					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P31					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 ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 8	
ISO/IEC 27002:2022	Kontrolli 5.25–5.27, 8	
ISO/IEC 27035:2016	Partijiet 1 u 3	
NIST SP 800-53 Rev.5	IR-1 sa IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Forensika ta’ apparati mobbli u midja diġitali	Forensika ta’ apparati mobbli u midja diġitali
NIST SP 800-86	Integrazzjoni ta’ tekniki forensiċi	Integrazzjoni ta’ tekniki forensiċi fir-rispons għall-inċidenti
GDPR tal-UE	Artikolu 5, 33–34	
Direttiva NIS2 tal-UE	Artikolu 23(1)–(4)	
DORA tal-UE	Artikolu 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Għan

1.1 Din il-politika tistabbilixxi qafas strutturat u legalment difensibbli għall-identifikazzjoni, il-ġbir, il-preservazzjoni, l-analiżi u r-rimi ta’ evidenza diġitali matul inċidenti tas-sigurtà attwali jew suspettati.

1.2 Tiżgura li l-proċessi tat-tħejjija forensika u tal-immaniġġjar tal-evidenza:

1.2.1 Iżommu l-integrità tal-evidenza u l-chain of custody

1.2.2 Jappoġġjaw investigazzjonijiet interni, proċedimenti legali jew rappurtar regolatorju

1.2.3 Ikunu allinjati ma’ standards forensiċi aċċettati internazzjonalment u kriterji ta’ ammissibbiltà legali

1.3 Il-politika tappoġġja l-impenn tal-organizzazzjoni għal rispons proattiv għall-inċidenti, konformità legali u trasparenza fil-governanza, filwaqt li timminimizza t-tfixkil operattiv.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-impjegati kollha, il-kuntratturi, il-forniturі u l-forniturі tas-servizzi involuti fl-amministrazzjoni tas-sistemi, l-immaniġġjar tal-inċidenti jew attivitajiet investigattivi

2.1.2 L-endpoints, is-servers, l-applikazzjonijiet, in-netwerks u l-pjattaformi cloud kollha taħt il-kontroll tal-organizzazzjoni jew ir-responsabbiltà kuntrattwali tagħha

2.1.3 Kull inċident jew avveniment li jeħtieġ immaniġġjar tal-evidenza, inkluż:

2.1.3.1 Theddid intern, ksur ta’ data jew investigazzjonijiet ta’ frodi

2.1.3.2 Użu ħażin tas-sistemi jew tal-kredenzjali

2.1.3.3 Inċidenti relatati ma’ sistemi tat-teknoloġija operattiva (OT) jew ta’ kontroll industrijali

2.1.3.4 Ksur tal-aċċess fiżiku li jinvolvi assi diġitali

2.2 Il-politika tirregola wkoll kull interazzjoni ma’ servizzi forensiċi ta’ partijiet terzi jew ma’ aġenziji tal-infurzar tal-liġi matul eskalazzjoni legali jew proċedimenti regolatorji.

3. Objettivi

3.1 Li tippermetti l-akkwist rapidu, sigur u konformi mal-politika tal-evidenza matul avvenimenti ta' sigurtà jew investigazzjonijiet.

3.2 Li tippreserva l-integrità, l-awtenticità u l-ammissibbiltà tal-evidenza diġitali miġbura permezz ta' kontroll strett tal-aċċess, logs u proċeduri ta' verifika.

3.3 Li tiżgura li l-attivitajiet forensiċi kollha jkunu kkoordinati mal-obbligi legali u regolatorji, inkluża l-protezzjoni tad-data, il-liġi tax-xogħol u r-restrizzjonijiet fuq trasferimenti internazzjonali.

3.4 Li tappoġġja l-analiżi ta' wara l-inċident, id-determinazzjoni tal-kawża ewlenija u t-titjib tal-kontrolli permezz ta' outputs forensiċi ta' kwalità għolja.

3.5 Li tintegra t-tħejjija forensika fis-Sistema ta' Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS) b'appoġġ għall-awditi, notifiki ta' ksur u teħid ta' deċiżjonijiet eżekuttivi.

4. Rwoli u responsabbiltajiet

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

4.1.1 Huwa s-sid ta' din il-politika u jiżgura li l-operazzjonijiet forensiċi kollha jkunu legalment difensibbli, adattati għall-awditjar u bbażati fuq ir-riskju.

