					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P33S					Titlu tad-dokument: **Politika tal-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, 10	Awditi interni, titjib kontinwu u rimedjazzjoni ta’ nuqqasijiet ta’ konformità
ISO/IEC 27002:2022	Kontrolli 5.35, 5.37	Rieżamijiet interni skedati u rieżamijiet indipendenti għal proċessi esternalizzati
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Valutazzjonijiet tas-sigurtà, monitoraġġ kontinwu, u rieżami/analiżi/rappurtar tal-awditjar
GDPR tal-UE	Artikoli 24 u 32	Awditjar ta’ miżuri tekniċi u organizzattivi, u evidenza tal-effettività tal-kontrolli
Direttiva NIS2 tal-UE	Artikolu 21(2)(f)	Rieżami proattiv u konformità bbażata fuq l-evidenza
DORA tal-UE	Artikolu 10	Ġestjoni tar-riskju tal-ICT, monitoraġġ u rappurtar
COBIT 2019	MEA01, MEA03	Monitoraġġ/evalwazzjoni tal-konformità, konformità, u l-kapaċità li tintwera l-konformità f’rieżamijiet minn partijiet terzi

1. Għan

1.1 Din il-politika tistabbilixxi l-approċċ tal-organizzazzjoni għat-twettiq ta’ awditi interni, verifiki tal-kontrolli tas-sigurtà u monitoraġġ tal-konformità regolatorja. Tiżgura li l-kontrolli, il-politiki, is-sistemi u l-forniturі tas-servizzi kollha jkunu soġġetti għal rieżami regolari u strutturat.

1.2 L-għan huwa li jiġu identifikati fallimenti fil-kontrolli, jiġi evitat nuqqas ta’ konformità u tintwera diliġenza dovuta skont ISO/IEC 27001, il-GDPR u oqfsa relatati.

1.3 Din tippermetti lill-SMEs iżommu kontroll operattiv u jkunu lesti għaċ-ċertifikazzjoni, anke mingħajr dipartiment dedikat għall-konformità, permezz ta’ listi ta’ kontroll sempliċi u ripetibbli u sejbiet ipprijoritizzati skont ir-riskju.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Id-dipartimenti interni kollha u l-forniturі esterni ta’ servizzi tal-IT b’responsabbiltajiet relatati ma’ sistemi tal-IT, data personali u servizzi kritiċi għan-negozju

2.1.2 Il-kontrolli u s-sistemi kollha fil-kamp ta’ applikazzjoni tas-Sistema ta’ Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS)

2.1.3 L-awditi interni kollha, ir-rieżamijiet tal-kontrolli tas-sigurtà u l-verifiki tal-konformità, kemm jekk isiru internament kif ukoll minn konsulent estern, klijent jew regolatur

2.2 Din il-politika tapplika wkoll għall-ġbir tal-evidenza u għar-rappurtar għal:

2.2.1 Awditi taċ-ċertifikazzjoni u taċ-ċertifikazzjoni mill-ġdid tal-ISO/IEC 27001

2.2.2 Awditi tal-protezzjoni tad-data skont il-GDPR jew skont termini kuntrattwali

2.2.3 Kwestjonarji tas-sigurtà mmexxija mill-klijent jew rieżamijiet ta’ diliġenza dovuta

2.2.4 Kwalunkwe rieżami regolatorju jew indipendenti skont in-NIS2 jew id-DORA, fejn applikabbli

3. Objettivi

3.1 Jiġi żgurat li l-kontrolli u l-politiki ewlenin kollha jiġu rieżaminati regolarment għall-effettività u l-konformità.

3.2 Jinżammu traċċi tal-awditjar u reġistri ta’ azzjonijiet korrettivi biex tintwera r-responsabbiltà u t-titjib.

3.3 Titħejja l-organizzazzjoni għaċ-ċertifikazzjoni, iċ-ċertifikazzjoni mill-ġdid u programmi ta’ assigurazzjoni għall-klijenti (eż. ISO 27001, integrazzjoni tal-fornitur).

3.4 Jiġu identifikati l-lakuni minn stadju bikri biex tkun possibbli rimedjazzjoni fil-pront qabel ma l-kwistjonijiet jeskalaw jew iwasslu għal ksur ta’ obbligi.

3.5 Jingħata appoġġ lill-Maniġer Ġenerali u lill-fornitur tas-servizzi tal-IT biex jikkoordinaw ir-rieżamijiet b’kumplessità minima filwaqt li jiġu żgurati riżultati difensibbli.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Jissorvelja l-programm tal-awditjar

4.1.2 Japprova l-pjanijiet u s-sejbiet tar-rieżami intern

4.1.3 Jassenja u jsegwi l-azzjonijiet korrettivi

4.1.4 Jawtorizza l-ingaġġ ta’ awdituri jew konsulenti esterni

4.2 Fornitur ta’ Appoġġ tal-IT / Amministratur

4.2.1 Jipprovdi evidenza waqt awditi interni u esterni (eż. logs, konfigurazzjonijiet, reġistri tal-kontroll tal-aċċess)

4.2.2 Jassisti fil-verifiki tekniċi (eż. status tal-backups, konformità tal-patches)

4.2.3 Iżomm ir-repożitorju tal-evidenza tal-awditjar

[... 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 annwali tal-politika u tal-pjan tal-awditjar

