					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P01S					Titlu tad-dokument: **Politika dwar is-Sigurtà tal-Informazzjoni**							
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 5.1, 5.2, 5.3, 6.1, 6.2, 8	Tispeċifika l-impenn tal-maniġment, ir-rekwiżiti tal-politika, l-assenjazzjoni tar-rwoli, il-valutazzjoni tar-riskju u l-kontroll operattiv
ISO/IEC 27002:2022	Kontrolli 5.1–5	Tispeċifika l-istabbiliment ta’ politiki dokumentati dwar is-sigurtà tal-informazzjoni, l-assenjazzjoni tar-rwoli, is-separazzjoni tad-dmirijiet u r-responsabbiltajiet tal-maniġment
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Rekwiżiti għal pjan tal-programm tas-sigurtà, politika ta’ ppjanar, valutazzjoni/awtorizzazzjoni u kontroll tal-aċċess
GDPR tal-UE (2016/679)	Artikolu 5(2), Artikolu 32	Prinċipju ta’ accountability u miżuri għas-sigurtà tal-ipproċessar, b’enfasi partikolari fuq rwoli dokumentati
Direttiva NIS2 tal-UE (2022/2555)	Artikolu 21(2)(a)	Teħtieġ miżuri ta’ ġestjoni tar-riskju, rwoli u responsabbiltajiet għar-riskju ċibernetiku
DORA tal-UE (2022/2554)	Artikolu 9, Artikolu 10	Teħtieġ l-assenjazzjoni ta’ rwoli għall-ġestjoni tar-riskju tal-ICT u għall-kontinwità tan-negozju
COBIT 2019	EDM03, APO13, DSS05	Jiżgura l-ottimizzazzjoni tar-riskju, il-ġestjoni tas-sigurtà u l-ġestjoni tas-servizzi tas-sigurtà permezz ta’ assenjazzjoni ċara tar-rwoli

1. Għan

1.1 Din il-politika tistabbilixxi l-impenn tal-organizzazzjoni tagħna biex tipproteġi l-informazzjoni tal-klijenti u tan-negozju billi tiddefinixxi b’mod ċar ir-responsabbiltajiet u l-miżuri prattiċi tas-sigurtà, adattati għal organizzazzjonijiet mingħajr timijiet dedikati tal-IT.

1.2 Tiżgura li l-impjegati, il-kuntratturi u l-forniturі tas-servizzi kollha jikkonformaw ma’ regoli vinkolanti, sabiex tkun possibbli konformità sħiħa mar-rekwiżiti għaċ-ċertifikazzjoni ISO/IEC 27001.

1.3 Din il-politika tippermetti lill-organizzazzjoni tagħna ssaħħaħ il-fiduċja tal-klijenti billi turi b’mod ċar kif nipproteġu l-informazzjoni tagħhom permezz ta’ responsabbiltajiet definiti, proċessi strutturati u accountability b’saħħitha.

2. Ambitu

2.1 Din il-politika tapplika għall-individwi kollha li jaċċessaw jew jimmaniġġjaw id-data u s-sistemi tal-organizzazzjoni, inklużi:

2.1.1 Is-sidien tan-negozju u l-maniġers ġenerali

2.1.2 L-impjegati, il-kuntratturi u l-apprendisti

2.1.3 Forniturі esterni ta’ servizzi tal-IT jew konsulenti

2.2 Tkopri t-tipi kollha ta’ informazzjoni, sistemi u servizzi, inklużi:

2.2.1 Reġistri tan-negozju, data tal-klijenti, passwords u emails

2.2.2 Ħardwer tal-IT bħal laptops u telefowns

2.2.3 Servizzi cloud użati għall-ħażna ta’ fajls, komunikazzjoni jew finanzi

2.2.4 Dokumenti fiżiċi maħżuna fil-postijiet tal-uffiċċju

2.3 Il-politika tapplika fl-ambjenti kollha tax-xogħol — fl-uffiċċju, b’mod remot u f’ambjent cloud — u tinkludi l-apparati u s-software kollha użati biex tiġi pproċessata jew maħżuna l-informazzjoni tan-negozju.

3. Objettivi

3.1 Assenjazzjoni ċara tar-responsabbiltà: Jiġi żgurat li dejjem ikun hemm persuna responsabbli għas-sigurtà tal-informazzjoni. Tipikament, din tkun il-Maniġer Ġenerali jew il-persuna maħtura formalment minnu jew minnha.

