					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P33					Titlu tad-dokument: **Politika ta' Monitoraġġ tal-Awditjar u l-Konformità**							
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 9.2, 9.3, 10	
ISO/IEC 27002:2022	Kontrolli 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
GDPR tal-UE	Artikoli 24, 32, 33	
Direttiva NIS2 tal-UE	Artikolu 21(2)(g), 27	
DORA tal-UE	Artikoli 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Għan

1.1 L-għan ta’ din il-politika huwa li tistabbilixxi u tirregola l-programm tal-organizzazzjoni għall-monitoraġġ tal-awditjar u l-konformità sabiex:

1.1.1 Tiġi vverifikata l-effettività tal-kontrolli tas-sigurtà u tal-privatezza

1.1.2 Tiġi żgurata l-allinjazzjoni ma’ standards applikabbli, oqfsa legali u obbligi kuntrattwali

1.1.3 Jinstabu fil-ħin nuqqasijiet ta’ konformità, ineffiċjenzi u riskji ta’ konformità

1.1.4 Jiġi appoġġat it-titjib kontinwu u l-kapaċità li tintwera l-konformità għal ċertifikazzjonijiet, evalwazzjonijiet u rieżamijiet regolatorji

1.2 Din il-politika tappoġġa l-integrità u l-maturità tas-Sistema ta’ Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS) billi tintegra prattiki ta’ awditjar u monitoraġġ strutturati, immexxija mir-riskju u bbażati fuq l-evidenza.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-unitajiet interni kollha tan-negozju, il-funzjonijiet u d-dipartimenti

2.1.2 Faċilitajiet fiżiċi, ambjenti cloud, pjattaformi SaaS u servizzi esternalizzati

2.1.3 Sistemi tal-informazzjoni, applikazzjonijiet, infrastruttura u assi tad-data rregolati mill-ISMS

2.1.4 Impjegati, kuntratturi u fornituri terzi ta’ servizzi b’obbligi ta’ awditjar jew ta’ konformità

2.2 Il-politika tkopri:

2.2.1 Awditjar intern

2.2.2 Awditi esterni/taċ-ċertifikazzjoni

2.2.3 Monitoraġġ tekniku tal-konformità

2.2.4 Awditi tal-fornituri u ta’ partijiet terzi

2.2.5 Azzjonijiet korrettivi u preventivi (CAPA)

2.2.6 Metriċi, dashboards u proċessi ta’ rappurtar

2.3 Tapplika wkoll għall-oqfsa rilevanti kollha li għalihom l-organizzazzjoni hija soġġetta, inklużi ISO/IEC 27001, GDPR, NIS2, DORA u SOC 2, fost oħrajn.

3. Objettivi

3.1 Li tiġi vverifikata l-adegwatezza u l-effettività tal-kontrolli, il-politiki u l-proċeduri implimentati fl-ISMS kollu u fl-ambjenti relatati.

3.2 Li jiġu identifikati u rimedjati kwalunkwe defiċjenzi, nuqqasijiet ta' konformità jew lakuni fil-konformità qabel ma jeskalaw f'inċidenti jew ksur.

3.3 Li tiġi żgurata tħejjija kontinwa għal rieżamijiet interni tal-governanza, awditi esterni u ċertifikazzjonijiet indipendenti.

3.4 Li tiġi ġġenerata evidenza difensibbli u traċċi tal-awditjar b'appoġġ għal mistoqsijiet regolatorji, proċessi legali jew talbiet ta' assigurazzjoni minn klijenti.

3.5 Li r-riżultati tal-awditjar jiġu integrati fil-ġestjoni usa' tar-riskju tal-organizzazzjoni, fil-metriċi tas-sigurtà u fl-attivitajiet ta' titjib kontinwu.

4. Rwoli u responsabbiltajiet

4.1 Responsabbli mill-Awditjar Intern / Maniġer tal-Konformità

4.1.1 Jippjana, jiskeda u jwettaq awditi interni abbażi tal-prijorità tar-riskju.

4.1.2 Iżomm ir-Reġistru tal-Awditjar, jikkoordina l-attivitajiet tal-awditjar u jsegwi l-azzjonijiet korrettivi.

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

4.2.1 Jiżgura li l-kamp ta' applikazzjoni tal-awditjar ikopri l-elementi rilevanti kollha tal-ISMS u l-kontrolli tal-Anness A.

4.2.2 Jeżerċita sorveljanza fuq il-verifika tal-CAPA u jintegra r-riżultati tal-awditjar fil-programm tas-sigurtà.

[... 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 kull sena mill-Maniġer tal-Konformità u mis-CISO, jew qabel b'reazzjoni għal:

9.1.1 Bidliet fl-oqfsa regolatorji, kuntrattwali jew taċ-ċertifikazzjoni

9.1.2 Sejbiet sinifikanti tal-awditjar jew fallimenti ripetuti tal-kontrolli

9.1.3 Ristrutturar organizzattiv jew bidliet fis-sistema GRC

9.1.4 Rakkomandazzjonijiet minn awdituri esterni jew feedback minn regolaturi

9.2 Il-proċess ta' rieżami għandu jevalwa:

9.2.1 Il-metodoloġija u l-frekwenza tal-ippjanar tal-awditjar

9.2.2 Bidliet fil-kamp ta' applikazzjoni tal-ISMS jew fl-infrastruttura

9.2.3 Aġġornamenti għall-katalgu tal-kontrolli jew għar-reġistru legali

9.2.4 Il-konsistenza u l-kwalità tal-evidenza tal-awditjar u tal-proċessi CAPA

9.3 Il-bidliet kollha fil-politika għandhom ikunu:

9.3.1 Dokumentati f'repożitorju taħt kontroll tal-verżjoni

9.3.2 Approvati mill-maniġment eżekuttiv

9.3.3 Ikkomunikati lill-persunal kollu affettwat u integrati fil-proċeduri aġġornati u fil-programmi ta' sensibilizzazzjoni

