					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P30					Titlu tad-dokument: **Politika dwar ir-Rispons għall-Inċidenti**							
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 8.1, Klawżola 9	Proċessi strutturati għall-ġestjoni tar-riskju u għar-rispons għall-inċidenti
ISO/IEC 27002:2022	Kontrolli 5.25–5.27	Rwoli, rappurtar, rispons u titjib relatati mal-inċidenti
NIST SP 800-53 Rev.5	IR-1 sa IR-9	Ċiklu tal-ħajja komprensiv għar-rispons għall-inċidenti
GDPR tal-UE	Artikolu 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Skadenzi għan-notifika ta' ksur, rappurtar u komunikazzjoni mas-suġġetti tad-data
Direttiva NIS2 tal-UE	Artikolu 23(1)–(4)	Notifika lill-awtorità nazzjonali u rappurtar strutturat
DORA tal-UE	Artikolu 17(1)–(3)	Rappurtar ta' inċidenti maġġuri relatati mal-ICT għal entitajiet finanzjarji
COBIT 2019	DSS02, DSS04, MEA	Jiddefinixxi, jimmonitorja u jevalwa l-ġestjoni tal-inċidenti, il-kontinwità u l-evalwazzjoni

1. Għan

1.1 Din il-politika tistabbilixxi qafas formali għall-identifikazzjoni, ir-rappurtar, l-analiżi, it-trażżin, ir-rispons, l-irkupru u r-rieżami wara l-inċident ta' inċidenti tas-sigurtà tal-informazzjoni li jaffettwaw lill-organizzazzjoni.

1.2 Tiżgura rispons f'waqtu, ikkoordinat u effettiv sabiex jitnaqqsu t-tfixkil operattiv, it-telf finanzjarju, id-dannu reputazzjonali u n-nuqqas ta' konformità regolatorja.

1.3 Il-politika tiffaċilita wkoll titjib kontinwu fil-pożizzjoni ta' reżiljenza ċibernetika tal-organizzazzjoni permezz ta' tagħlimiet meħuda u l-integrazzjoni tas-sejbiet ta' wara l-inċident fil-governanza, fl-għodod u fil-programmi ta' taħriġ.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Il-persunal kollu, inklużi impjegati, kuntratturi, konsulenti u fornituri terzi ta' servizzi

2.1.2 Is-sistemi kollha tal-informazzjoni, l-applikazzjonijiet, l-infrastruttura, in-netwerks u d-data — kemm fuq il-post, fil-cloud jew f'ambjenti ibridi

2.1.3 It-tipi kollha ta' inċidenti tas-sigurtà, inklużi iżda mhux limitati għal:

2.1.3.1 Aċċess mhux awtorizzat jew elevazzjoni tal-privileġġi

2.1.3.2 Attakki ta' malware u ransomware

2.1.3.3 Attakki ta' ċaħda tas-servizz (DoS/DDoS)

2.1.3.4 Telf, tnixxija jew eżfiltrazzjoni tad-data

2.1.3.5 Użu ħażin intern jew ksur tal-politika

2.1.3.6 Ksur tas-sigurtà fiżika li jaffettwa assi diġitali

2.2 Il-politika tkopri s-sejbien, it-triage, l-investigazzjoni, l-eskalazzjoni, it-trażżin, il-ġestjoni tal-evidenza, in-notifika, l-irkupru u l-analiżi tal-kawża ewlenija.

3. Objettivi

3.1 Jiġi stabbilit kapaċità ta' rispons għall-inċidenti li tkun ripetibbli u skalabbli, u li tippermetti s-sejbien, il-klassifikazzjoni u l-mitigazzjoni rapidi ta' inċidenti tas-sigurtà.

3.2 Jitnaqqas l-impatt fuq in-negozju ta' avvenimenti tas-sigurtà permezz ta' proċeduri strutturati ta' trażżin, eliminazzjoni tat-theddida u rkupru tas-sistemi.

3.3 Jiġi żgurat li r-rappurtar u r-rispons għall-inċidenti jkunu allinjati mar-rekwiżiti legali, regolatorji u kuntrattwali, b'mod partikolari dawk relatati mal-iskadenzi tan-notifika ta' ksur u mal-ġestjoni tal-evidenza.

3.4 Tissaħħaħ it-trasparenza u r-responsabbiltà permezz ta' logging xieraq, dokumentazzjoni u traċċar tal-metriċi għall-inċidenti tas-sigurtà kollha.

3.5 Jiġi promoss titjib kontinwu permezz ta' rieżamijiet wara l-inċident, azzjonijiet korrettivi u taħriġ għall-partijiet interessati.

4. Rwoli u responsabbiltajiet

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

4.1.1 Huwa s-sid tal-qafas tar-rispons għall-inċidenti, jiżgura l-applikazzjoni tal-politika u jissorvelja l-koordinazzjoni tal-inċidenti fil-livell tal-intrapriża.

4.1.2 Jaġixxi bħala l-punt ewlieni ta' kuntatt mar-regolaturi, mat-tmexxija eżekuttiva u mal-konsulenti legali esterni waqt inċidenti maġġuri.

4.2 Koordinatur tar-Rispons għall-Inċidenti

4.2.1 Jikkoordina timijiet ta' rispons interfunzjonali, jimmaniġġja l-flussi tax-xogħol u jsegwi l-istatus tat-trażżin u tal-irkupru.

