					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P37					Titlu tad-dokument: **Politika dwar il-Konformità Legali u Regolatorja**							
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**

1. Għan

1.1 Din il-politika tistabbilixxi l-qafas obbligatorju għall-identifikazzjoni, il-ġestjoni u l-konformità mal-obbligi legali, regolatorji u kuntrattwali kollha rilevanti għas-sigurtà tal-informazzjoni, il-privatezza tad-data u l-funzjonijiet operattivi tal-organizzazzjoni.

1.2 L-għan huwa li jiġi evitat nuqqas ta' konformità li jista' jwassal għal multi, responsabbiltà legali, tfixkil fin-negozju, ħsara reputazzjonali jew infurzar regolatorju.

1.3 Din il-politika tappoġġa l-integrazzjoni tal-obbligi ta' konformità fil-governanza, fil-proċessi tal-ġestjoni tar-riskju, fil-flussi tax-xogħol operattivi, fiċ-ċikli tal-ħajja tal-proġetti u fid-disinn tas-sistemi.

1.4 Tiżgura li l-obbligi rilevanti kollha—f'ġurisdizzjonijiet, setturi industrijali u oqsma regolatorji differenti—ikunu dokumentati, evalwati, immonitorjati u applikati b'mod ċar fi ħdan l-organizzazzjoni.

2. Kamp ta' applikazzjoni

2.1 Din il-politika tapplika għad-dipartimenti, il-funzjonijiet, l-unitajiet tan-negozju u l-individwi kollha li jaġixxu f'isem l-organizzazzjoni, inklużi:

2.1.1 Impjegati permanenti u temporanji

2.1.2 Kuntratturi, konsulenti u interns

2.1.3 Fornituri terzi, proċessuri jew sħab li jimmaniġġjaw id-data, is-sistemi jew ir-responsabbiltajiet regolatorji tal-organizzazzjoni

2.1.4 Kwalunkwe proċess tan-negozju, proġett jew inizjattiva suġġett għal kontroll legali jew regolatorju

2.2 L-oqsma ta' konformità koperti minn din il-politika jinkludu, iżda mhumiex limitati għal:

2.2.1 Obbligi ta' sigurtà tal-informazzjoni u taċ-ċibersigurtà (eż. ISO/IEC 27001, NIS2, DORA)

2.2.2 Leġiżlazzjoni dwar il-protezzjoni tad-data u l-privatezza (eż. GDPR, liġijiet speċifiċi għas-settur dwar il-privatezza)

2.2.3 Regolamenti settorjali (eż. finanzjarji, mediċi, tal-karozzi, tad-difiża)

2.2.4 Obbligi kuntrattwali li jirriżultaw minn Ftehimiet ta' Nuqqas ta' Żvelar, Ftehimiet dwar il-Livell tas-Servizz (SLAs) jew ftehimiet ma' partijiet terzi dwar l-ipproċessar

2.2.5 Rekwiżiti legali relatati mar-rappurtar tal-inċidenti, l-interazzjoni mal-infurzar tal-liġi u t-trasferiment internazzjonali tad-data

3. Objettivi

3.1 Tiżgura li l-liġijiet, ir-regolamenti, l-istandards u l-obbligi kuntrattwali kollha applikabbli jiġu identifikati, dokumentati, interpretati u applikati fl-organizzazzjoni kollha.

3.2 Tintegra r-rekwiżiti legali u regolatorji fl-ISMS tal-organizzazzjoni, fil-proċess tal-ġestjoni tar-riskju, fil-kuntratti tal-fornituri u fid-disinn tal-prodotti u s-servizzi.

3.3 Tipprovdi mekkaniżmu għall-monitoraġġ proattiv tat-tibdil regolatorju u għall-aġġornament tal-kontrolli u d-dokumentazzjoni kif meħtieġ.

3.4 Tiddefinixxi responsabbiltà ċara għas-sorveljanza tal-konformità, l-eskalazzjoni tal-ksur, il-ġestjoni tal-eċċezzjonijiet u r-rappurtar estern.

3.5 Tiżgura l-awditabbiltà u d-difensibbiltà tal-pożizzjoni legali u regolatorja tal-organizzazzjoni waqt spezzjonijiet, investigazzjonijiet jew rieżamijiet ta' ċertifikazzjoni.

4. Rwoli u responsabbiltajiet

4.1 Il-Maniġment Eżekuttiv

4.1.1 Iġorr ir-responsabbiltà strateġika għall-allinjament legali u regolatorju fl-organizzazzjoni kollha.

4.1.2 Jirrieżamina u japprova deċiżjonijiet ta’ konformità b’riskju għoli, inklużi l-aċċettazzjoni tar-riskju u tilwim legali.

