					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P15					Titlu tad-dokument: **Politika dwar il-Backup u r-Restawr**							
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 6.1.3, 8.1	Trattament tar-riskju, ippjanar u kontrolli operattivi tal-backup
ISO/IEC 27002:2022	Kontrolli 8.13, 5.28, 5.29	Ġestjoni tal-backup, rimi sigur u reżiljenza
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Rekwiżiti għall-backup tas-sistema, l-irkupru u s-sanitizzazzjoni tal-mezzi
GDPR tal-UE	Artikolu 32, Premessa 49	Restawr u disponibbiltà tad-data personali, kontinwità tan-negozju
Direttiva NIS2 tal-UE	Artikolu 21(2)(c-e)	Kontrolli tal-backup u tal-kontinwità għar-reżiljenza
DORA tal-UE	Artikoli 10, 11	Rekwiżiti għas-settur finanzjarju dwar backup, irkupru u ttestjar
COBIT 2019	DSS01, DSS04, MEA03	Operazzjonijiet tal-backup, kontinwità u monitoraġġ tal-konformità

1. Għan

1.1 L-għan ta’ din il-politika huwa li tiddefinixxi r-rekwiżiti obbligatorji għall-backup u r-restawr tad-data, tas-sistemi u tal-applikazzjonijiet biex tappoġġa r-reżiljenza operattiva, l-integrità tad-data u l-kontinwità tan-negozju.

1.2 Il-politika tistabbilixxi qafas standardizzat biex:

1.2.1 Tipproteġi d-data tal-organizzazzjoni minn telf minħabba tħassir, korruzzjoni, ħsara, jew attakki ċibernetiċi

1.2.2 Tiddefinixxi l-aspettattivi tal-irkupru permezz ta’ parametri ċari ta’ RTO (Recovery Time Objective) u RPO (Recovery Point Objective)

1.2.3 Tintegra l-operazzjonijiet tal-backup mal-ISMS usa’ u mal-Pjanijiet ta’ Kontinwità tan-Negozju (BCP/DRP)

1.2.4 Tiżgura l-konformità mal-liġijiet applikabbli u mar-regolamenti settorjali dwar id-disponibbiltà u l-irkuprabbiltà

1.3 Il-politika tagħti effett lill-kontrolli ta’ ISO/IEC 27001:2022 relatati mar-rimi sigur tad-data (5.28), ir-reżiljenza (5.29) u l-irkupru operattiv (8.13), u torbot mal-aħjar prattiki ta’ ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA u NIS2.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Is-sistemi kollha kritiċi għan-negozju u s-sistemi operattivi fi ħdan il-kamp ta’ applikazzjoni tal-ISMS

2.1.2 Id-data kollha strutturata u mhux strutturata tan-negozju, inklużi databases, fajls, emails u konfigurazzjonijiet

2.1.3 L-ambjenti kollha — fuq il-post, cloud, ibridi u ħażna remota/barra mis-sit

2.1.4 Il-persunal kollu responsabbli mill-ġestjoni, l-eżekuzzjoni, il-verifika jew ir-restawr tal-proċessi tal-backup

2.2 Tapplika wkoll għal:

2.2.1 Il-mezzi u l-infrastruttura tal-backup, inklużi tejps fiżiċi, appliances virtwali, snapshots tad-diska u soluzzjonijiet ta' backup f'ambjent cloud

2.2.2 Fornituri ta' servizzi ta' partijiet terzi kkuntrattati biex jospitaw, jimmaniġġjaw jew jipproċessaw backups tal-organizzazzjoni

2.2.3 Backup ta' logs, konfigurazzjonijiet, traċċi ta' awditjar u dokumentazzjoni operattiva kritika għall-kontinwità

2.3 Sistemi espliċitament esklużi mill-backup għandhom ikunu dokumentati, soġġetti għal valutazzjonijiet tar-riskju, u aċċettati formalment mill-Maniġer tal-ISMS u mis-Sid tas-Sistema.

3. Objettivi

3.1 Jiġi żgurat li s-sistemi u d-data kritiċi kollha jkollhom backup affidabbli bi frekwenza, ridondanza u kontrolli tas-sigurtà suffiċjenti.

3.2 Jiġu pprovduti mekkaniżmi ta' restawr li jilħqu l-aspettattivi ddefiniti ta' RTO u RPO f'allinjament mal-Valutazzjonijiet tal-Impatt fuq in-Negozju.

3.3 Tinżamm dokumentazzjoni sħiħa tal-proċeduri tal-backup, l-iskedi taż-żamma, ir-rwoli u t-teknoloġiji.

3.4 Tiġi vverifikata l-effettività tal-kontrolli tal-operazzjonijiet tal-backup permezz ta' testijiet sistemiċi ta' restawr, logging tal-fallimenti u traċċar tal-azzjonijiet ta' rimedju.

3.5 Id-data tal-backup tiġi protetta minn aċċess mhux awtorizzat, modifika jew qerda matul iċ-ċiklu kollu tal-ħajja tagħha.

