					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P31S					Titlu tad-dokument: **Politika dwar il-Ġbir tal-Evidenza u l-Forensika**							
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	Klawżoli 6.1, 6.3, 8	Ippjanar ibbażat fuq ir-riskju, azzjonijiet ta' titjib u kontrolli operattivi għall-integrità tal-evidenza
ISO/IEC 27002:2022	Kontrolli 5.24–5.27	Jiggwidaw il-ġestjoni sigura, ir-rieżami wara l-inċident u t-titjib ibbażat fuq l-evidenza
ISO/IEC 27035-3:2016	Klawżoli 6.3, 6.4, 7	Jiżguraw ippjanar xieraq, ġbir legali u ġestjoni sigura tal-evidenza diġitali b'dokumentazzjoni tal-chain of custody
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Tħejjija forensika, protezzjoni tal-logs tal-awditjar u integrazzjoni effettiva mar-rispons għall-inċidenti
GDPR tal-UE	Artikoli 33, 34	Dokumentazzjoni u traċċabbiltà għal ksur ta' data personali
Direttiva NIS2 tal-UE	Artikolu 23	Rapportar traċċabbli tal-inċidenti u ġestjoni sigura tal-evidenza
DORA tal-UE	Artikolu 17(1), 17(2)	Tiżgura l-ġbir, il-ħażna u ż-żamma tal-evidenza għal inċidenti relatati mal-ICT, il-validità forensika u mistoqsijiet regolatorji
COBIT 2019	DSS05.06, DSS05.07	Logging affidabbli u ġestjoni strutturata tal-evidenza għal investigazzjonijiet siguri u awditabbli

1. Għan

1.1. Din il-politika tiddefinixxi kif l-organizzazzjoni tiġġestixxi evidenza diġitali relatata ma' inċidenti tas-sigurtà, ksur ta' data jew investigazzjonijiet interni. Tiżgura li l-evidenza tinġabar, tinħażen u tiġi ppreservata b'mod legalment validu u lest għall-awditjar, b'appoġġ kemm għat-teħid ta' deċiżjonijiet interni kif ukoll għal azzjonijiet esterni potenzjali.

1.2. Il-politika tippermetti lill-organizzazzjonijiet żgħar jipproteġu l-integrità tal-logs, tal-fajls u tal-immaġnijiet tas-sistema filwaqt li juru diliġenza dovuta skont ISO/IEC 27001, il-GDPR u standards relatati.

1.3. Hija tappoġġa t-tħejjija forensika mingħajr ma teħtieġ riżorsi tekniċi avvanzati jew tim tal-IT full-time, billi tistabbilixxi responsabbiltajiet, proċessi u rekwiżiti ta' żamma ċari.

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għal:

2.1.1. l-impjegati kollha, il-fornituri tas-servizzi tal-IT u l-konsulenti esterni involuti fir-rispons għall-inċidenti, fl-investigazzjoni jew fl-analiżi ta' ksur

2.1.2. is-sistemi kollha tal-kumpanija, inklużi laptops, apparati mobbli, servers, kontijiet tal-email, pjattaformi SaaS u ħażna fil-cloud (eż. Microsoft 365, Google Workspace)

2.1.3. kwalunkwe avveniment li jeħtieġ evidenza għal azzjoni dixxiplinari interna, difiża legali, talbiet ta' assigurazzjoni jew involviment ta' regolatur

2.2. Dan jinkludi kemm avvenimenti reali kif ukoll suspettati li jinvolvu:

2.2.1. tnixxija ta' data

2.2.2. theddid minn ġewwa jew użu ħażin

2.2.3. ksur tas-sigurtà (eż. malware, aċċess mhux awtorizzat)

2.2.4. ilmenti tal-klijenti li jeħtieġu verifika diġitali

2.2.5. mistoqsijiet minn regolaturi jew mill-infurzar tal-liġi

3. Objettivi

3.1. Tiżgura li l-evidenza kollha tinġabar u tiġi ġestita b'mod li jżomm l-integrità, l-awtentiċità u l-chain of custody tagħha.

3.2. Tipprevjeni modifika aċċidentali, tħassir jew ġestjoni mhux xierqa ta' logs, fajls jew immaġnijiet tas-sistema li jistgħu jkunu meħtieġa għal investigazzjonijiet.

3.3. Tipprovdi approċċ konsistenti u awditabbli għall-ġestjoni tal-evidenza li jissodisfa l-aspettattivi legali u regolatorji (eż. notifiki ta' ksur skont il-GDPR, traċċabbiltà skont in-NIS2).

3.4. Tiddefinixxi rwoli u responsabbiltajiet ċari biex tiżgura l-qbid rapidu, sigur u konformi mar-rekwiżiti legali tal-evidenza waqt inċidenti tas-sigurtà.

3.5. Tappoġġa t-tħejjija forensika fil-livell tal-SMEs filwaqt li tnaqqas il-kumplessità u tevita tfixkil għall-operazzjonijiet ta' kuljum.

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM)

4.1.1. Japprova l-investigazzjonijiet formali kollha li jeħtieġu ġbir ta' evidenza.

4.1.2. Jirrieżamina u japprova rapporti ta' inċidenti li jinvolvu azzjonijiet legali jew dixxiplinari potenzjali.

4.1.3. Jiddeċiedi jekk għandhomx jiġu nnotifikati konsulent legali estern jew regolaturi.

4.1.4. Jiżgura li l-politika tiġi rieżaminata u aġġornata regolarment.

4.2. Fornitur tas-Servizzi tal-IT / Amministratur tas-Sistema

4.2.1. Jiġbor u jippreserva l-evidenza diġitali skont proċeduri siguri.

4.2.2. Jiddokumenta timestamps, dettalji tas-sistema u passi tal-ġestjoni.

4.2.3. Jiżgura li l-materjal kollu miġbur jinżamm f'post protett.

4.2.4. Jassisti fl-analiżi forensika jekk ikun meħtieġ.