4.2 L-Uffiċjal tal-Konformità / il-Konsulent Ġenerali / il-Konsulent Legali

4.2.1 Iżomm Reġistru tal-Obbligi ta’ Konformità li jelenka l-liġijiet, l-istandards, iċ-ċertifikazzjonijiet u l-klawżoli kuntrattwali kollha applikabbli.

4.2.2 Jagħmel valutazzjonijiet tal-impatt legali għal servizzi, swieq jew flussi tad-data ġodda.

4.2.3 Jipprovdi interpretazzjoni awtorevoli tal-liġijiet u l-istandards.

[... 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

9.1.1 Din il-politika għandha tiġi rieżaminata mill-inqas darba kull sena kalendarja biex:

9.1.1.1 Tiżgura allinjament kontinwu ma’ liġijiet aġġornati, standards tal-industrija u oqfsa regolatorji

9.1.1.2 Tivverifika l-effettività operattiva abbażi tas-sejbiet tal-awditjar u l-istorja tal-inċidenti

9.1.1.3 Tirrifletti bidliet organizzattivi (eż. ġurisdizzjonijiet, sistemi jew linji tan-negozju ġodda)

9.2 Rieżamijiet ibbażati fuq attivaturi

9.2.1 Għandhom jinbdew rieżamijiet interim meta:

9.2.2 Jiġi adottat jew aġġornat rekwiżit legali jew regolatorju ġdid

9.2.3 Inċident ta’ konformità jew awditu juri nuqqasijiet fil-politika

9.2.4 L-organizzazzjoni tidħol f’suq jew linja ta’ servizz ġdida regolata minn oqfsa ta’ konformità distinti

9.2.5 Xejriet ta’ infurzar regolatorju jew gwida mir-regolaturi jindikaw bidliet fil-pożizzjoni tar-riskju

9.3 Sjieda u approvazzjoni

9.3.1 Id-Dipartiment Legali u l-Uffiċjal tal-Konformità huma responsabbli b’mod konġunt għall-koordinazzjoni tal-proċess ta’ rieżami.

9.3.2 Ir-reviżjonijiet finali tal-politika għandhom jiġu approvati mill-Maniġment Eżekuttiv u rreġistrati fir-Reġistru tal-Bidliet fil-Politiki, b’referenzi relatati għall-kontroll tat-tibdil u pjanijiet ta’ komunikazzjoni.

9.4 Kontroll tal-verżjoni u komunikazzjoni

9.4.1 Kull verżjoni aġġornata ta’ din il-politika għandha:

9.4.1.1 Tinkludi sommarju tal-bidliet ewlenin

9.4.1.2 Tinqasam mill-ġdid permezz ta’ kanali uffiċjali (eż. portal tal-politiki, LMS, bullettini interni)

9.4.1.3 Teħtieġ rikonoxximent mill-persunal affettwat, b’mod partikolari dawk f’rwoli legali, operattivi, ta’ sigurtà u ta’ ġestjoni tal-forniturі

10. Politiki relatati u rabtiet

10.1 Din il-politika topera flimkien ma’ u ssaħħaħ il-politiki li ġejjin fi ħdan l-ISMS tal-organizzazzjoni:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-prinċipji bażiċi ta’ governanza li jiżguraw li l-politiki kollha tas-sigurtà tal-informazzjoni—inkluża l-konformità—ikunu allinjati mar-rekwiżiti strateġiċi tan-negozju u dawk regolatorji.

10.1.2 P2 – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiddefinixxi l-awtoritajiet għat-teħid tad-deċiżjonijiet, inklużi r-rwoli legali u tal-konformità responsabbli għas-sorveljanza regolatorja u r-responsabbiltà.

10.1.3 P6 – Politika tal-Ġestjoni tar-Riskju: Tappoġġa l-valutazzjoni, is-sjieda u l-mitigazzjoni tar-riskji ta' konformità legali u regolatorja fl-organizzazzjoni kollha.

10.1.4 P8 – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-persunal kollu jkun infurmat dwar ir-responsabbiltajiet ta' konformità u jirċievi taħriġ xieraq għar-rwol tiegħu.

10.1.5 P12 – Politika tal-Ġestjoni tal-Assi: Issaħħaħ l-obbligi legali għall-ġestjoni u l-protezzjoni ta' assi regolati jew kuntrattwali, inklużi dawk li jinvolvu data personali u infrastruttura kritika.

10.1.6 P30 – Politika dwar ir-Rispons għall-Inċidenti: Tirregola notifiki legali obbligatorji (eż. Artikolu 33 tal-GDPR) u proċeduri ta' eskalazzjoni f'każ ta' ksur ta' konformità jew avveniment regolatorju.