3.6 Tippermetti l-konformità ma':

3.6.1 Rekwiżiti ta' kontroll operattiv u ta' kontinwità ta' ISO/IEC 27001

3.6.2 Il-familji CP u MP ta' NIST SP 800-53 għal backup u sanitizzazzjoni

3.6.3 L-Artikolu 32 u l-Premessa 49 tal-GDPR għar-restawr tal-aċċess għad-data personali

3.6.4 L-Artikolu 10 ta' DORA u l-Artikolu 21 ta' NIS2 għall-kontinwità u r-reżiljenza tal-ICT

3.7 Jiġi żgurat li s-servizzi ta' backup ipprovduti minn partijiet terzi jissodisfaw obbligi kuntrattwali u regolatorji tas-sigurtà, inklużi protokolli ta' iċċifrar, rimi u notifika.

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Japprova din il-politika u jiżgura li s-sistemi kritiċi għan-negozju jkunu protetti b'mod adegwat permezz ta' prattiki approvati ta' backup u restawr.

4.1.2 Iġorr ir-responsabbiltà li jiżgura li l-operazzjonijiet tal-backup ikollhom riżorsi adegwati u jkunu soġġetti għal rieżami perjodiku għall-konformità regolatorja.

4.2 Uffiċjal Kap tas-Sigurtà tal-Informazzjoni (CISO)

4.2.1 Huwa s-sid ta' din il-politika u jiżgura l-allinjament mal-oqfsa usa' tas-sigurtà tal-informazzjoni, tar-riskju u tal-kontinwità.

4.2.2 Jissorvelja l-integrazzjoni tal-proċeduri tal-backup fil-BCP/DRP, fir-rispons għall-inċidenti u fl-ippjanar tar-reżiljenza.

4.2.3 Jagħmel rieżami tal-eċċezzjonijiet tal-backup u jevalwa proposti ta' aċċettazzjoni tar-riskju għal esklużjonijiet ta' sistemi kritiċi.

[... 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 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena, jew qabel jekk jiġi attivat rieżami minħabba:

9.1.1 Bidliet fl-istrateġija tal-kontinwità tan-negozju jew tal-irkupru minn diżastri

9.1.2 Obbligi regolatorji jew legali ġodda li jaffettwaw il-frekwenza tal-backup jew iż-żamma tad-data

9.1.3 Bidliet fl-arkitettura tas-sistema, fl-għodod tal-backup jew fil-fornituri tas-servizzi

9.1.4 Inċidenti sinifikanti jew sejbiet tal-awditjar relatati ma' telf ta' data jew fallimenti tal-irkupru

9.2 Ir-rieżami għandu jiġi kkoordinat mis-CISO b'kollaborazzjoni ma':

9.2.1 Infrastruttura tal-IT u Operazzjonijiet

9.2.2 Awditjar Intern

9.2.3 Uffiċjal tal-Protezzjoni tad-Data (DPO)

9.2.4 Timijiet tal-Kontinwità tan-Negozju u tal-Irkupru minn Diżastri

9.3 L-iskedi tal-backup, il-listi ta' inklużjoni tas-sistemi, id-dokumentazzjoni tar-restawr u r-reġistri tal-eċċezzjonijiet għandhom jiġu rieżaminati b'mod parallel biex jiġi żgurat:

9.3.1 L-eżattezza tal-kopertura tal-backup għall-assi kritiċi kollha

9.3.2 Il-konformità mar-rekwiżiti ta' RTO/RPO u taż-żamma

9.3.3 Il-kompletezza tal-logs tat-testijiet u r-rapporti tal-inċidenti

9.3.4 Il-korrezzjoni ta' lakuni sistemiċi fil-kontrolli identifikati qabel

9.4 L-aġġornamenti kollha għandhom:

9.4.1 Ikunu taħt kontroll tal-verżjoni u miżmuma fir-Repożitorju tad-Dokumenti tal-ISMS

9.4.2 Jinkludu sommarju tal-bidliet u l-ġustifikazzjoni tagħhom

9.4.3 Ikunu approvati mill-Maniġment Eżekuttiv

9.4.4 Jiġu kkomunikati lill-persunal tekniku u tan-negozju kollu affettwat

10. Politiki relatati u rabtiet

10.1 Din il-politika tappoġġa direttament u tinteraġixxi mad-dokumenti relatati li ġejjin:

10.1.1 P6 - Politika tal-Ġestjoni tar-Riskju: Tidentifika l-prijoritizzazzjoni bbażata fuq ir-riskju tal-protezzjoni tal-backup għas-sistemi u s-servizzi.

10.1.2 P12 - Politika tal-Ġestjoni tal-Assi: Tiżgura li s-sistemi eliġibbli għall-backup ikunu inklużi fl-inventarju u marbuta mat-traċċar taċ-ċiklu tal-ħajja u mal-klassifikazzjoni.

10.1.3 P13 - Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data: Tiggwida liema kategoriji ta' data jeħtieġu backup, inkluż metadata tat-tikkettar għall-prijoritizzazzjoni.

