					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P30S					Titlu tad-dokument: **Politika ta’ 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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 6.1, 6.3, 8	ġestjoni tal-inċidenti, titjib kontinwu, kontroll operattiv
ISO/IEC 27002:2022	Kontrolli 5.24, 5.25	sejbien ta’ inċidenti, tħejjija, tagħlim
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	ġestjoni u monitoraġġ tal-inċidenti, rappurtar
GDPR tal-UE	Artikolu 33	rekwiżiti għan-notifika ta’ ksur
Direttiva NIS2 tal-UE	Artikolu 23	rappurtar obbligatorju ta’ inċidenti ċibernetiċi
DORA tal-UE	Artikolu 17	ġestjoni tal-inċidenti tal-ICT
COBIT 2019	DSS02, DSS04	ġestjoni tas-servizzi u tal-inċidenti, u kontinwità

1. Għan

1.1. Din il-politika tistabbilixxi kif l-organizzazzjoni tiskopri, tirrapporta u tirrispondi għal inċident tas-sigurtà tal-informazzjoni li jaffettwa s-sistemi diġitali, id-data jew is-servizzi tagħha.

1.2. Hija tippermetti lill-organizzazzjoni timminimizza l-ħsara, tipproteġi d-data tal-klijenti u tissodisfa l-obbligi regolatorji, bħar-rekwiżit tal-GDPR għan-notifika ta’ ksur fi żmien 72 siegħa.

1.3. Il-politika tiżgura responsabbiltajiet ċari, passi ta’ komunikazzjoni u segwitu wara l-inċident, anke f’organizzazzjonijiet żgħar mingħajr tim dedikat għas-sigurtà.

2. Kamp ta’ applikazzjoni

2.1. Din il-politika tapplika għal:

2.1.1. L-impjegati, il-kuntratturi u l-forniturі esterni kollha ta’ servizzi tal-IT

2.1.2. Is-sistemi u s-servizzi kollha ġestiti mill-kumpanija, inklużi siti web, pjattaformi cloud, apparati mobbli, laptops u kontijiet tal-posta elettronika

2.1.3. It-tipi kollha ta’ inċidenti, inklużi:

2.1.3.1. Aċċess mhux awtorizzat għad-data jew għas-sistemi

2.1.3.2. Infezzjonijiet b’malware jew ransomware

2.1.3.3. Tentattivi ta’ phishing jew inġinerija soċjali

2.1.3.4. Interruzzjoni fis-sistemi minħabba attakk ċibernetiku jew użu ħażin

2.1.3.5. Żvelar aċċidentali jew tħassir ta’ informazzjoni sensittiva

2.1.3.6. Telf jew serq ta’ apparati tan-negozju jew mezzi ta’ ħżin

3. Objettivi

3.1. Li jistabbilixxu proċess ċar għar-rikonoxximent u l-eskalazzjoni ta’ inċidenti tas-sigurtà.

3.2. Li jiżguraw li l-inċidenti jiġu rrappurtati, illoggjati u indirizzati fi ħdan skadenzi definiti minn qabel.

3.3. Li jippermettu trażżin rapidu tal-ħsara, irkupru tad-data u restawr tas-servizzi.

3.4. Li jiżguraw li l-partijiet affettwati (eż. klijenti, regolaturi) jiġu nnotifikati meta dan ikun meħtieġ mil-liġi.

3.5. Li jipprevjenu rikorrenza permezz ta’ analiżi tal-kawża ewlenija, azzjoni korrettiva u titjib fil-politika.

3.6. Li jippermettu lill-SMEs jissodisfaw ir-rekwiżiti taċ-ċertifikazzjoni ISO 27001 u juru responsabbiltà waqt l-awditi.

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM)

4.1.1. Huwa s-sid ta' din il-politika u jiżgura l-implimentazzjoni tagħha.

4.1.2. Jissorvelja l-attivitajiet ta' rispons għall-inċidenti u japprova n-notifiki lir-regolaturi jew lill-klijenti.

4.1.3. Jirrevedi r-rapporti ta' wara l-inċident u jiżgura li jsiru aġġornamenti fil-politika meta jkun meħtieġ.

4.1.4. Jista' jiddelega d-dmirijiet ta' koordinazzjoni, iżda jżomm ir-responsabbiltà aħħarija.

4.2. Fornitur ta' appoġġ tal-IT / amministratur tas-sistemi (intern jew estern)

4.2.1. Jiskopri u jinvestiga inċidenti potenzjali tas-sigurtà.

4.2.2. Jimplimenta azzjonijiet ta' trażżin u rkupru (eż. jiddiżattiva l-aċċess, jirrestawra backups).

4.2.3. Jinnotifika lill-GM bl-inċidenti kollha kkonfermati jew suspettati fi żmien siegħa minn meta jiġu skoperti.

4.2.4. Iżomm log tal-inċidenti bit-timestamps, valutazzjoni tal-impatt u azzjonijiet ta' rispons.

[... 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 skedat

9.1.1. Din il-politika għandha tiġi rieżaminata mill-inqas darba kull 12-il xahar mill-Maniġer Ġenerali (GM) biex jiġi żgurat:

