					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P32S					Titlu tad-dokument: **Politika dwar il-Kontinwità tan-Negozju u l-Irkupru minn Diżastru**						
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, 6.3, 8	
ISO/IEC 27002:2022	Kontrolli 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
GDPR tal-UE	Artikoli 32, 33	
Direttiva NIS2 tal-UE	Artikolu 21(2)(f)	
DORA tal-UE	Artikolu 10	
COBIT 2019	DSS04	

1. Għan

1.1 Din il-politika tiżgura li l-organizzazzjoni tkun tista’ żżomm l-operazzjonijiet tan-negozju u tirkupra s-servizzi essenzjali tal-IT waqt u wara avvenimenti ta’ tfixkil, bħal qtugħ tad-dawl, attakki ċibernetiċi, infezzjonijiet b’ransomware jew fallimenti tas-sistemi.

1.2 Hija tipprovdi qafas ċar għall-ippjanar tal-kontinwità tan-negozju u tal-irkupru minn diżastru (BC/DR), adattat għal SMEs mingħajr timijiet tal-IT dedikati.

1.3 Din il-politika tgħin lill-organizzazzjoni tissodisfa rekwiżiti obbligatorji skont ISO/IEC 27001:2022, il-GDPR, in-NIS2, id-DORA u COBIT 2019, filwaqt li ssaħħaħ ir-reżiljenza operattiva u l-fiduċja tal-klijenti.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 Is-sistemi u s-servizzi kollha kritiċi għan-negozju (eż. email, ħażna fil-cloud, pjattaformi tal-fatturazzjoni, reġistri tal-klijenti)

2.1.2 L-impjegati kollha u l-forniturі esterni ta’ servizzi tal-IT responsabbli għat-tħejjija u l-eżekuzzjoni tal-BC/DR

2.1.3 It-tipi kollha ta’ tfixkil, inklużi inċidenti ċibernetiċi, falliment tal-ħardwer, qtugħ tad-dawl, għargħar u nuqqas ta’ aċċess għall-uffiċċju

2.2 Din tkopri:

2.2.1 il-ġestjoni tal-backups

2.2.2 l-ippjanar tal-kontinwità tan-negozju (BCP)

2.2.3 l-operazzjonijiet ta’ rkupru minn diżastru

2.2.4 it-taħriġ u l-ittestjar tal-persunal

2.2.5 il-proċeduri ta’ rispons legali u regolatorju

3. Objettivi

3.1 Tħares il-kapaċità tal-organizzazzjoni li twassal servizzi ewlenin minkejja tfixkil mhux ippjanat.

3.2 Tiżgura rkupru f’waqtu tas-sistemi u tad-data b’objettivi ta’ ħin għall-irkupru (RTOs) definiti minn qabel.

3.3 Tippermetti lill-persunal kollu jsegwi l-proċeduri ta’ kontinwità waqt kriżijiet b’konfużjoni minima.

3.4 Iżżomm il-konformità regolatorja mal-liġijiet dwar il-protezzjoni tad-data u r-reżiljenza operattiva, inkluż l-Artikolu 32 tal-GDPR u l-Artikolu 21 tan-NIS2.

3.5 Tistabbilixxi strateġija prattika u ttestjabbli għall-kontinwità u l-irkupru, xierqa għall-SMEs.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Huwa responsabbli mis-sjieda tal-proċess tal-BC/DR u ta' din il-politika

4.1.2 Japprova l-Pjan ta' Kontinwità tan-Negozju (BCP)

4.1.3 Jikkoordina r-rispons għall-inċidenti u l-komunikazzjoni interna waqt tfixkil

4.1.4 Jagħmel notifiki regolatorji kif meħtieġ (eż. rapporti ta' ksur skont il-GDPR)

4.2 Fornitur Estern ta' Servizzi tal-IT / Amministratur tas-Sistema

4.2.1 Iżomm u jittestja l-backups

4.2.2 Jesegwixxi l-proċeduri ta' rkupru minn diżastru meta jiġu attivati

4.2.3 Jiddokumenta l-azzjonijiet kollha ta' rkupru u l-avvenimenti ta' restawr tas-sistema

4.2.4 Jirrapporta minnufih lill-GM kull inċident kritiku tal-IT

[... 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 u tal-pjan

9.1.1 Il-Maniġer Ġenerali (GM) għandu jiżgura li din il-politika u l-Pjan ta' Kontinwità tan-Negozju (BCP) assoċjat magħha jiġu rieżaminati formalment mill-inqas darba fis-sena.