9.1.1 Il-Maniġer Ġenerali (GM) għandu jirrieżamina din il-politika u l-iskeda tal-awditjar mill-inqas darba fis-sena.

9.1.2 Ir-rieżami għandu jevalwa:

9.1.2.1 L-effettività tal-awditi fl-identifikazzjoni tal-lakuni

9.1.2.2 Ir-rata ta’ tlestija tal-awditi u tal-azzjonijiet korrettivi

9.1.2.3 Bidliet fir-rekwiżiti legali, regolatorji jew taċ-ċertifikazzjoni applikabbli

9.2 Aġġornamenti bbażati fuq skattaturi

9.2.1 Il-politika għandha tiġi rieżaminata u aġġornata meta:

9.2.2 Ċertifikazzjoni jew awditu ta’ sorveljanza jirriżulta f’nuqqas ta’ konformità maġġuri

9.2.3 Jinbidlu l-oqfsa legali jew regolatorji (eż. gwida ġdida dwar il-GDPR, implimentazzjoni nazzjonali tan-NIS2)

9.2.4 Bidliet fin-negozju jaffettwaw sistemi, proċessi jew forniturі inklużi fil-kamp ta’ applikazzjoni tal-awditjar

9.2.5 Inċident kritiku jew ksur jiżvela lakuni fil-kontrolli li ma kinux instabu qabel

9.3 Dokumentazzjoni tal-aġġornamenti

9.3.1 Ir-reviżjonijiet kollha għandhom jiġu rreġistrati f’log tal-kontroll tal-verżjoni tal-politika

9.3.2 L-aġġornamenti għandhom jitqassmu lill-membri kollha tat-tim involuti fl-awditi

9.3.3 Sommarju tal-bidliet għandu jiġi inkluż mal-politika aġġornata biex jiżgura l-fehim

10. Politiki relatati u rabtiet

10.1 Din il-politika hija appoġġata minn u ssaħħaħ diversi politiki oħra għall-SMEs:

10.1.1 P1S – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-linja bażi għall-aspettattivi kollha tal-kontrolli u teħtieġ l-applikazzjoni tagħhom permezz tal-awditi.

10.1.2 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tistabbilixxi r-responsabbiltà għall-ippjanar tal-awditjar, l-eżekuzzjoni u s-sjieda tal-azzjoni korrettiva.

10.1.3 P6S – Politika tal-Ġestjoni tar-Riskju: Tidentifika d-dgħufijiet fil-kontrolli żvelati fl-awditi u tiżgura li s-sejbiet jiġu dokumentati fir-Reġistru tar-Riskji.

10.1.4 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiddefinixxi l-kontrolli tal-GDPR li għandhom jiġu awditjati, inkluż l-immaniġġjar tad-data, ir-rispons għall-ksur u n-notifiki tal-privatezza.

10.1.5 P22S – Politika tal-Illoggjar u l-Monitoraġġ: Tipprovdi l-logs tal-awditjar u d-data forensika użati waqt rieżamijiet tal-konformità u tal-kontrolli.

10.1.6 P30S – Politika dwar ir-Rispons għall-Inċidenti: Teħtieġ awditjar perjodiku tar-reġistri tal-inċidenti u rieżamijiet wara l-avveniment biex tiġi vverifikata l-effettività tar-rispons.

10.1.7 P31S – Politika dwar il-Ġbir tal-Evidenza u l-Forensika: Tipprovdi l-proċeduri għall-ġbir ta' evidenza verifikabbli b'chain of custody waqt l-awditi.

10.2 Flimkien, dawn il-politiki joħolqu ambjent ta' kontroll b'ċiklu magħluq li jippermetti verifika interna, assigurazzjoni esterna u governanza allinjata mal-istandards.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:

11.1.1 Klawżola 9.2 – Teħtieġ awditi interni biex jevalwaw il-prestazzjoni tal-ISMS u l-allinjament tiegħu mar-rekwiżiti.

11.1.2 Klawżola 10.1 – Tobbliga titjib kontinwu bbażat fuq ir-riżultati tal-awditjar u r-rimedjazzjoni tan-nuqqasijiet ta' konformità.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 5.35 – Jeħtieġ rieżamijiet interni skedati tal-kontrolli u tal-proċessi.

11.2.2 Kontroll 5.37 – Jenfasizza rieżamijiet indipendenti, b'mod partikolari għal proċessi esternalizzati.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Valutazzjonijiet tas-Sigurtà: Jeħtieġ awditi tal-kontrolli implimentati biex tiġi vverifikata l-effettività.

11.3.2 CA-7 – Monitoraġġ Kontinwu: Jenfasizza s-sejbien proattiv u r-rieżami tad-dgħufijiet fil-kontrolli.

11.3.3 AU-6 – Rieżami, Analiżi u Rappurtar tal-Awditjar: Tobbliga analiżi regolari u riżoluzzjoni tal-logs tal-awditjar u tas-sejbiet.

11.4 GDPR tal-UE:

11.4.1 Artikoli 24 u 32 – Jeħtieġu l-implimentazzjoni u l-awditjar ta' miżuri tekniċi u organizzattivi, inkluża evidenza tal-effettività tal-kontrolli u t-titjib maż-żmien.

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

11.5.1 Artikoli 20–21 – Tobbliga rieżami proattiv tal-kontrolli, konformità bbażata fuq l-evidenza u awditabbiltà għal entitajiet essenzjali u importanti.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Jeħtieġ valutazzjoni perjodika tal-prestazzjoni tal-proċessi u tal-kontrolli kontra standards u għanijiet.

11.6.2 MEA03 – Ensure Compliance with External Requirements: Jiffoka fuq monitoraġġ intern u l-kapaċità li tintwera l-konformità għal awditi minn partijiet terzi u rieżamijiet regolatorji.