4.1.2 Jawtorizza l-eskalazzjoni lejn entitajiet legali esterni u fornituri ta' servizzi forensiċi.

4.2 Analisti Forensiċi / Persunal tal-Immaniġġjar tal-Inċidenti

4.2.1 Imexxu l-akkwist, il-preservazzjoni u l-analiżi teknika tal-evidenza.

4.2.2 Jiżguraw li l-chain of custody tiġi rreġistrata u miżmuma kif xieraq.

4.2.3 Jiddokumentaw l-azzjonijiet, is-sejbiet u l-konfigurazzjonijiet tal-għodod kollha użati matul l-investigazzjonijiet.

[... 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 darba fis-sena u aġġornata kif meħtieġ biex tirrifletti:

9.1.1 Bidliet fil-liġijiet, regolamenti jew ġurisprudenza li jaffettwaw il-proċeduri forensiċi jew l-immaniġġjar tad-data

9.1.2 Aġġornamenti għal standards jew settijiet ta' għodod forensiċi rikonoxxuti fl-industrija

9.1.3 Lessons learned minn rieżami ta' wara l-inċident, tilwim legali jew sejbiet tal-awditjar

9.1.4 Bidliet teknoloġiċi fil-pjattaformi, apparati jew sistemi taħt investigazzjoni

9.2 Il-proċess tar-rieżami huwa taħt is-sjieda tas-CISO u għandu jinkludi konsultazzjoni ma':

9.2.1 Legali u Konformità

9.2.2 Data Protection Officer (DPO)

9.2.3 Timijiet tal-Operazzjonijiet tas-Sigurtà u tal-Forensika

9.2.4 Awditjar Intern

9.3 Ir-reviżjonijiet kollha għandhom ikunu:

9.3.1 Taħt kontroll tal-verżjoni u maħżuna fir-repożitorju tal-politiki

9.3.2 Ikkomunikati lill-partijiet interessati affettwati, inklużi t-timijiet forensiċi u dawk tar-rispons

9.3.3 Akkumpanjati b'aġġornamenti għall-proċeduri operattivi rilevanti u l-materjal tat-taħriġ

9.4 Rieżamijiet interim għandhom jiġu attivati wara kull inċident kritiku li jinvolvi immaniġġjar ħażin tal-evidenza, falliment tal-chain of custody jew kwistjonijiet ta' ammissibbiltà legali.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija allinjata ma' u appoġġjata mill-politiki organizzattivi li ġejjin:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-mandat bażiku għall-investigazzjoni, il-kontroll tal-evidenza u l-konformità mal-liġijiet applikabbli.

10.1.2 P5 – Politika tal-Ġestjoni tat-Tibdil: Tiżgura li s-sistemi taħt investigazzjoni ma jiġux mibdula matul proċessi forensiċi attivi.

10.1.3 P14 – Politika ta' Żamma u Rimi tad-Data: Tirregola r-rimi sigur u l-perjodi ta' żamma għall-evidenza u d-data relatata mal-każijiet.

10.1.4 P18 – Politika tal-Kontrolli Kriptografiċi: Tipprovdi rekwiżiti ta' iċċifrar għall-ħażna u t-trasferiment ta' data sensittiva jew ta' evidenza.

10.1.5 P22 – Politika tal-Logging u l-Monitoraġġ: Tiżgura d-disponibbiltà ta' logs tal-avvenimenti u telemetrija għall-ġbir tal-evidenza u l-korrelazzjoni forensika.

10.1.6 P30 – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi t-triage tal-inċidenti u l-mogħdijiet ta' eskalazzjoni fejn jiġu attivati l-proċeduri forensiċi.

10.1.7 P33 – Politika dwar il-Monitoraġġ tal-Awditjar u l-Konformità: Tivverifika l-osservanza tal-protokolli forensiċi u r-rekwiżiti tal-chain of custody permezz ta' awditi regolari.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' standards internazzjonali dwar il-forensika u l-immaniġġjar tal-inċidenti biex tiżgura l-integrità tal-evidenza, difensibbiltà legali u konformità bejn ġurisdizzjonijiet differenti.

