					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P06S					Titlu tad-dokument: **Politika tal-Ġestjoni tar-Riskju**							
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 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 sa RA-7, PM-9	
Direttiva NIS2 tal-UE	Artikolu 21(2)(a–d)	
DORA tal-UE	Artikolu 5	
COBIT 2019	APO12, MEA01	

1. Skop

1.1 Din il-politika tiddefinixxi kif l-organizzazzjoni tidentifika, tevalwa u timmaniġġja r-riskji relatati mas-sigurtà tal-informazzjoni, mal-operazzjonijiet, mat-teknoloġija u mas-servizzi ta’ partijiet terzi.

1.2 Tiżgura li l-proċess tal-ġestjoni tar-riskju jkun parti integrali mill-ippjanar, mill-eżekuzzjoni tal-proġetti, mill-għażla tal-forniturі u mir-rispons għall-inċidenti, f’allinjament ma’ ISO 27001, ISO 31000 u mar-rekwiżiti regolatorji.

1.3 Il-politika tappoġġa teħid ta’ deċiżjonijiet informat, il-protezzjoni tal-assi tal-informazzjoni u r-reżiljenza tal-operazzjonijiet ewlenin tan-negozju.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Id-dipartimenti, is-sistemi u l-utenti kollha fl-organizzazzjoni.

2.1.2 L-informazzjoni, is-servizzi u l-assi kollha ġestiti internament jew permezz ta’ partijiet terzi.

2.1.3 Attivitajiet relatati mar-riskju, inklużi rieżamijiet tal-proġetti, titjib tas-sistemi, esternalizzazzjoni u konformità regolatorja.

2.2 Tkopri kull tip ta’ riskju, inkluż:

2.2.1 Theddid taċ-ċibersigurtà u vulnerabbiltajiet tas-sistemi.

2.2.2 Tfixkil operattiv u interruzzjoni tas-servizz.

2.2.3 Esponimenti legali, ta’ konformità jew reputazzjonali.

2.2.4 Riskji relatati ma’ partijiet terzi u mal-katina tal-provvista.

2.3 L-impjegati, il-kuntratturi u l-forniturі ta’ servizzi kollha għandhom isegwu din il-politika meta jidentifikaw jew jirrapportaw riskji.

3. Objettivi

3.1 Jiġu integrati proċeduri sempliċi u ripetibbli ta’ evalwazzjoni tar-riskju fl-operazzjonijiet normali tan-negozju.

3.2 Jiġu identifikati u prijoritizzati riskji li jistgħu jaffettwaw il-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) jew il-konformità legali.

3.3 Tiġi assenjata s-sjieda u jiġu definiti azzjonijiet ta’ rimedju għar-riskji sinifikanti kollha.

3.4 Jinżamm Reġistru tar-Riskji preċiż u aġġornat biex jappoġġa d-dimostrazzjoni tal-konformità għall-awditjar u t-traċċar tar-riskji.

3.5 Jiġi żgurat l-involviment tal-maniġment fl-approvazzjoni tat-tolleranza għar-riskju u tal-pjanijiet ewlenin ta’ trattament tar-riskju.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali

4.1.1 Jistabbilixxi l-aptit għar-riskju tal-organizzazzjoni u japprova l-qafas tal-ġestjoni tar-riskju.

4.1.2 Japprova deċiżjonijiet ewlenin dwar it-trattament tar-riskju u r-riżorsi meħtieġa.

4.1.3 Jirrevedi r-riskji ewlenin kull tliet xhur mal-Koordinatur tar-Riskju.

4.2 Koordinatur tar-Riskju (jew sid tal-ISMS)

4.2.1 Jiffaċilita evalwazzjonijiet tar-riskju u jżomm ir-Reġistru tar-Riskji.

4.2.2 Jiżgura li l-punteġġ tar-riskju, is-sjieda tar-riskju u l-azzjonijiet ta' rimedju jkunu dokumentati.

4.2.3 Jorganizza mill-inqas rieżami formali wieħed tar-riskju kull sena.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti ta' rieżami u aġġornament

9.1 Rieżami annwali tal-politika

9.1.1 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena mill-Maniġer Ġenerali u mill-Koordinatur tar-Riskju biex tiġi żgurata r-rilevanza u l-kompletezza tagħha.