10.1.4 P14 - Politika taż-Żamma u r-Rimi tad-Data: Tikkoordina ż-żamma tal-backup mal-limiti regolatorji taż-żamma u mar-rimi xieraq ta' mezzi skaduti.

10.1.5 P16 - Politika dwar il-Masking tad-Data u l-Psewdonimizzazzjoni: Tappoġġa l-minimizzazzjoni tad-data waqt il-backup ta' settijiet ta' data sensittivi.

10.1.6 P30 - Politika dwar ir-Rispons għall-Inċidenti: Tiġi attivata waqt fallimenti tal-backup, problemi ta' restawr jew kompromess ta' repożitorji tad-data tal-backup.

10.2 Dawn il-politiki interkonnessi jiffurmaw qafas koerenti li jiżgura li l-governanza tal-backup tkun integrata fl-ISMS usa' tal-organizzazzjoni u fl-istrateġija tagħha għar-reżiljenza operattiva.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:

11.1.1 Klawżola 6.1.3 - Pjan ta' Trattament tar-Riskju: Tappoġġa l-prijoritizzazzjoni tal-backup ibbażata fuq ir-riskju u l-ippjanar tar-restawr.

11.1.2 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Tintegra kontrolli ta' rkupru u ta' kontinwità bħala parti mis-salvagwardji operattivi.

11.1.3 Kontroll 5.28 tal-Anness A - Rimi jew Użu mill-Ġdid ta' Tagħmir b'mod Sigur: Jindirizza s-sanitizzazzjoni sigura ta' mezzi tal-backup.

11.1.4 Kontroll 5.29 tal-Anness A - Sigurtà tal-Informazzjoni waqt Tfixkil: Jiżgura kapaċitajiet ta' restawr waqt inċidenti jew diżastri.

11.1.5 Kontroll 8.13 tal-Anness A - Backup tal-Informazzjoni: Jiġi implimentat direttament permezz ta' operazzjonijiet ta' backup skedati, ittestjati u siguri.

11.2 ISO/IEC 27002:2022 - Kontrolli 8.13, 5.28, 5.29: Dawn il-kontrolli jsaħħu r-rekwiżit għal backups regolari, verifika tal-integrità u ppjanar tar-restawr fl-ambjenti kollha tal-IT.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Backup tas-Sistema: Jistabbilixxi proċeduri komprensivi ta' backup, inklużi ħażna barra mis-sit u ttestjar tar-restawr.

11.3.2 CP-10 - Irkupru u Restawr tas-Sistema: Jeħtieġ proċeduri vverifikati għal restawr sħiħ jew parzjali allinjat mal-objettivi ta' rkupru.

11.3.3 MP-6 - Sanitizzazzjoni tal-Mezzi: Tiżgura l-immaniġġjar sigur ta' mezzi tal-backup skaduti.

11.3.4 SI-12 - Proċeduri għall-Immaniġġjar tal-Informazzjoni: Isaħħaħ ir-responsabbiltajiet ta' backup u rkupru għal data sensittiva.

11.4 GDPR tal-UE (2016/679):

11.4.1 Artikolu 32 - Sigurtà tal-Ipproċessar: Jobbliga kapaċitajiet ta' restawr u salvagwardji għad-disponibbiltà tad-data, b'mod partikolari għal data personali.

11.4.2 Premessa 49: Tappoġġa miżuri ta' kontinwità tan-negozju u ta' rkupru minn diżastri, inkluż backup sigur bħala parti mir-reżiljenza tal-organizzazzjoni.

11.5 Direttiva NIS2 tal-UE (2022/2555):

11.5.1 Artikolu 21(2)(c-e): Jeħtieġ miżuri tekniċi u organizzattivi, inklużi kontrolli tal-backup u tal-kontinwità, biex tiġi żgurata r-reżiljenza tas-servizzi.

11.6 DORA tal-UE (2022/2554):

11.6.1 Artikolu 10 - Kontinwità tan-Negozju tal-ICT: Jeħtieġ li entitajiet finanzjarji jkollhom backup sħiħ tad-data, irkupru u ppjanar tal-kontinwità.

11.6.2 Artikolu 11 - Ittestjar tal-Pjanijiet ta' Kontinwità tan-Negozju tal-ICT: Jenfasizza l-verifika tal-kapaċità ta' rkupru permezz ta' ttestjar regolari.

11.7 COBIT 2019:

11.7.1 DSS01 - Operazzjonijiet Immaniġġjati: Jappoġġa l-għoti affidabbli tas-servizzi permezz ta' disponibbiltà protetta tad-data.

11.7.2 DSS04 - Kontinwità Immaniġġjata: Jiddefinixxi kontrolli strateġiċi u operattivi tal-kontinwità, inklużi backups verifikati.

11.7.3 MEA03 - Immonitorja, Evalwa u Ivvaluta l-Konformità: Jobbliga rieżami perjodiku tal-miżuri ta' kontinwità, inkluża l-effettività tal-kontrolli tal-backup.