regolatorji u bbażati fuq standards relatati mal-integrità tas-sistema, l-iġjene tal-patches u r-rimedjazzjoni fil-ħin tad-difetti.

3.5 Tiġi ddefinita b'mod ċar ir-responsabbiltà u l-accountability bejn ir-rwoli għaċ-ċiklu tal-ħajja kollu tal-ġestjoni tal-vulnerabbiltajiet, filwaqt li jiġi żgurat li l-partijiet interessati kollha jaġixxu fi ħdan l-SLAs definiti u l-metriċi tal-kontroll li jridu jiġu rrappurtati.

3.6 Tissaħħaħ il-kapaċità li tintwera l-konformità u titjieb ir-reżiljenza kontra theddid emerġenti, inkluži vulnerabbiltajiet zero-day, ktajjen ta' sfruttament attivi, u żvelar ta' riskju għoli minn fornituri.

4. Rwoli u responsabbiltajiet

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

4.1.1 Huwa s-sid tal-politika u jiżgura l-integrazzjoni tagħha fl-ISMS.

4.1.2 Jiddefinixxi l-pożizzjoni tar-riskju tal-organizzazzjoni u jiżgura allinjament mal-aspettattivi regolatorji u mal-kontrolli applikabbli.

4.2 Responsabbli għall-Ġestjoni tal-Vulnerabbiltajiet / Maniġer tal-Operazzjonijiet tas-Sigurtà

4.2.1 Jissorvelja l-operazzjonijiet end-to-end tal-ġestjoni tal-vulnerabbiltajiet u tal-patches.

4.2.2 Jikkoordina l-iskedi tal-iskannjar, il-mudelli ta' prijoritizzazzjoni u l-iskadenzi tar-rimedjazzjoni.

4.2.3 Iżomm ir-Reġistru tal-Vulnerabbiltajiet u jikkollabora fuq il-valutazzjoni ta' kontrolli kumpensatorji.

[... 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 mill-inqas kull sena jew meta jseħħ wieħed minn dawn li ġejjin:

9.1.1 Aġġornamenti regolatorji sinifikanti (eż. bidliet fid-DORA, NIS2)

9.1.2 Bidliet fil-qafas ta' prijoritizzazzjoni tal-vulnerabbiltajiet (eż. aġġornamenti tas-CVSS)

9.1.3 Bidliet kbar fl-ambjent tal-IT (eż. migrazzjoni għall-cloud, bidla estensiva fl-EDR)

9.1.4 Ksur ta' profil għoli jew avviżi esterni li jeħtieġu tisħiħ tal-politika

9.2 Ir-rieżamijiet għandhom isiru mis-CISO b'kollaborazzjoni mal-Operazzjonijiet tas-Sigurtà, il-Ġestjoni tar-Riskju u t-Tmexxija tal-Infrastruttura.

9.3 L-aġġornamenti tal-politika għandhom ikunu:

9.3.1 Dokumentati fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS

9.3.2 Rieżaminati u approvati mill-Maniġment Eżekuttiv

9.3.3 Ikkomunikati lill-partijiet interessati affettwati kollha, inklużi proċessuri ta' partijiet terzi

9.4 Verżjonijiet storiċi għandhom jinżammu b'mod sigur għal finijiet ta' awditjar u accountability.

10. Politiki relatati u rabtiet

10.1 P1 - Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-impenn ġenerali biex tipproteġi s-sistemi u d-data, inkluża l-ġestjoni proattiva tal-vulnerabbiltajiet u l-assigurazzjoni tal-integrità tas-softwer.

10.2 P5 - Politika tal-Ġestjoni tat-Tibdil. Tirregola l-implimentazzjoni kollha tal-patches u l-aġġustamenti tal-konfigurazzjoni, u teħtieġ dokumentazzjoni, ittestjar, approvazzjoni u proċeduri ta' treġġigħ lura li jikkumplimentaw il-proċessi ta' rimedjazzjoni tal-vulnerabbiltajiet.

10.3 P6 - Politika tal-Ġestjoni tar-Riskju. Tappoġġa l-klassifikazzjoni u t-trattament ta' vulnerabbiltajiet mhux irrimedjati permezz ta' valutazzjonijiet strutturati tar-riskju, analiżi tal-impatt u proċeduri ta' aċċettazzjoni tar-riskju residwu.