4.2.2 Jattiva u jmexxi rieżamijiet wara l-inċident (PIRs) u jiżgura li l-azzjonijiet korrettivi jiġu rreġistrati u implimentati.

[... 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 tal-anqas darba fis-sena u riveduta kif meħtieġ biex tinkorpora:

9.1.1 Bidliet fil-pajsaġġ tat-theddid, fit-tipi ta' inċidenti jew fil-vetturi tal-attakk

9.1.2 Tagħlimiet meħuda minn inċidenti maġġuri, near misses jew sejbiet regolatorji

9.1.3 Aġġornamenti għal liġijiet u regolamenti applikabbli (eż. GDPR, DORA, NIS2)

9.1.4 Feedback minn eżerċizzji ta' rispons għall-inċidenti u minn rieżamijiet wara l-inċident

9.2 Il-CISO huwa responsabbli biex jibda u jikkoordina l-proċess tar-rieżami, b'konsultazzjoni ma':

9.2.1.1 Konsulent Legali u d-DPO

9.2.1.2 Is-SOC u l-Operazzjonijiet tal-IT

9.2.1.3 It-timijiet tal-kontinwità tan-negozju u tal-ġestjoni tar-riskju

9.2.1.4 It-Tmexxija Eżekuttiva

9.3 Il-bidliet fil-politika għandhom ikunu:

9.3.1 Dokumentati f'repożitorju taħt kontroll tal-verżjoni

9.3.2 Ikkomunikati lit-timijiet kollha affettwati u aġġornati fit-taħriġ ta' sensibilizzazzjoni

9.3.3 Ivverifikati permezz ta’ eżerċizzji tabletop jew eżerċizzji live ta’ rispons għall-inċidenti fi żmien tliet xhur mill-approvazzjoni

9.4 Aġġornamenti urġenti skattati minn theddid emerġenti, sejbiet tal-awditjar jew obbligi legali ġodda għandhom jiġu implimentati immedjatament u nnotati fl-istorja tar-reviżjonijiet tal-politika.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija appoġġata minn u tiddependi fuq il-politiki organizzattivi li ġejjin:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi r-rekwiżit ġenerali għal operazzjonijiet ibbażati fuq ir-riskju u lesti għar-rispons għall-inċidenti.

10.1.2 P5 – Politika tal-Ġestjoni tat-Tibdil: Tiżgura li l-attivitajiet ta’ trażżin u ta’ rkupru li jinvolvu infrastruttura jew servizzi jsegwu proċeduri formali.

10.1.3 P13 – Politika ta’ Klassifikazzjoni u Tikkettar tad-Data: Tappoġġa l-klassifikazzjoni tas-severità tal-inċidenti abbażi tas-sensittività tad-data.

10.1.4 P15 – Politika dwar il-Backup u r-Restawr: Tippermetti l-irkupru minn ransomware jew attakki distruttivi b’assigurazzjoni tal-integrità.

10.1.5 P18 – Politika tal-Kontrolli Kriptografiċi: Tiddefinixxi miżuri ta’ kriptaġġ li jnaqqsu l-impatt tal-inċidenti u r-riskji ta’ espożizzjoni tad-data.

10.1.6 P22 – Politika tal-Illoggjar u l-Monitoraġġ: Tipprovdi l-viżibbiltà bażika tal-avvenimenti, it-twissijiet u ż-żamma tal-logs meħtieġa għal sejbien effettiv u għall-forensika.

10.1.7 P29 – Politika dwar id-Data tat-Test u l-Ambjent tat-Test: Tiżgura li l-inċidenti li jaffettwaw sistemi mhux ta’ produzzjoni wkoll jiġu ġestiti b’mod strutturat u sigur.

10.1.8 P33 – Politika tal-Monitoraġġ tal-Awditjar u l-Konformità: Tivverifika l-kapaċità ta’ tħejjija għall-inċidenti u l-effettività tar-rispons permezz ta’ awditi strutturati u valutazzjonijiet tal-konformità.

11. Standards u oqfsa ta’ referenza

11.1 ISO/IEC 27001: Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Proċessi strutturati għall-ġestjoni tar-riskji u għall-ippjanar tar-rispons għall-inċidenti.

11.2 ISO/IEC 27002:2022 – Kontrolli 5.25–5.27: Responsabbiltajiet għall-ġestjoni tal-inċidenti, għar-rappurtar, għar-rispons, għall-komunikazzjoni u għat-titjib.

11.3 NIST SP 800-53 Rev.5: IR-1 sa IR-9, AU-6, PL-2: Rekwiżiti komprensivi għaċ-ċiklu tal-ħajja tar-rispons għall-inċidenti, għall-awditjar u għall-ippjanar tas-sigurtà.

11.4 GDPR tal-UE: Artikoli 33 u 34: Obbligi ta’ rappurtar lill-awtoritajiet superviżorji u rekwiżiti ta’ notifika lis-suġġetti tad-data (b’eċċezzjonijiet definiti).

11.5 Direttiva NIS2 tal-UE (2022/2555): Artikolu 23: Rappurtar nazzjonali obbligatorju, b’obbligi ta’ rappurtar intermedju u finali.

11.6 DORA tal-UE (2022/2554): Artikolu 17: Rekwiżiti ta’ rappurtar lill-awtoritajiet dwar inċidenti ICT għall-istituzzjonijiet finanzjarji.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Ġestjoni tal-inċidenti tas-servizz u tal-kontinwità, flimkien mal-monitoraġġ tal-prestazzjoni u tal-konformità.