3.2 Protezzjoni tal-informazzjoni tal-klijenti u tan-negozju: Jiġu implimentati salvagwardji affidabbli u konsistenti biex jiġi evitat l-użu ħażin, it-telf jew is-serq ta’ data sensittiva, inklużi reġistri tal-klijenti u finanzjarji.

3.3 Appoġġ għaċ-ċertifikazzjoni ISO/IEC 27001: L-organizzazzjoni tkun tista’ turi konformità sħiħa mar-rekwiżiti ta’ ISO/IEC 27001, tkun lesta għall-awditjar u eliġibbli għaċ-ċertifikazzjoni mingħajr ma teħtieġ infrastruttura kumplessa.

3.4 Integrazzjoni tas-sigurtà fl-operat tan-negozju: Is-sigurtà tal-informazzjoni tiġi integrata fil-kompiti u fid-deċiżjonijiet ta’ kuljum madwar l-organizzazzjoni kollha.

3.5 Tisħiħ tal-għarfien u tal-kultura tas-sigurtà: Kull impjegat għandu jifhem u josserva l-prattiki tas-sigurtà, bħall-użu ta’ passwords b’saħħithom u r-rappurtar ta’ attività suspettuża.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali jew Sid tan-Negozju

4.1.1 Iġorr accountability sħiħa għas-sigurtà tal-informazzjoni.

4.1.2 Japprova u jżomm din il-politika aġġornata.

4.1.3 Jiżgura li l-kompiti ewlenin kollha tas-sigurtà jitwettqu direttament jew jiġu delegati bil-miktub.

4.1.4 Jivverifika li kwalunkwe kompitu tas-sigurtà delegat (bħall-ġestjoni tal-aċċess jew ir-rispons għall-inċidenti) jitwettaq b’mod effettiv.

4.1.5 Isservi bħala l-punt ta’ kuntatt awtomatiku għall-kwistjonijiet kollha tas-sigurtà interni u esterni, inklużi awditi u mistoqsijiet tal-klijenti.

4.1.6 Jimmonitorja l-progress lejn dawn l-objettivi matul ir-rieżami annwali. L-objettivi għandhom ikunu jistgħu jitkejlu fejn possibbli (eż. % tal-persunal imħarreġ, numru ta’ inċidenti rrappurtati, eċċ.) u għandhom jiġu riveduti skont is-sejbiet tas-sigurtà u l-bidliet fir-riskju.

4.2 Impjegat Maħtur (jekk applikabbli)

4.2.1 Jista’ jassisti lill-Maniġer Ġenerali billi jimmaniġġja l-kompiti ta’ kuljum, bħall-ħolqien ta’ kontijiet tal-utenti, it-tneħħija tal-aċċess għal min jitlaq mill-impjieg, jew il-koordinazzjoni mal-fornitur tal-IT.

4.2.2 Irid ikun maħtur uffiċjalment u jkollu biżżejjed awtorità u għodod biex iwettaq il-kompiti.

4.2.3 Jirrapporta kwalunkwe kwistjoni lill-Maniġer Ġenerali.

[... 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

9.1.1 Din il-politika trid tiġi rieżaminata mill-Maniġer Ġenerali (GM) mill-inqas darba fis-sena biex tiġi żgurata konformità kontinwa mar-rekwiżiti għaċ-ċertifikazzjoni ISO/IEC 27001, mal-bidliet regolatorji (bħal GDPR, NIS2 u DORA) u mal-ħtiġijiet tan-negozju li qed jevolvu.

9.2 Rieżamijiet interim

9.2.1 Għandhom isiru rieżamijiet addizzjonali kull meta jkun hemm bidliet sinifikanti, bħal:

9.2.1.1 Inċidenti tas-sigurtà kbar jew ksur tad-data.

9.2.1.2 Introduzzjoni ta' proċessi jew teknoloġiji ġodda tan-negozju (eż. software ġdid, pjattaformi ta' xogħol remot jew servizzi cloud).

9.2.1.3 Bidliet fir-rekwiżiti legali jew regolatorji li jaffettwaw l-immaniġġjar tal-informazzjoni.

9.3 Dokumentazzjoni tal-bidliet

9.3.1 Ir-rieżamijiet kollha tal-politika u l-bidliet għandhom jiġu dokumentati formalment, b'dikjarazzjoni ċara tad-data, in-natura tar-reviżjonijiet u l-approvazzjoni tal-GM.

9.3.2 Reġistru storiku tal-verżjonijiet tal-politika għandu jinżamm b'mod sigur biex juri l-evoluzzjoni tal-politika u l-konformità waqt l-awditi.

