					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P02					Titlu tad-dokument: **Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza**						
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**

Allinjament ma' standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 5.3; Kontroll 5 tal-Anness A	
ISO/IEC 27002:2022	Kontroll 5	
NIST SP 800-53 Rev.5	PL-1 sa PL-4, PM-1 sa PM-13	
GDPR tal-UE	Artikoli 5(1)(f), 24, 37	
Direttiva NIS2 tal-UE	Artikolu 21(2)(a)	
DORA tal-UE	Artikolu 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Għan

1.1 Din il-politika tiddefinixxi l-mudell ta' governanza, ir-rwoli organizzattivi u r-responsabbiltajiet meħtieġa għat-tħaddim ta' Sistema ta' Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS) effettiva.

1.2 Tistabbilixxi linji ċari ta' responsabbiltà, awtorità għat-teħid ta' deċiżjonijiet u mogħdijiet ta' eskalazzjoni sabiex tiżgura li s-sigurtà tal-informazzjoni tkun integrata fil-livelli kollha tal-organizzazzjoni u allinjata mal-objettivi strateġiċi tan-negozju.

1.3 Din il-politika timplimenta r-rekwiżiti tal-ISO/IEC 27001:2022 Klawżola 5.3 u Kontroll A.5.2, u tiżgura li r-responsabbiltajiet għal attivitajiet relatati mas-sigurtà jkunu assenjati b'mod ċar, dokumentati, ikkomunikati u rieżaminati perjodikament.

1.4 Din il-politika tipprovdi wkoll bażi għal governanza integrata ma' dixxiplini oħra bħall-ġestjoni tar-riskju, il-konformità, l-operazzjonijiet tal-IT u l-funzjoni legali.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għall-individwi u l-entitajiet kollha involuti fil-governanza, it-tħaddim u s-sorveljanza tas-sigurtà tal-informazzjoni fi ħdan il-kamp ta' applikazzjoni tal-ISMS. Dan jinkludi:

2.1.1 It-tmexxija eżekuttiva, il-maniġment superjuri u l-membri tal-bord

2.1.2 Il-maniġers tal-ISMS, is-CISO u s-sidien tal-kontrolli

2.1.3 Is-sidien tal-proċessi u tal-assi

2.1.4 Il-kuntratturi u l-forituri ta' servizzi ta' partijiet terzi b'responsabbiltajiet ta' sigurtà delegati

2.2 Tkopri kemm il-funzjonijiet interni kif ukoll dawk esternalizzati (eż. SOC esternalizzat, amministraturi ta' pjattaformi cloud) fejn ir-rwoli ta' governanza jkunu assenjati formalment jew definiti kuntrattwalment.

2.3 Il-politika tapplika wkoll għal unitajiet organizzattivi, dipartimenti u timijiet ta' proġett li jimmaniġġjaw jew jinfluwenzaw assi, sistemi jew servizzi rilevanti għas-sigurtà.

3. Objettivi

3.1 Jiġi żgurat li r-rwoli u r-responsabbiltajiet tas-sigurtà tal-informazzjoni jkunu definiti, assenjati, ikkomunikati u dokumentati formalment.

3.2 Jinżamm mudell ta' governanza li jiżgura s-separazzjoni tad-dmirijiet, jelimina kunflitti ta' interess u jippermetti l-eskalazzjoni ta' kwistjonijiet ta' sigurtà mhux solvuti.

3.3 Jiġi żgurat li r-responsabbiltà u l-awtorità għal deċiżjonijiet ta’ sigurtà jitqassmu b’mod allinjat mal-impatt fuq in-negozju u mal-istruttura organizzattiva.

3.4 Jiġi stabbilit qafas għall-ġestjoni tad-delegi, il-bidliet fir-rwoli u r-rieżami tar-responsabbiltajiet assenjati.

3.5 Tingħata assigurazzjoni lill-partijiet interessati, inklużi r-regolaturi, l-awdituri u l-klijenti, li s-sigurtà tal-informazzjoni hija gvernata b’mod effettiv u f’konformità mal-istandards applikabbli.

4. Rwoli u responsabbiltajiet

4.1 Il-Maniġment Eżekuttiv (Top Management)

4.1.1 Jipprovdi sorveljanza strateġika, jalloka r-riżorsi u jiżgura l-allinjament bejn l-objettivi tal-ISMS u l-għanijiet tan-negozju.

4.1.2 Japprova d-dokumentazzjoni ewlenija tal-ISMS, inkluża l-Politika tas-Sigurtà tal-Informazzjoni, il-pjanijiet ta’ trattament tar-riskju u d-deċiżjonijiet dwar ir-rimedjazzjoni tal-awditjar.

4.1.3 Jieħu sehem fir-rieżamijiet tal-maniġment tal-ISMS u jeskala deċiżjonijiet li jeħtieġu approvazzjoni fil-livell tal-Bord.

