					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P15S					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	Klawżola 8	Kontrolli tal-backup skont ir-rekwiżiti tal-ISMS
ISO/IEC 27002:2022	Kontrolli 5.29, 8	Prattiki tajbin għall-backup, integrazzjoni mal-kontinwità tan-negozju
NIST SP 800-53 Rev.5	CP-9, MP-6	Backup u protezzjoni tal-mezzi
Direttiva NIS2 tal-UE	Artikolu 21(2)(c)	Reżiljenza u kontinwità permezz tal-backup
DORA tal-UE	Artikolu 10(1)	Kontinwità tal-ICT - backup għal organizzazzjonijiet finanzjarji
COBIT 2019	BAI04.05, DSS04	Iddokumentar u ttestjar tal-backups, kontroll fuq il-proċessi
GDPR tal-UE	Artikoli 5(1)(f), 32(1)(c)	Integrità, disponibbiltà u restawr f’waqtu tad-data

1. Għan

1.1 Din il-politika tiddefinixxi kif l-organizzazzjoni twettaq u timmaniġġja l-backups sabiex tiżgura l-kontinwità tan-negozju, tipproteġi kontra t-telf ta’ data u tippermetti rkupru f’waqtu wara inċidenti.

1.2 Hija tistabbilixxi regoli vinkolanti dwar kif is-sistemi u d-data għandhom jiġu kkupjati, maħżuna u rrestawrati, b’mod partikolari f’SMEs mingħajr infrastruttura tal-IT kumplessa.

1.3 Din il-politika tappoġġa l-istat ta’ tħejjija tal-organizzazzjoni għall-awditjar u ċ-ċertifikazzjoni ISO/IEC 27001 billi tiżgura li l-kontrolli essenzjali tal-backup ikunu fis-seħħ, applikati b’mod konsistenti u rieżaminati regolarment.

1.4 Il-kapaċità tal-organizzazzjoni li tirkupra minn fallimenti tekniċi, tħassir aċċidentali jew inċidenti ċibernetiċi tiddependi fuq il-konformità stretta ma’ din il-politika.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għas-sistemi tan-negozju u għad-data kollha, inklużi:

2.1.1 rekords finanzjarji, informazzjoni tal-klijenti u data tar-Riżorsi Umani

2.1.2 desktops, laptops, servers u applikazzjonijiet cloud użati fl-operazzjonijiet tan-negozju

2.1.3 mezzi tal-backup bħal USB drives, ħażna esterna jew backups f’ambjent cloud

2.2 Tapplika wkoll għall-individwi kollha responsabbli mill-ġestjoni jew mill-amministrazzjoni tal-proċessi tal-backup, inklużi:

2.2.1 il-Maniġer Ġenerali (GM) jew persuna responsabbli maħtura

2.2.2 fornituri esterni ta’ servizzi ta’ appoġġ tal-IT jew konsulenti

2.2.3 l-impjegati kollha responsabbli biex isalvaw id-data f’postijiet approvati

3. Objettivi

3.1 Jiġi żgurat li d-data u s-sistemi kritiċi kollha tan-negozju jkollhom backup sigur f’intervalli xierqa skont ir-riskju u l-ħtieġa operattiva.

3.2 Tiġi żgurata l-kapaċità li d-data tiġi rkuprata kompletament u fi żmien xieraq wara tfixkil.

3.3 Jiġi evitat aċċess mhux awtorizzat, tbagħbis jew telf ta’ data tal-backup permezz ta’ kontrolli effettivi tal-ħażna.

3.4 Ir-rwoli u r-responsabbiltajiet għall-implimentazzjoni u l-ittestjar tal-proċeduri tal-backup għandhom ikunu attribwiti b'mod ċar u infurzati.