10.4 P12 - Politika tal-Ġestjoni tal-Assi. Tiżgura li s-sistemi jkunu inventarjati u kklassifikati b'mod preċiż, biex tippermetti skannjar konsistenti tal-vulnerabbiltajiet, assenjazzjoni tas-sjieda u kopertura tal-patches tul iċ-ċiklu tal-ħajja.

10.5 P22 - Politika tal-Logging u l-Monitoraġġ. Tiddefinixxi rekwiżiti għas-sejbien tal-avvenimenti u l-ġenerazzjoni ta' traċċa tal-awditjar. Din il-politika tappoġġa l-viżibbiltà tal-attività tal-applikazzjoni tal-patches, bidliet mhux awtorizzati u tentattivi ta' sfruttament immirati lejn vulnerabbiltajiet magħrufa.

10.6 P30 - Politika dwar ir-Rispons għall-Inċidenti. Tispeċifika protokolli ta' eskalazzjoni u strateġiji ta' trażżin għal vulnerabbiltajiet sfruttati, investigazzjonijiet ta' ksur, u azzjonijiet korrettivi allinjati mal-kontrolli ta' din il-politika.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001: Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Teħtieġ trattament sistematiku tal-vulnerabbiltajiet tekniċi biex tiżgura l-effettività kontinwa tal-kontrolli tas-sigurtà.

11.2 ISO/IEC 27002:2022 - Kontrolli 8.8, 8.9, 5: Tipprovdi gwida għall-implimentazzjoni tal-applikazzjoni tal-patches, skannjar tal-vulnerabbiltajiet, integrità tas-softwer u integrazzjoni ma' konfigurazzjoni sigura u inventarji tal-assi.

11.3 NIST SP 800-53 Rev.5: RA-5 - Monitoraġġ u skannjar tal-vulnerabbiltajiet: Jobbliga skannjar frekwenti u traċċar tar-rimedjazzjoni. SI-2 - Rimedjazzjoni tad-difetti: Teħtieġ valutazzjoni fil-pront u mitigazzjoni tad-difetti permezz ta' patches disponibbli jew azzjonijiet oħra. CM-2 / CM-6 - Linji bażi u kontrolli tal-ġestjoni tal-konfigurazzjoni: Jistabbilixxi l-pedament għal konfigurazzjonijiet siguri tas-sistema marbuta mal-applikazzjoni tal-patches.

11.4 GDPR tal-UE (2016/679): Artikolu 32 - Sigurtà tal-Ipproċessar: Jeħtieġ l-implimentazzjoni ta' miżuri tekniċi xierqa, bħall-applikazzjoni fil-pront tal-patches u t-trattament tal-vulnerabbiltajiet, biex jiġu żgurati l-kunfidenzjalità u r-reżiljenza tas-sistema. Premessa 49: Tħeġġeġ lill-entitajiet jimplimentaw kontrolli preventivi kontra theddid magħruf biex jappoġġaw is-sigurtà u l-kontinwità.

11.5 Direttiva NIS2 tal-UE (2022/2555): Artikolu 21(2)(d): Tobbliga lill-entitajiet essenzjali u importanti jiskopru, jirrispondu għal, u jimmitigaw il-vulnerabbiltajiet tas-sistema u jżommu livell għoli ta' iġjene ċibernetika.

11.6 DORA tal-UE (2022/2554): Artikolu 8 - Ġestjoni tar-Riskju tal-ICT: Jeħtieġ identifikazzjoni u rimedjazzjoni f'waqthom tal-vulnerabbiltajiet fit-teknoloġiji tal-informazzjoni u tal-komunikazzjoni użati fis-sistemi finanzjarji. Artikolu 10(2)(f): Jenfasizza valutazzjonijiet kontinwi tal-vulnerabbiltajiet immexxija mit-theddid u l-applikazzjoni tal-patches bħala parti mir-reżiljenza operattiva.

11.7 COBIT 2019: DSS05.02 - Ġestjoni tal-Vulnerabbiltajiet tas-Sigurtà: Jagħti direzzjoni lill-organizzazzjonijiet biex jiskannjaw, jittraċċaw u jimmitigaw dgħufijiet tekniċi magħrufa. DSS01.03 - Monitoraġġ tal-Infrastruttura: Jiżgura li s-sistemi jiġu mmonitorjati għal sinjali ta' sfruttament jew dgħufija. MEA03 - Monitoraġġ, Evalwazzjoni u Valutazzjoni tal-Konformità: Jeħtieġ awditjar regolari tal-effettività tal-kontrolli, inkluż l-istatus tal-patches u l-ġestjoni tal-eċċezzjonijiet.