					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P08					Titlu tad-dokument: **Politika dwar l-Għarfien u t-Taħriġ fis-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	Klawżola 7.3, Kontroll 6.3 tal-Anness A	Tistabbilixxi rekwiżiti ta’ għarfien u taħriġ indirizzati minn din il-politika
ISO/IEC 27002:2022	Kontroll 6	Tappoġġa taħriġ ta’ sensibilizzazzjoni xieraq ibbażat fuq ir-rwoli tax-xogħol
NIST SP 800-53 Rev.5	AT-1 sa AT-5	Allinjat mal-politika u l-proċeduri, taħriġ ta’ sensibilizzazzjoni, taħriġ ibbażat fuq ir-rwoli, reġistri tat-taħriġ u kuntatt ma’ gruppi tas-sigurtà
GDPR tal-UE	Artikoli 32, 39; Premessa 78	Jobbliga taħriġ għal min jimmaniġġja data personali u sensibilizzazzjoni ġenerali għall-persunal
Direttiva NIS2 tal-UE	Artikoli 21(2)(a, b), 21(3)	Teħtieġ politiki dwar ir-riskju u taħriġ fis-sigurtà, kif ukoll inizjattivi ta’ sensibilizzazzjoni
DORA tal-UE	Artikoli 5, 8, 13	Teħtieġ għarfien u taħriġ dwar il-ġestjoni tar-riskju tal-ICT bħala parti mill-kontrolli tar-reżiljenza
COBIT 2019	APO07, DSS05, MEA	Issaħħaħ l-għarfien tal-forza tax-xogħol, l-edukazzjoni tal-utenti u l-monitoraġġ tal-konformità

1. Għan

1.1 Din il-politika tistabbilixxi l-qafas formali biex tiżgura li l-persunal kollu jkun konxju mir-responsabbiltajiet tiegħu dwar is-sigurtà tal-informazzjoni u jirċievi t-taħriġ meħtieġ biex jipproteġi l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tal-assi tal-informazzjoni.

1.2 Din tappoġġa l-Klawżola 7.3 tal-ISO/IEC 27001 u l-Kontroll 6.3 tal-Anness A billi tirrikjedi programm strutturat ta’ sensibilizzazzjoni u taħriġ, ibbażat fuq ir-riskju u mfassal skont ir-rwoli organizzattivi u t-theddid li qed jevolvi.

1.3 Il-politika tikkontribwixxi għat-tnaqqis tal-vulnerabbiltajiet marbuta mal-fattur uman, għall-promozzjoni ta’ mġiba konxja mis-sigurtà, u għat-tisħiħ kontinwu ta’ prattiki siguri f’konformità mar-rekwiżiti regolatorji u kuntrattwali.

2. Ambitu

2.1 Din il-politika tapplika għall-individwi interni u esterni kollha li għandhom aċċess għas-sistemi ta’ informazzjoni, għad-data jew għall-faċilitajiet tal-organizzazzjoni, inklużi:

2.1.1 Impjegati (full-time, part-time, temporanji)

2.1.2 Kuntratturi, konsulenti, fornituri u interns

2.1.3 Partijiet terzi b’aċċess loġiku jew fiżiku skont ftehimiet ta’ servizz

2.2 L-ambitu jinkludi:

2.2.1 Taħriġ inizjali ta’ sensibilizzazzjoni dwar is-sigurtà

2.2.2 Taħriġ speċifiku għar-rwol (eż. żviluppaturi, persunal tal-finanzi, utenti privileġġjati)

2.2.3 Taħriġ perjodiku ta’ aġġornament u kampanji ta’ sensibilizzazzjoni

2.2.4 Taħriġ ad hoc b’reazzjoni għal inċidenti jew theddid ġdid

2.3 Il-metodi ta’ twassil tat-taħriġ koperti minn din il-politika jinkludu e-learning, sessjonijiet ta’ tagħrif fil-preżenza, simulazzjonijiet, testijiet tal-għarfien, posters, bullettini tas-sigurtà u rikonoxximenti obbligatorji.

3. Objettivi

3.1 Jiġi żgurat li l-persunal kollu jifhem ir-responsabbiltajiet tiegħu fil-protezzjoni tal-assi tal-organizzazzjoni u fil-konformità mal-politiki tas-sigurtà.

3.2 Jiġi pprovdut taħriġ kontinwu u miżurabbli ta’ sensibilizzazzjoni allinjat mal-esponiment għar-riskju skont ir-rwol.

3.3 Tiġi integrata mġiba sigura fl-operazzjonijiet ta’ kuljum billi jissaħħu prattiki bħall-użu sigur tal-passwords, ir-rappurtar tal-inċidenti u r-reżistenza għall-phishing.

3.4 Tiġi żgurata l-konformità regolatorja u li l-organizzazzjoni tkun lesta għall-awditjar fir-rigward tal-obbligi ta’ taħriġ fis-sigurtà tal-informazzjoni f’diversi industriji u ġurisdizzjonijiet.