11.2 ISO/IEC 27001

11.2.1 Klawżola 8.1 – Tappoġġja l-kontroll operattiv tat-tħejjija forensika u l-proċeduri tal-evidenza

11.3 ISO/IEC 27002

11.3.1 Kontroll tal-Anness A 5.25 – Responsabbiltajiet għall-Ġestjoni tal-Inċidenti: Jeħtieġ rwoli definiti għall-immaniġġjar ta' inċidenti tas-sigurtà tal-informazzjoni u investigazzjonijiet.

11.3.2 Kontroll tal-Anness A 5.26 – Rappurtar ta' Avvenimenti tas-Sigurtà tal-Informazzjoni: Jappoġġja l-ġbir ta' artifacts relatati mal-avvenimenti bħala evidenza.

11.3.3 Kontroll tal-Anness A 5.27 – Rispons għal Inċidenti tas-Sigurtà tal-Informazzjoni: Jeħtieġ rimedjazzjoni u investigazzjoni strutturati u mmexxija mill-evidenza.

11.3.4 Kontroll tal-Anness A 8.27 – Żvilupp Sigur u Forensika (fejn applikabbli): Jindirizza l-protezzjoni tas-sistemi u tal-għodod matul l-investigazzjonijiet.

11.4 ISO/IEC 27035:2016 (Partijiet 1 u 3)

11.4.1 Jiddeskrivi l-prinċipji tas-sejbien tal-inċidenti, ir-rispons u t-tħejjija forensika, inklużi l-ippjanar, il-chain of custody u l-ġestjoni tal-evidenza tal-inċidenti.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1 sa IR-9, AU-6, PL-2: Jiddefinixxi rekwiżiti strutturati għall-ippjanar, is-sejbien, l-analiżi, it-trażżin u r-rispons għal inċidenti ta' sigurtà. Jappoġġja l-ġbir u l-kapaċità li l-evidenza tintwera għall-awditjar (AU-6) u jiżgura allinjament mal-pjanijiet tas-sigurtà u tal-privatezza tas-sistemi (PL-2) matul investigazzjonijiet forensiċi.

11.6 NIST SP 800-86

11.6.1 Jipprovdi gwida dwar l-integrazzjoni tal-proċessi forensiċi fiċ-ċiklu usa' tal-ħajja tar-rispons għall-inċidenti u dwar kif tiġi żgurata t-tħejjija forensika.

11.7 NIST SP 800-101 Rev.1

11.7.1 Jiffoka fuq l-aħjar prattiki għall-akkwist, il-preservazzjoni u l-analiżi ta' evidenza minn midja diġitali u apparati mobbli b'mod legalment difensibbli.

11.8 GDPR tal-UE (2016/679)

11.8.1 Artikolu 5 – Prinċipji relatati mal-ipproċessar ta’ data personali: Japplika għall-evidenza li tinkludi data personali jew sensittiva, u jiżgura l-minimizzazzjoni u l-limitazzjoni tal-għan.

11.8.2 Artikoli 33–34 – Notifika ta’ ksur ta’ data: Id-data forensika tappoġġja l-konformità mal-obbligi ta’ notifika ta’ ksur u l-proċessi ta’ żvelar legali.

11.9 Direttiva NIS2 tal-UE (2022/2555)

11.9.1 Artikolu 23 – Obbligi ta’ Rappurtar: Id-dokumentazzjoni u s-sejbiet forensiċi jappoġġjaw rapporti ta’ inċidenti preċiżi u f’waqthom lill-awtoritajiet kompetenti.

11.10 DORA tal-UE (2022/2554)

11.10.1 Artikolu 17 – Rappurtar ta’ Inċidenti tal-ICT: Jeħtieġ reġistri dettaljati tal-kawża ewlenija u tal-evidenza għal inċidenti ewlenin relatati mal-ICT, b’mod partikolari fis-settur finanzjarju.

11.11 COBIT 2019

11.11.1 DSS01.07 – Ġestjoni ta’ Inċidenti tas-Sigurtà: Jitlob dokumentazzjoni tal-inċidenti u rigorożità investigattiva.

11.11.2 DSS05.04 – Ġestjoni ta’ Investigazzjonijiet tas-Sigurtà: Jenfasizza l-preservazzjoni tal-evidenza diġitali u l-appoġġ għal azzjonijiet dixxiplinari u legali.