9.4 Komunikazzjoni tal-aġġornamenti

9.4.1 Kwalunkwe bidla f'din il-politika trid tiġi kkomunikata minnufih lill-impjegati kollha, lill-kuntratturi u lill-partijiet terzi rilevanti.

9.4.2 Verżjonijiet aġġornati tal-politika għandhom ikunu faċilment aċċessibbli għall-persunal kollu affettwat (eż. maqsuma elettronikament jew imwaħħla fiżikament fil-post tax-xogħol).

10. Politiki relatati u rabtiet

10.1 Din il-politika hija marbuta mill-qrib ma' politiki oħra fis-sett ta' politiki SME tal-organizzazzjoni, b'mod partikolari:

10.1.1 P2S – Politika dwar ir-rwoli u r-responsabbiltajiet ta' governanza: Tiċċara l-assenjazzjoni tad-dmirijiet u r-responsabbiltajiet tas-sigurtà.

10.1.2 P4S – Politika dwar il-kontroll tal-aċċess: Tiddefinixxi l-immaniġġjar sigur tal-aċċess għall-informazzjoni tal-kumpanija.

10.1.3 P8S – Politika dwar l-għarfien u t-taħriġ fis-sigurtà tal-informazzjoni: Tipprovdi linji gwida essenzjali għat-taħriġ u l-għarfien tal-persunal.

10.1.4 P17S – Politika dwar il-protezzjoni tad-data u l-privatezza: Tiżgura konformità mal-GDPR u ma' liġijiet oħra dwar il-protezzjoni tad-data.

10.1.5 P30S – Politika dwar ir-rispons għall-inċidenti: Tiddeskrivi l-azzjonijiet dettaljati meħtieġa b'rispons għal inċidenti tas-sigurtà.

10.2 Dawn il-politiki marbuta jipprovdu gwida operattiva ċara u għandhom jiġu implimentati b'mod kollettiv biex tinkiseb konformità sħiħa għaċ-ċertifikazzjoni ISO/IEC 27001.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 5.1 – Tmexxija u impenn: Teħtieġ impenn mill-ogħla maniġment u accountability għall-effettività tas-sigurtà tal-informazzjoni fi ħdan l-organizzazzjoni.

11.1.2 Klawżola 5.2 – Politika dwar is-sigurtà tal-informazzjoni: Tesiġi politiki ċari u dokumentati allinjati mal-istrateġija organizzattiva u mar-rekwiżiti ta' konformità.

11.1.3 Klawżola 5.3 – Rwoli u responsabbiltajiet organizzattivi: Tiddefinixxi assenjazzjoni ċara tar-responsabbiltajiet għas-sigurtà tal-informazzjoni madwar l-organizzazzjoni, essenzjali għal governanza effettiva u konformità mal-awditjar.

11.1.4 Klawżola 6.1 – Azzjonijiet biex jiġu indirizzati r-riskji u l-opportunitajiet: Tiżgura li r-riskji għas-sigurtà tal-informazzjoni jiġu identifikati, ivvalutati u trattati b'mod sistematiku.

11.1.5 Klawżola 8.1 – Ippjanar u kontroll operattiv: Teħtieġ li l-organizzazzjoni tippjana u timplimenta l-proċessi meħtieġa biex jintlaħqu l-objettivi tas-sigurtà tal-informazzjoni u biex ir-riskji assoċjati jiġu ġestiti b'mod effettiv.

11.2 Kontrolli 5.1–5 ta' ISO/IEC 27002:2022

11.2.1 Kontroll 5.1 tal-Anness A – Politiki għas-sigurtà tal-informazzjoni: Tispeċifika l-istabbiliment u l-komunikazzjoni ta' politiki dokumentati dwar is-sigurtà tal-informazzjoni.

11.2.2 Kontroll 5.2 tal-Anness A – Rwoli għas-sigurtà tal-informazzjoni: Jiċċara u jassenja formalment ir-rwoli u r-responsabbiltajiet għas-sigurtà tal-informazzjoni lill-partijiet rilevanti.

11.2.3 Kontroll 5.3 tal-Anness A – Separazzjoni tad-dmirijiet: Jeħtieġ separazzjoni ċara tad-dmirijiet biex jitnaqqsu l-kunflitti ta' interess u r-riskji ta' frodi fil-ġestjoni ta' informazzjoni sensittiva.