3.5 Jitnaqqsu l-inċidenti tas-sigurtà li jirriżultaw minn negliġenza, nuqqas ta’ għarfien jew ġudizzju ħażin permezz ta’ tisħiħ tal-imġiba u rinfurzar kontinwu.

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Japprova l-istrateġija tat-taħriġ fis-sigurtà tal-informazzjoni tal-organizzazzjoni u jiżgura li din ikollha r-riżorsi meħtieġa u tkun integrata fil-prijoritajiet korporattivi.

4.1.2 Jissorvelja l-konformità fil-livell maniġerjali u jiżgura l-osservanza tal-politika fid-dipartimenti kollha.

4.2 Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni / Maniġer tal-ISMS

4.2.1 Huwa s-sid ta’ din il-politika u jiddefinixxi l-qafas ta’ sensibilizzazzjoni u taħriġ skont ir-riskju, il-konformità u l-ħtiġijiet tan-negozju.

4.2.2 Jissorvelja t-tfassil, it-twassil, it-traċċar u r-rieżami tal-inizjattivi kollha ta’ taħriġ fis-sigurtà.

4.2.3 Jiżgura li t-taħriġ jiġi aġġornat perjodikament u jirrifletti t-theddid li qed jevolvi u t-teknoloġiji emerġenti.

[... 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 Frekwenza tar-rieżami

9.1.1 Din il-politika u l-programm ta’ taħriġ assoċjat għandhom jiġu rieżaminati:

9.1.1.1 Kull sena, jew

9.1.1.2 Wara inċidenti kbar li jinvolvu żball uman jew theddid intern

9.1.1.3 Meta jiġu introdotti teknoloġiji jew theddid ġodda sinifikanti

9.1.1.4 B’reazzjoni għal bidliet fl-obbligi legali, kuntrattwali jew taċ-ċertifikazzjoni

9.2 Proċess tar-rieżami

9.2.1 Ir-rieżami għandu jitmexxa mill-Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni f’koordinazzjoni ma’:

9.2.1.1 Id-dipartimenti tar-Riżorsi Umani u tat-Taħriġ

9.2.1.2 Uffiċjali Legali u tal-Protezzjoni tad-Data

9.2.1.3 Il-funzjonijiet tas-Sigurtà tal-IT u tar-Riskju Operattiv

9.2.2 L-aġġornamenti kollha għandhom ikunu:

9.2.2.1 Approvati mill-Kumitat ta' Tmexxija tal-ISMS

9.2.2.2 Taħt kontroll tal-verżjoni u dokumentati fir-Reġistru tad-Dokumenti tal-ISMS

9.2.2.3 Ikkomunikati lill-utenti jekk bidliet materjali jaffettwaw l-ambitu tat-taħriġ jew ir-responsabbiltajiet

9.3 Governanza tal-aġġornament tal-kontenut

9.3.1 Il-moduli tat-taħriġ u l-materjal ta' sensibilizzazzjoni għandhom jiġu rieżaminati kull 12-il xahar biex jiġi żgurat:

9.3.1.1 Ir-rilevanza għall-pajsaġġ tat-theddid

9.3.1.2 L-eżattezza regolatorja

9.3.1.3 Il-kompatibbiltà tal-format (eż. aċċessibbiltà, lokalizzazzjoni)

9.3.2 Kontenut skadut jew qarrieqi għandu jitneħħa minnufih u jiġi sostitwit b'alternattivi approvati.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija sostnuta minn u tappoġġa l-osservanza ta':

10.1.1 P01 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-għarfien dwar is-sigurtà bħala kontroll fundamentali fl-ISMS tal-organizzazzjoni.

10.1.2 P03 – Politika dwar l-Użu Aċċettabbli: Teħtieġ rikonoxximent mill-utent waqt it-taħriġ u tiċċara r-responsabbiltajiet marbuta mal-użu ta' kuljum tat-teknoloġija.

10.1.3 P07 – Politika ta' Induzzjoni u Terminazzjoni: Tiżgura li t-taħriġ ikun integrat fid-dħul u segwit tul il-perjodu kollu tal-impjieg.

10.1.4 P06 – Politika tal-Ġestjoni tar-Riskju: Tgħaqqad taħriġ iffukat fuq il-fattur uman ma' mmudellar tat-theddid u strateġiji għat-tnaqqis tar-riskju residwu.

10.1.5 P33 – Politika tal-Monitoraġġ, l-Awditjar u l-Konformità: Tivvalida li l-kontrolli ta' sensibilizzazzjoni jkunu operattivi, miżurabbli u effettivi matul l-awditi.

10.2 Flimkien, dawn il-politiki jiffurmaw qafas komprensiv ta' kontroll tal-imġiba li jintegra s-sensibilizzazzjoni, l-accountability u t-tisħiħ kulturali.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 7.3 – Sensibilizzazzjoni: Teħtieġ li l-organizzazzjonijiet jiżguraw li l-ħaddiema jkunu konxji mill-politiki tas-sigurtà tal-informazzjoni u mir-responsabbiltajiet tagħhom. Din il-politika tagħmel dan rekwiżit operattiv permezz ta' onboarding strutturat, taħriġ perjodiku u parteċipazzjoni miżurabbli fil-kampanji.