10.1.7 P33 – Politika dwar il-Monitoraġġ tal-Awditjar u l-Konformità: Tipprovdi attivitajiet strutturati ta' assigurazzjoni—inklużi ttestjar tal-kontrolli u l-ġbir tal-evidenza—meħtieġa għall-verifika interna u esterna tal-konformità.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 4.2 – Fehim tal-Ħtiġijiet u l-Aspettattivi tal-Partijiet Interessati: Teħtieġ l-identifikazzjoni u l-integrazzjoni tar-rekwiżiti legali u regolatorji fl-ISMS.

11.1.2 Klawżola 5.1 – Tmexxija u Impenn: Tobbliga responsabbiltà eżekuttiva għall-istabbiliment u ż-żamma tal-konformità legali fl-organizzazzjoni kollha.

11.1.3 Klawżola 5.3 – Rwoli, Responsabbiltajiet u Awtoritajiet Organizzattivi: Tiżgura ċarezza fir-rwoli għas-sorveljanza legali u l-konformità regolatorja.

11.1.4 Kontroll 5.36 tal-Anness A – Konformità mar-Rekwiżiti Legali u Kuntrattwali: Jistabbilixxi r-rekwiżit li jiġu identifikati u ssodisfati l-obbligi li jirriżultaw minn liġijiet, regolamenti u kuntratti.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.36: Jagħti gwida għall-implimentazzjoni taż-żamma ta' reġistru tal-obbligi ta' konformità, il-verifika tar-rekwiżiti regolatorji u l-iżgurar ta' żamma strutturata tal-evidenza.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika u Proċeduri tal-Ippjanar tas-Sigurtà: Jeħtieġ li l-obbligi ta' konformità jiġu integrati fl-istrutturi ta' governanza u fid-dokumentazzjoni.

11.3.2 PM-1 – Pjan tal-Programm tas-Sigurtà tal-Informazzjoni: Jobbliga kontrolli regolatorji bħala komponent tal-programm usa' tas-sigurtà.

11.3.3 CA-7 – Monitoraġġ Kontinwu: Jappoġġa s-sorveljanza tal-effettività tal-kontrolli fit-twettiq tar-rekwiżiti legali u tal-politika.

11.3.4 AU-9 – Protezzjoni tal-Informazzjoni tal-Awditjar: Jiżgura li logs u reġistri tal-awditjar tal-konformità jkunu protetti u disponibbli għall-ispezzjoni.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 5 – Prinċipji Relatati mal-Ipproċessar: Jeħtieġ ipproċessar legali, trasparenza u responsabbiltà.

11.4.2 Artikolu 6 – Legalità tal-Ipproċessar: Jobbliga bażijiet legali xierqa għall-attivitajiet kollha relatati mad-data.

11.4.3 Artikolu 24 – Responsabbiltà tal-Kontrollur: Jistabbilixxi responsabbiltà diretta biex tiġi żgurata l-konformità regolatorja.

11.4.4 Artikolu 32 – Sigurtà tal-Ipproċessar: Jeżiġi l-implimentazzjoni ta' miżuri tekniċi u organizzattivi (TOMs) xierqa.

11.4.5 Artikolu 33 – Notifika ta’ Ksur: Jeħtieġ li ksur ta’ data personali jiġu rrappurtati lill-awtoritajiet rilevanti fi żmien 72 siegħa.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikoli 20–21: Jeħtieġu li entitajiet essenzjali u importanti jimplimentaw governanza dokumentata, strateġiji ta’ konformità legali u rieżami kontinwu tar-riskji legali.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 5(2) – Qafas tal-Ġestjoni tar-Riskju tal-ICT: Jeħtieġ l-integrazzjoni tal-konformità legali fi ħdan il-funzjonijiet usa’ tal-ġestjoni tar-riskju u s-sorveljanza.

11.6.2 Artikolu 19 – Riskju tal-ICT ta’ Partijiet Terzi: Jimponi rekwiżiti legali speċifiċi għall-ġestjoni tal-obbligi kuntrattwali u regolatorji li jinvolvu fornituri esterni u pjattaformi.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: Jinkorpora l-konformità legali u regolatorja bħala komponent kritiku tal-governanza tar-riskju tal-organizzazzjoni.

11.7.2 MEA03 – Monitor Compliance with External Requirements: Jiddefinixxi monitoraġġ kontinwu, ġestjoni tal-eċċezzjonijiet u l-kapaċità li tintwera l-konformità għall-forom kollha ta’ obbligi regolatorji.