9.4 Verifika wara r-rieżami għandha tikkonferma li r-rekwiżiti aġġornati huma riflessi fir-Reġistru tal-Awditjar, fl-għodod tal-konformità u fid-dashboards interni tal-monitoraġġ.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija allinjata mal-politiki organizzattivi relatati li ġejjin:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tiddefinixxi l-ISMS u tistabbilixxi r-responsabbiltà għall-konformità u t-titjib kontinwu

10.1.2 P5 – Politika tal-Ġestjoni tat-Tibdil: Tiżgura viżibbiltà għall-awditjar dwar bidliet fl-infrastruttura u fil-konfigurazzjoni li jaffettwaw l-ambjenti tal-kontroll

10.1.3 P6 – Politika tal-Ġestjoni tar-Riskju: Tintegra l-eżiti tal-awditjar fl-evalwazzjoni u fl-attivitajiet ta' trattament tar-riskju fil-livell tal-intrapriża

10.1.4 P14 – Politika taż-Żamma u r-Rimi tad-Data: Tirregola ż-żamma tal-evidenza tal-awditjar, il-logs u r-reġistri tal-konformità

10.1.5 P18 – Politika tal-Kontrolli Kriptografiċi: Tappoġġa l-ħażna u t-trasferiment siguri ta' data sensittiva tal-awditjar

10.1.6 P26 – Politika tas-Sigurtà ta' Partijiet Terzi u tal-Fornituri: Tkopri d-drittijiet tal-awditjar, id-dokumentazzjoni ta' assigurazzjoni u s-sorveljanza tal-konformità tal-fornituri

10.1.7 P30 – Politika dwar ir-Rispons għall-Inċidenti: Tallinja l-awditi tal-proċessi tal-immaniġġjar tal-inċidenti mal-għanijiet ta' assigurazzjoni tal-ISMS

10.1.8 P32 – Politika dwar il-Kontinwità tan-Negozju u l-Irkupru minn Diżastri: Teħtieġ verifika tat-testijiet tal-kontinwità u tal-konformità mad-DRP waqt iċ-ċikli tal-awditjar

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata ma' standards globali u rekwiżiti legali għall-awditjar u l-verifika kontinwa tal-konformità.

11.2 ISO/IEC 27001:

11.2.1 Klawżola 9.2 – Awditjar intern: Teħtieġ awditi regolari u bbażati fuq ir-riskju tal-ISMS biex jiġu evalwati l-effettività u l-konformità.

11.2.2 Klawżola 9.3 – Rieżami tal-ġestjoni: L-eżiti tal-awditjar għandhom jidħlu fir-rieżami strateġiku u fit-titjib.

11.2.3 Klawżola 10.1 – Nuqqas ta' konformità u azzjoni korrettiva: Is-sejbiet tal-awditjar għandhom jiġu indirizzati permezz ta' proċeduri CAPA dokumentati.

11.3 ISO/IEC 27002:2022 – Kontrolli 5.35–5.37:

11.3.1 Kontrolli tal-Anness A 5.35–5.37: Ikopru rieżami indipendenti, konformità mar-rekwiżiti legali/kuntrattwali u reġistrazzjoni tal-awditjar.

11.3.2 Jipprovdu gwida ta' implimentazzjoni għall-ippjanar, l-eżekuzzjoni u t-titjib tal-programmi tal-awditjar u tal-konformità.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Evalwazzjonijiet tal-kontrolli: Jeħtieġ rieżami ta' rutina tal-kontrolli tas-sigurtà implimentati.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): Jallinja mat-traċċar u mar-rimedjazzjoni tas-sejbiet tal-awditjar.

11.4.3 CA-7 – Monitoraġġ kontinwu: Jappoġġa evalwazzjonijiet proattivi u awtomatizzati tal-konformità.

11.5 GDPR tal-UE (2016/679):

11.5.1 Artikoli 24 u 32: Jeħtieġu evidenza tal-implimentazzjoni u l-effettività tal-kontrolli tas-sigurtà permezz ta' strutturi xierqa ta' governanza.

11.5.2 Artikolu 33: Jappoġġa l-ħtieġa għal traċċi tal-awditjar verifikati fir-rispons għal ksur u fin-notifika.

11.6 Direttiva NIS2 tal-UE (2022/2555):

11.6.1 Artikolu 21(2)(g): Jeħtieġ awditjar tal-politiki u l-proċeduri bħala parti mill-miżuri minimi tal-ġestjoni tar-riskju taċ-ċibersigurtà.

11.6.2 Artikolu 27: L-awtoritajiet nazzjonali jistgħu jwettqu jew jeħtieġu awditi għal entitajiet essenzjali u importanti.

11.7 DORA tal-UE (2022/2554):

11.7.1 Artikolu 10(2)(e): L-entitajiet għandhom iwettqu awditi interni u esterni tal-prattiki tal-ġestjoni tar-riskju tal-ICT.

11.7.2 Artikolu 25 – Rekwiżiti tal-awditjar: Jeħtieġ awditi perjodiċi minn awdituri interni jew awdituri esterni indipendenti b'viżibbiltà regolatorja.

11.8 COBIT 2019:

11.8.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Jiżgura li l-effettività tal-kontrolli tiġi vverifikata u rrappurtata lill-korpi ta' governanza.

11.8.2 MEA03 – Monitor, Evaluate and Assess Compliance: Jeħtieġ allinjament tal-prattiki organizzattivi mar-rekwiżiti legali, kuntrattwali u bbażati fuq standards.