11.2.4 Kontroll 5.4 tal-Anness A – Responsabbiltajiet tal-maniġment: Tesiġi li l-maniġment juri impenn għas-sigurtà tal-informazzjoni permezz ta' sorveljanza attiva u allokazzjoni tar-riżorsi.

11.2.5 Issaħħaħ il-ħtieġa ta' politiki, rwoli, responsabbiltajiet u strutturi ta' governanza dwar is-sigurtà tal-informazzjoni dokumentati b'mod ċar, biex tiġi żgurata ġestjoni konsistenti u traċċabbiltà għall-awditjar fl-organizzazzjoni kollha.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Pjan tal-programm tas-sigurtà tal-informazzjoni: Jeħtieġ strateġiji u politiki dokumentati ta' governanza għas-sigurtà tal-informazzjoni, li jipprovdu qafas għal implimentazzjoni u ġestjoni konsistenti.

11.3.2 PL-1 – Politika ta' ppjanar tas-sigurtà: Tesiġi politika ta' ppjanar tas-sigurtà għall-organizzazzjoni kollha biex tiggwida l-operat sigur u l-allinjament strateġiku tal-attivitajiet tas-sigurtà tal-informazzjoni.

11.3.3 CA-1 – Politika ta' valutazzjoni u awtorizzazzjoni tas-sigurtà: Teħtieġ rwoli definiti b'mod ċar għall-valutazzjoni u l-awtorizzazzjoni biex tiġi żgurata effettività kontinwa u konformità mar-rekwiżiti tas-sigurtà tal-informazzjoni.

11.3.4 AC-1 – Politika dwar il-kontroll tal-aċċess: Teħtieġ li l-organizzazzjonijiet jiddefinixxu, jiddokumentaw u japplikaw b'mod ċar il-prattiki u r-responsabbiltajiet għall-ġestjoni tal-aċċess.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 5(2) – Prinċipju ta' accountability: Jeħtieġ li l-organizzazzjonijiet juru konformità mal-prinċipji tal-protezzjoni tad-data, inklużi rwoli u politiki dokumentati għar-responsabbiltajiet relatati mal-protezzjoni tad-data.

11.4.2 Artikolu 32 – Sigurtà tal-ipproċessar: Tesiġi l-implimentazzjoni ta' miżuri tekniċi u organizzattivi xierqa, inklużi responsabbiltajiet ċari tas-sigurtà, biex tipproteġi d-data personali minn ksur u aċċess mhux awtorizzat.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(a) – Miżuri ta' ġestjoni tar-riskju: Jeħtieġ arranġamenti ċari ta' governanza, inklużi rwoli u responsabbiltajiet definiti għas-sigurtà tal-informazzjoni, essenzjali biex ir-riskji ċibernetiċi jiġu ġestiti b'mod effettiv.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 9 – Ġestjoni tar-riskju tal-ICT: Jeħtieġ li l-organizzazzjonijiet jassenjaw b'mod ċar ir-rwoli u r-responsabbiltajiet relatati mal-ġestjoni tar-riskju tal-ICT, u b'hekk isaħħu r-reżiljenza u t-tħejjija għall-kontinwità tan-negozju.

11.6.2 Artikolu 10 – Kontinwità tan-negozju tal-ICT: Jeħtieġ accountability ċara u rwoli strutturati biex tinżamm ir-reżiljenza u l-kontinwità tal-ICT, u jiżgura li l-organizzazzjonijiet ikunu jistgħu jirrispondu b'mod affidabbli għal tfixkil.

11.7 COBIT 2019

11.7.1 EDM03 – Jiżgura l-ottimizzazzjoni tar-riskju: Jenfasizza accountability u rwoli definiti b'mod ċar fil-ġestjoni tar-riskji organizzattivi, u jipprovdi governanza b'saħħitha u sorveljanza effettiva tar-riskji għas-sigurtà tal-informazzjoni.

11.7.2 APO13 – Ġestjoni tas-sigurtà: Teħtieġ li l-organizzazzjonijiet jistabbilixxu u jikkomunikaw b'mod ċar ir-responsabbiltajiet tal-ġestjoni tas-sigurtà, u jiżguraw allinjament mal-objettivi tan-negozju u mar-rekwiżiti regolatorji.

11.7.3 DSS05 – Ġestjoni tas-servizzi tas-sigurtà: Titlob rwoli strutturati u responsabbiltajiet ċari fil-ġestjoni tas-servizzi tas-sigurtà, biex tippermetti implimentazzjoni konsistenti u verifika tal-konformità.