3.5 Tiġi appoġġata l-konformità ma' ISO/IEC 27001, il-GDPR u obbligi regolatorji oħra permezz ta' prattiki tal-backup strutturati u dokumentati.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Japprova din il-politika u jiżgura li tiġi implimentata

4.1.2 Jalloka r-riżorsi u jassenja r-responsabbiltà għall-attivitajiet tal-backup u r-restawr

4.1.3 Jirrieżamina fallimenti tal-backup, inċidenti jew devjazzjonijiet mill-politika

4.1.4 Imexxi r-rieżamijiet annwali tal-politika u jiżgura li l-organizzazzjoni tkun lesta għall-awditjar

4.2 Fornitur Estern ta' Appoġġ tal-IT (jekk applikabbli)

4.2.1 Jimplimenta u jimmaniġġja soluzzjonijiet tal-backup (lokali jew f'ambjent cloud)

4.2.2 Jimmonitorja s-suċċess tal-backup u jippjana testijiet ta' restawr

4.2.3 Jirrapporta fallimenti u inċidenti direttament lill-GM

4.2.4 Jiżgura l-iċċifrar, ir-restrizzjonijiet tal-aċċess u l-ġestjoni korretta tal-mezzi tal-backup

[... 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 mill-GM. Attivaturi għal rieżamijiet interim jinkludu:

9.1.1 bidliet kbar fis-sistemi jew fil-metodi tal-ħażna

9.1.2 introduzzjoni ta' pjattaformi cloud jew pjattaformi ġodda tal-IT

9.1.3 bidliet legali jew regolatorji li jaffettwaw l-irkupru tad-data

9.1.4 sejbiet minn awditi jew inċidenti

9.2 Il-GM huwa responsabbli biex jibda r-rieżami, japprova l-bidliet u jikkomunika l-aġġornamenti.

9.3 Il-verżjonijiet tal-politika għandhom jiġu traċċati u arkivjati. Verżjonijiet sostitwiti għandhom ikunu ristretti fl-aċċess sabiex tiġi evitata konfużjoni waqt awditi jew avvenimenti ta' rkupru tan-negozju.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija allinjata ma' u tiddependi fuq il-politiki SME li ġejjin:

10.1.1 P14S – Politika ta' Żamma tad-Data u r-Rimi: Tiddefinixxi kemm għandha tinżamm id-data tal-backup u kif għandha titħassar b'mod sigur.

10.1.2 P13S – Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data: Tgħin biex tingħata prijorità lil liema data għandha tiġi koperta mill-backup skont il-livelli ta' klassifikazzjoni.

10.1.3 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tkopri l-proċeduri jekk il-backups ifallu jew jekk ikun meħtieġ l-irkupru tad-data wara ksur jew interruzzjoni fis-servizz.

10.1.4 P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tassenja awtorità ċara għas-sorveljanza tal-backup u l-infurzar tal-politika.

10.1.5 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li l-ġestjoni tal-backup ta' data personali tkun allinjata mar-regolamenti legali u tal-privatezza.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 8.1: Ippjanar operattiv u kontroll tas-sistemi tal-backup bħala parti mill-ISMS

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.13: Jistabbilixxi prattiki tajbin għall-iskedar tal-backup, il-monitoraġġ u r-restawr

11.2.2 Anness A Kontroll 5.29: Integrazzjoni tal-backup mal-kontinwità tan-negozju u l-kapaċità ta' restawr

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (Ippjanar ta' Kontinġenza): Jiddefinixxi strateġiji strutturati ta' backup għar-reżiljenza tan-negozju

11.3.2 MP-6 (Protezzjoni tal-Mezzi): Jeħtieġ ġestjoni u qerda sigura tal-mezzi tal-backup

11.4 GDPR tal-UE

11.4.1 Artikolu 5(1)(f): Jobbliga l-integrità u d-disponibbiltà tad-data personali

11.4.2 Artikolu 32(1)(c): Jeħtieġ il-kapaċità li l-aċċess għad-data personali jiġi rrestawrat f'waqtu

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(c): Jeħtieġ backup u rkupru bħala parti mill-ippjanar tar-reżiljenza u l-kontinwità

11.6 DORA tal-UE

11.6.1 Artikolu 10(1): L-organizzazzjonijiet tas-settur finanzjarju għandhom jiżguraw il-backup bħala parti mill-miżuri ta' kontinwità tal-ICT

11.7 COBIT 2019

11.7.1 BAI04.05: Jeħtieġ strateġiji ta' backup dokumentati

11.7.2 DSS04.07: Jenfasizza l-ittestjar ta' rutina u l-kontroll fuq il-proċessi tal-backup u tal-irkupru tad-data