9.2 Attivaturi għall-aġġornament

9.2.1 Għandu jsir rieżami u aġġornament qabel iż-żmien jekk:

9.2.1.1 Inċident ewlieni jew sejba tal-awditjar juri lakuni fil-ġestjoni tar-riskju.

9.2.1.2 Jiġu introdotti unitajiet ġodda tan-negozju, teknoloġiji jew sħubijiet.

9.2.1.3 Jinbidel rekwiżit regolatorju jew kuntrattwali.

9.3 Kontroll tal-verżjoni

9.3.1 L-aġġornamenti kollha għal din il-politika għandhom jiġu verżjonati bil-metadata li ġejja:

9.3.1.1 Numru tal-verżjoni u data tad-dħul fis-seħħ.

9.3.1.2 Sommarju tal-bidliet.

9.3.1.3 Approvatur (Maniġer Ġenerali).

9.3.1.4 Verżjonijiet preċedenti arkivjati għal finijiet ta' awditjar.

9.4 Komunikazzjoni u sensibilizzazzjoni

9.4.1 Verżjonijiet aġġornati tal-politika u pjanijiet ewlenin ta' trattament għandhom jiġu kkomunikati lill-persunal affettwat. It-taħriġ annwali ta' sensibilizzazzjoni għandu jinkludi prinċipji bażiċi ta' għarfien tar-riskju.

10. Politiki relatati u rabtiet

10.1 Din il-politika taħdem f'koordinazzjoni ma' diversi oħrajn biex tiżgura governanza komprensiva tas-sigurtà:

10.1.1 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiddefinixxi min huwa responsabbli għas-sjieda tar-riskju u għat-teħid ta' deċiżjonijiet.

10.1.2 P5S – Politika tal-Ġestjoni tat-Tibdil: Teħtieġ evalwazzjoni tar-riskju qabel ma jiġu implimentati bidliet tekniċi jew ta' proċess.

10.1.3 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tindirizza riskju regolatorju assoċjat mal-ġestjoni tad-data personali.

10.1.4 P30S – Politika ta' Rispons għall-Inċidenti: Tiżgura li t-trattament tar-riskju jkompli matul u wara inċidenti tas-sigurtà.

10.1.5 P33S – Politika tal-Kontinwità tan-Negozju: Tidentifika espożizzjoni residwa u miżuri ta' rkupru għal servizzi kritiċi.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:

11.1.1 Klawżola 6.1 – Tistabbilixxi proċess formali tal-ġestjoni tar-riskju u l-ippjanar tat-trattament.

11.1.2 Klawżola 6.1.3 – Teħtieġ li l-organizzazzjonijiet iżommu pjanijiet ta' trattament u approvazzjonijiet dokumentati.

11.2 ISO/IEC 27002:

11.2.1 Kontrolli 5.4, 5.25 – Jipprovdu gwida għall-implimentazzjoni dwar is-sjieda tar-riskju, il-prijoritizzazzjoni u l-ġestjoni taċ-ċiklu tal-ħajja tal-politiki.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 sa RA-7 – Jiddefinixxu evalwazzjoni tar-riskju, strateġiji ta' rispons, dokumentazzjoni u mekkaniżmi ta' rieżami.

11.4 PM-9 – Jeħtieġ sorveljanza konsistenti fil-livell tal-maniġment tar-riskji organizzattivi.

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(a–d) – Jobbliga evalwazzjoni tar-riskju, mitigazzjoni u kontrolli ta' governanza obbligatorji għal entitajiet essenzjali u importanti.

11.6 DORA tal-UE

11.6.1 Artikolu 5 – Jeħtieġ li entitajiet regolati jiddefinixxu u jimmaniġġjaw oqfsa tal-ġestjoni tar-riskju tal-ICT, inklużi l-identifikazzjoni, il-klassifikazzjoni u r-rispons.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: Jintegra r-riskju fl-ippjanar strateġiku u operattiv.

11.7.2 MEA01 – Monitor, Evaluate, and Assess: Jiżgura l-effettività u l-konformità tal-proċessi u tal-azzjonijiet relatati mar-riskju.