11.1.2 Kontroll 6.3 tal-Anness A – Għarfien, edukazzjoni u taħriġ dwar is-sigurtà tal-informazzjoni: Indirizzat bis-sħiħ permezz ta' programmi ta' taħriġ inizjali, ibbażati fuq ir-rwol u kontinwi mfassla skont il-profili ta' riskju tal-utenti.

11.2 ISO/IEC 27002:2022 – Kontroll 6

11.2.1 Tappoġġa l-iżvilupp u t-twassil ta' taħriġ ta' sensibilizzazzjoni xieraq għar-rwoli tax-xogħol, b'enfasi fuq it-tisħiħ ta' mġiba sigura u aġġornamenti perjodiċi abbażi ta' intelligence dwar it-theddid u feedback mill-awditjar.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 sa AT-5 (familja ta' kontrolli dwar is-sensibilizzazzjoni u t-taħriġ): Din il-politika hija allinjata ma' AT-1 (Politika u Proċeduri), AT-2 (Taħriġ ta' Sensibilizzazzjoni), AT-3 (Taħriġ Ibbażat fuq ir-Rwoli), AT-4 (Reġistri tat-Taħriġ fis-Sigurtà) u AT-5 (Kuntatt ma' Gruppi tas-Sigurtà).

11.3.2 IA-5, AC-2: Issaħħaħ ir-responsabbiltà tal-utent għal awtentikazzjoni sigura u użu aċċettabbli — elementi ewlenin għar-riżultati fl-imġiba tal-programmi ta' sensibilizzazzjoni.

11.3.3 IR-1 sa IR-8: It-tħejjija għar-rispons għall-inċidenti tissaħħaħ permezz ta' kampanji ta' sensibilizzazzjoni mmirati u simulazzjonijiet.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 32 – Sigurtà tal-ipproċessar: Jobbliga li l-persunal li jimmaniġġja data personali jkun imħarreġ biex jagħraf, jipprevjeni u jirrapporta riskji għall-informazzjoni personali. Din il-politika tiżgura li min jimmaniġġja d-data u r-rwoli rilevanti kollha jiġu mħarrġa kif xieraq.

11.4.2 Artikolu 39 – Kompiti tal-Uffiċjal tal-Protezzjoni tad-Data: Jinkludi ż-żieda tal-għarfien u t-taħriġ tal-persunal involut fl-operazzjonijiet tal-ipproċessar.

11.4.3 Premessa 78: Tinkoraġġixxi miżuri xierqa ta' sensibilizzazzjoni biex jiġi żgurat li jkun hemm prattiki robusti ta' sigurtà u konformità mal-politika.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(a, b): Jeħtieġ li l-entitajiet jadottaw politiki dwar l-analiżi tar-riskju u taħriġ fis-sigurtà għall-persunal rilevanti kollu. Din il-politika tissodisfa dan ir-rekwiżit billi tistabbilixxi proċessi ta' taħriġ kontinwi u sensittivi għar-rwol.

11.5.2 Artikolu 21(3): Jinkoraġġixxi l-promozzjoni tal-għarfien dwar ir-riskju taċ-ċibersigurtà fost il-maniġment u l-persunal permezz ta' inizjattivi ta' sensibilizzazzjoni u simulazzjonijiet.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 13 – Strateġija ta' Reżiljenza Operattiva Diġitali: Jobbliga li l-għarfien u t-taħriġ dwar ir-riskju tal-ICT ikunu parti mill-mudell ta' governanza. Din il-politika tiżgura li r-riskju uman jiġi indirizzat permezz ta' edukazzjoni kontinwa u simulazzjoni tat-theddid.

11.6.2 Artikoli 5 u 8: Jenfasizzaw l-importanza tal-oqfsa tal-kontroll intern, li fihom is-sensibilizzazzjoni u t-taħriġ huma komponenti fundamentali għar-reżiljenza tal-ICT u l-iġjene ċibernetika.

11.7 COBIT 2019

11.7.1 APO07 – Ġestjoni tar-Riżorsi Umani: Issaħħaħ il-ħtieġa li jiġi żviluppat l-għarfien dwar ir-responsabbiltajiet tas-sigurtà u li dan jiġi integrat fil-ġestjoni tal-forza tax-xogħol.

11.7.2 DSS05: Jistabbilixxi kontrolli fuq l-edukazzjoni tal-utenti u r-rappurtar tal-inċidenti, li t-tnejn huma integrali għal din il-politika.

11.7.3 MEA03 – Monitoraġġ, evalwazzjoni u valutazzjoni tal-konformità: Jitlob rieżami tal-effettività tal-imġiba tal-utenti u l-osservanza tal-politika — implimentat hawnhekk permezz ta' testijiet tal-phishing, kwiżżijiet u metriċi tal-kampanji ta' sensibilizzazzjoni.