9.1.1.1. Allinjament mal-kontrolli tal-ISO/IEC 27001:2022

9.1.1.2. Reattività għal theddid, riskji u inċidenti ġodda

9.1.1.3. Konformità kontinwa mal-obbligi legali u kuntrattwali (eż. GDPR, DORA)

9.2. Avvenimenti skattaturi

9.2.1. Il-politika għandha wkoll tiġi rieżaminata u aġġornata wara:

9.2.1.1. Kwalunkwe inċident ta' severità għolja jew notifika regolatorja

9.2.1.2. Introduzzjoni ta' infrastruttura ġdida tal-IT jew bidliet fis-sistemi

9.2.1.3. Emendi fir-rekwiżiti legali relatati ma' ksur tas-sigurtà

9.3. Dokumentazzjoni u distribuzzjoni tar-rieżami

9.3.1. Ir-rieżamijiet u l-bidliet kollha għandhom jiġu dokumentati fil-log tat-tibdil tal-politika.

9.3.2. Verżjonijiet aġġornati għandhom jitqassmu lill-impjegati, lill-forniturі u lill-forniturі tal-IT kollha involuti fis-sigurtà jew fl-operazzjonijiet tas-sistema.

9.3.3. Evidenza tal-għarfien tal-persunal (eż. noti tal-laqgħat jew konfermi bl-imejl) għandha tinżamm biex l-organizzazzjoni tkun lesta għall-awditjar.

10. Politiki relatati u rabtiet

10.1. Din il-politika għandha tiġi applikata f'koordinazzjoni mal-politiki li ġejjin tal-SME:

10.1.1. P1S – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-aspettattivi ġenerali għaż-żamma tal-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) waqt l-operazzjonijiet, inkluża l-ġestjoni tal-inċidenti.

10.1.2. P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tistabbilixxi strutturi ta' awtorità u responsabbiltà għas-sejbien, ir-rappurtar u l-eskalazzjoni tal-inċidenti.

10.1.3. P4S – Politika dwar il-Kontroll tal-Aċċess: Tippermetti revoka immedjata tad-drittijiet ta' aċċess waqt azzjonijiet ta' rispons għall-inċidenti.

10.1.4. P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-impjegati kollha jkunu jistgħu jidentifikaw u jirrappurtaw inċidenti tas-sigurtà b'mod effettiv.

10.1.5. P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiggwida l-proċeduri legali ta' notifika ta' ksur skont il-GDPR u tappoġġa l-konformità regolatorja waqt l-inċidenti.

10.1.6. P22S – Politika tal-Illoggjar u l-Monitoraġġ: Tipprovdi l-għodod u l-viżibbiltà meħtieġa għas-sejbien, l-analiżi u l-awditjar ta' avvenimenti ta' sigurtà.

10.1.7. P31S – Politika dwar il-Ġbir tal-Evidenza u l-Forensika: Tappoġġa l-investigazzjoni u d-difensibbiltà legali ta' azzjonijiet relatati mal-inċidenti billi tiggwida l-immaniġġjar korrett tal-evidenza.

10.2. Dawn il-politiki flimkien jistabbilixxu l-qafas operattiv tal-SME għas-sejbien, ir-rispons u l-irkupru minn inċidenti tas-sigurtà tal-informazzjoni.

11. Standards u oqfsa ta' referenza

11.1. ISO/IEC 27001

11.1.1. Klawżola 6.1 – Teħtieġ ippjanar għat-trattament tar-riskju, inkluża t-tħejjija għall-inċidenti.

11.1.2. Klawżola 6.3 – Tappoġġa t-titjib kontinwu permezz ta' lessons learned minn avvenimenti ta' sigurtà.

11.1.3. Klawżola 8.1 – Tenfasizza l-kontroll operattiv biex jiġu ġestiti l-inċidenti u t-tfixkil.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.24 – Jeħtieġ approċċ strutturat għar-rappurtar, il-valutazzjoni u r-rispons għal inċidenti tas-sigurtà tal-informazzjoni.

11.2.2. Kontroll 5.25 – Jiffoka fuq it-tagħlim mill-inċidenti biex titjieb it-tħejjija futura u r-reżiljenza tas-sistema.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Jiddefinixxi proċeduri għall-ġestjoni tal-inċidenti, inklużi t-trażżin u l-irkupru.

11.3.2. IR-5 – Jistabbilixxi rekwiżiti għall-monitoraġġ u l-analiżi tal-inċidenti.

11.3.3. IR-6 – Jobbliga protokolli ta' rappurtar tal-inċidenti kemm esterni kif ukoll interni.

11.4. GDPR tal-UE

11.4.1. Artikolu 33 – Jeħtieġ rappurtar ta' ksur ta' data personali lir-regolaturi fi żmien 72 siegħa, b'dettalji dwar il-kamp ta' applikazzjoni u l-mitigazzjoni.

11.5. Direttiva NIS2 tal-UE (2022/2555)

11.5.1. Artikolu 23 – Jeħtieġ li entitajiet essenzjali u importanti jinnotifikaw lill-awtoritajiet kompetenti dwar inċidenti sinifikanti bl-użu ta' formati standardizzati ta' rappurtar.

11.6. Regolament DORA tal-UE (2022/2554)

11.6.1. Artikolu 17 – Jeħtieġ li entitajiet finanzjarji jikklassifikaw, jirrappurtaw u jsegwu inċidenti u tfixkil relatati mal-ICT.

11.7. COBIT 2019

11.7.1. DSS02 – Manage Service Requests and Incidents: Jiggwida l-ġestjoni effettiva ta' talbiet għas-servizz u ta' inċidenti operattivi u tas-sigurtà f'konformità mal-objettivi ta' governanza.

11.7.2. DSS04 – Manage Continuity: Jorbot ir-rispons għall-inċidenti ma' strateġiji usa' ta' kontinwità u rkupru.