4.1.4 Jippromwovi kultura ta’ sigurtà u jsaħħaħ l-osservanza organizzattiva tal-prinċipji ta’ governanza tas-sigurtà.

4.2 Il-Kumitat ta’ Tmexxija tas-Sigurtà tal-Informazzjoni (ISSC)

4.2.1 Jaġixxi bħala l-korp ta’ governanza interfunzjonali għas-sorveljanza tal-ISMS.

4.2.2 Jagħmel rieżami tal-pożizzjoni tar-riskju, il-prestazzjoni tal-kontrolli, is-sejbiet tal-awditjar u l-inizjattivi strateġiċi tas-sigurtà.

4.2.3 Jiffaċilita l-koordinazzjoni bejn id-dipartimenti (eż. IT, Legali, HR, Riskju, Konformità, Operazzjonijiet).

4.2.4 Japprova limiti ta’ eskalazzjoni, allokazzjonijiet tal-baġit u bidliet fil-politika li jeħtieġu input eżekuttiv.

[... 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 Skeda ta’ rieżami

9.1.1 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena jew meta jseħħ xi wieħed minn dawn li ġejjin:

9.1.1.1 Bidliet fl-istruttura organizzattiva jew fit-tim eżekuttiv

9.1.1.2 Espansjoni jew ridefinizzjoni tal-kamp ta’ applikazzjoni tal-ISMS

9.1.1.3 Bidliet regolatorji li jaffettwaw l-assenjazzjoni tar-rwoli jew is-sorveljanza

9.1.1.4 Sejbiet sinifikanti tal-awditjar jew inċidenti li jinvolvu falliment tal-governanza

9.2 Proċess ta’ rieżami u approvazzjoni

9.2.1 Il-Maniġer tal-ISMS għandu jibda u jmexxi l-proċess ta’ rieżami, inkluż il-ġbir tal-input tal-partijiet interessati u r-rispons mill-awditjar.

9.2.2 L-aġġornamenti proposti għandhom jiġu rieżaminati mill-ISSC u approvati formalment mill-Maniġment Eżekuttiv.

9.2.3 Kull verżjoni għandha tiġi traċċata fir-Reġistru tad-Dokumenti tal-ISMS u tinkludi l-metadata li ġejja:

9.2.3.1 L-ID u t-titlu tal-politika

9.2.3.2 In-numru tal-verżjoni u sommarju tal-bidliet

9.2.3.3 Id-data tad-dħul fis-seħħ u d-data tar-rieżami li jmiss

9.2.3.4 Is-sid tal-politika u l-approvatur

9.2.3.5 Il-livell ta’ klassifikazzjoni tad-dokument

9.2.3.6 L-istorja taż-żamma u tal-arkivjar

10. Politiki relatati u rabtiet

10.1 Din il-politika għandha tinqara flimkien mal-politiki li ġejjin:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-programm ġenerali tas-sigurtà u tiddeskrivi r-responsabbiltajiet tat-tmexxija għall-approvazzjoni tal-politika u s-sorveljanza strateġika.

10.1.2 P5 – Politika tal-Ġestjoni tal-Bidla: Tiżgura li l-bidliet fl-istrutturi ta’ governanza, fir-rwoli jew fir-responsabbiltajiet ikunu soġġetti għal approvazzjoni dokumentata u rieżami tar-riskju.

10.1.3 P6 – Politika tal-Ġestjoni tar-Riskju: Tidentifika u tittratta riskji ta’ governanza li jirriżultaw minn kunflitti fir-rwoli, dmirijiet mhux assenjati jew nuqqas ta’ eskalazzjoni.

10.1.4 P7 – Politika tal-Onboarding u t-Terminazzjoni: Tiżgura l-proċessi ta’ assenjazzjoni u revoka tal-kontrolli waqt bidliet fiċ-ċiklu tal-ħajja tal-persunal.

10.1.5 P33 – Politika tal-Awditjar u l-Monitoraġġ tal-Konformità: Tappoġġja rieżami indipendenti tal-effettività tal-governanza u tiżgura azzjonijiet korrettivi għal nuqqas ta’ konformità.

10.2 Dawn il-politiki flimkien jappoġġjaw qafas ta’ governanza tal-ISMS unifikat u applikabbli.

11. Standards u oqfsa ta’ referenza

11.1 Din il-politika hija allinjata ma’ standards u oqfsa rikonoxxuti globalment għall-governanza tas-sigurtà tal-informazzjoni u r-responsabbiltà marbuta mar-rwoli. Tiżgura traċċabbiltà mar-rekwiżiti regolatorji u taċ-ċertifikazzjoni, u tappoġġja struttura tal-ISMS li tista’ tiġi difiża.

11.2 ISO/IEC 27001

11.2.1 Klawżola 5.3 – Rwoli, Responsabbiltajiet u Awtoritajiet Organizzattivi: Din il-politika tissodisfa r-rekwiżit li r-rwoli rilevanti għas-sigurtà tal-informazzjoni jkunu assenjati, ikkomunikati u dokumentati b’mod ċar.

11.2.2 Klawżola 9.3 – Rieżami tal-Maniġment: Din il-politika tiżgura s-sorveljanza eżekuttiva tar-rwoli tal-ISMS u tal-governanza permezz ta’ rieżamijiet trimestrali u annwali.

11.2.3 Kontroll 5.2 tal-Anness A – Rwoli u Responsabbiltajiet tas-Sigurtà tal-Informazzjoni: Tiddefinixxi rwoli fuq livelli tekniċi, operattivi u strateġiċi biex tiżgura s-separazzjoni tad-dmirijiet, is-sjieda tar-riskju u responsabbiltà traċċabbli.

11.3 ISO/IEC 27002:2022 – Kontroll 5

11.3.1 Jipprovdi gwida għall-implimentazzjoni tal-assenjazzjoni tar-responsabbiltajiet tas-sigurtà tal-informazzjoni madwar l-organizzazzjoni. Din il-politika tadotta dik il-gwida billi tiddefinixxi tipi ta’ rwoli, regoli ta’ delega, proċeduri ta’ eskalazzjoni u mekkaniżmi ta’ rieżami.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 sa PL-4: Jiżguraw il-ħtieġa għal dokumentazzjoni formali tal-ippjanar, inklużi politiki li jiddefinixxu l-governanza u jassenjaw ir-responsabbiltajiet tas-sigurtà.

11.4.2 PM-1 (Pjan tal-Programm tas-Sigurtà tal-Informazzjoni) u PM-2 (Uffiċjal Superjuri tas-Sigurtà tal-Informazzjoni): Riflessi f’din il-politika permezz tal-assenjazzjoni tas-CISO/Maniġer tal-ISMS u ta’ rwoli formali ta’ governanza.

11.4.3 PM-5 sa PM-13: Din il-politika tissodisfa r-rekwiżiti għad-dokumentazzjoni tar-rwoli, rwoli ta’ riskju fil-livell tal-intrapriża, sorveljanza tal-ġestjoni tal-konfigurazzjoni u integrazzjoni mal-funzjonijiet tal-missjoni/negozju.

11.5 GDPR tal-UE (2016/679)

11.5.1 Artikolu 5(1)(f): Jeħtieġ li d-data personali tiġi protetta kontra pproċessar mhux awtorizzat jew illegali. Din il-politika tiżgura li l-individwi responsabbli għall-protezzjoni tad-data jkunu ddeżinjati u mmonitorjati b'mod ċar.

11.5.2 Artikolu 24: Jeħtieġ miżuri organizzattivi xierqa, inklużi strutturi ta' governanza.

11.5.3 Artikolu 37: Jeħtieġ id-deżinjazzjoni ta' Uffiċjal tal-Protezzjoni tad-Data (DPO), li għandha tkun riflessa fil-qafas ta' governanza tal-organizzazzjoni u fir-reġistru tar-responsabbiltajiet.

11.6 Direttiva NIS2 tal-UE (2022/2555)

11.6.1 Artikolu 21(2)(a): Jobbliga lill-entitajiet jimplimentaw politiki dwar l-analiżi tar-riskju u s-sigurtà tas-sistemi tal-informazzjoni, inklużi responsabbiltajiet speċifiċi għar-rwoli. Din il-politika tiddefinixxi dawn ir-rwoli u l-mekkaniżmi ta' governanza tagħhom.

11.7 DORA tal-UE (2022/2554)

11.7.1 Artikolu 5 – Qafas ta' Governanza u Kontroll Intern: Jeħtieġ assenjazzjoni formali tar-responsabbiltajiet għall-ġestjoni tar-riskju tal-ICT, rwoli għat-teħid ta' deċiżjonijiet u kanali ta' rapportar. Din il-politika tipprovdi l-bażi għall-governanza ta' rwoli relatati mas-sigurtà f'ambjenti tal-ICT.

11.8 COBIT 2019

11.8.1 EDM01 – Ensured Governance Framework Setting: Din il-politika tiżgura li l-ISMS ikollha struttura ta' governanza definita b'mod ċar u allinjata mal-ħtiġijiet tal-intrapriża.

11.8.2 EDM02 – Ensured Benefits Delivery: Tallinja l-attivitajiet tas-sigurtà bbażati fuq ir-rwoli mal-objettivi strateġiċi u operattivi, u tiżgura responsabbiltà u riżultati li jistgħu jitkejlu.

11.8.3 APO01 – Managed I&T Management Framework u APO12 – Managed Risk: Din il-politika tappoġġja ġestjoni strutturata tar-rwoli tas-sigurtà tal-informazzjoni fi ħdan qafas usa' ta' governanza tal-IT u tar-riskju.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: Tintegra mekkaniżmi ta' rieżami biex jiġi vverifikat li r-rwoli ta' governanza huma effettivi, aġġornati u applikati.