9.1.2 Ir-rieżami għandu jinkludi:

9.1.2.1 evalwazzjoni ta' riskji ġodda jew emerġenti

9.1.2.2 revalidazzjoni tar-RTOs/RPOs

9.1.2.3 verifika tal-informazzjoni tal-forniturі u tal-kuntatti

9.1.2.4 allinjament ma' bidliet fis-sistemi tal-IT, fl-obbligi legali jew fl-operazzjonijiet

9.2 Aġġornamenti bbażati fuq attivaturi

9.2.1 Din il-politika għandha wkoll tiġi aġġornata b'reazzjoni għal:

9.2.1.1 inċidenti jew tfixkil maġġuri, speċjalment jekk l-objettivi ma jkunux intlaħqu

9.2.1.2 obbligi legali jew regolatorji ġodda (eż. emendi għad-DORA)

9.2.1.3 bidliet f'sistemi kritiċi, pjattaformi cloud jew persunal

9.2.1.4 sejbiet minn testijiet annwali tal-BCP/DR

9.3 Proċess ta' kontroll tat-tibdil

9.3.1 Il-bidliet kollha għandhom jiġu approvati mill-GM

9.3.2 Għandu jinżamm log tal-istorja tal-verżjonijiet, inklużi d-data, id-deskrizzjoni tat-tibdil u l-approvatur

9.3.3 Il-politika aġġornata għandha terġa' titqassam lill-persunal rilevanti kollu, inkluż il-fornitur tal-IT u l-kapijiet tad-dipartimenti

9.4 Dokumentazzjoni tal-lessons learned

9.4.1 Wara testijiet jew tfixkil reali, il-lessons learned dokumentati għandhom jiġu integrati fir-rieżamijiet futuri

9.4.2 Dawn ir-rieżamijiet għandhom jinkludu wkoll evalwazzjonijiet tal-prestazzjoni tal-forniturі u kontrolli tal-adegwatezza tar-rispons

10. Politiki relatati u rabtiet

10.1 Din il-politika hija integrata mill-qrib mal-politiki SME li ġejjin:

10.1.1 P1S – Politika tas-Sigurtà tal-Informazzjoni: Tiddeskrivi l-objettivi ta' sigurtà ta' livell għoli li l-prattiki tal-kontinwità u tal-irkupru għandhom jappoġġjaw.

10.1.2 P4S – Politika dwar il-Kontroll tal-Aċċess: Tippermetti revoka jew restawr ta' emerġenza tal-aċċess tal-utenti waqt xenarji ta' tfixkil fin-negozju.

10.1.3 P6S – Politika tal-Ġestjoni tar-Riskju: Tifforma l-bażi għall-identifikazzjoni, il-valutazzjoni u l-prijoritizzazzjoni ta' riskji relatati mal-kontinwità.

10.1.4 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Tiżgura li l-impjegati jkunu ppreparati biex jaġixxu waqt tfixkil u jifhmu l-BCP.

10.1.5 P15S – Politika dwar il-Backup u r-Restawr: Tipprovdi proċeduri tekniċi speċifiċi għas-salvagwardja tad-disponibbiltà tad-data u l-irkupru.

10.1.6 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tiżgura li l-ippjanar tal-kontinwità jirrispetta l-protezzjoni tad-data personali u jikkonforma mal-GDPR waqt u wara l-inċidenti.

10.1.7 P22S – Politika tal-Illoggjar u l-Monitoraġġ: Tappoġġja s-sejbien ta' avvenimenti li jistgħu jattivaw il-proċessi tal-BC/DR, u tipprovdi traċċi ta' awditjar forensiċi wara t-tfixkil.

10.1.8 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tiġi qabel, b'mod dirett, l-attivazzjoni tal-proċess ta' rkupru f'każ ta' inċidenti ċibernetiċi jew operattivi.

10.1.9 P31S – Politika dwar il-Ġbir tal-Evidenza u l-Forensika: Tiżgura li l-evidenza diġitali tinqabad waqt xenarji ta' kontinwità għal bżonnijiet ta' konformità, assigurazzjoni jew investigazzjoni.

10.2 Dawn il-politiki jiffurmaw qafas koerenti u lest għall-awditjar għar-reżiljenza, ir-responsabbiltà u l-kontinwità tal-kontrolli fl-operazzjonijiet kollha tal-SME.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001:

11.1.1 Klawżola 6.1 – Teħtieġ ippjanar u trattament ibbażati fuq ir-riskju, inklużi l-kontinwità tan-negozju u l-irkupru.

11.1.2 Klawżola 6.3 – Tenfasizza t-titjib kontinwu wara tfixkil.

11.1.3 Klawżola 8.1 – Tagħmel obbligatorji kontrolli operattivi, li jinkludu miżuri ta' kontinwità dokumentati.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 5.29 – Jeħtieġ l-istabbiliment u ż-żamma ta' arranġamenti għall-kontinwità tan-negozju.

11.2.2 Kontroll 5.30 – Jeħtieġ l-ittestjar u r-rieżami ta' dawk l-arranġamenti.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Jiddefinixxi rekwiżiti għall-ippjanar ta' kontinġenza.

11.3.2 CP-4 – Jagħmel obbligatorju taħriġ dwar il-kontinġenza għall-persunal tal-organizzazzjoni.

11.3.3 CP-6 – Ikopri rekwiżiti għal sit alternattiv ta' ħażna.

11.3.4 CP-7 – Jirregola aspettattivi għal sit alternattiv ta' pproċessar.

11.4 GDPR tal-UE:

11.4.1 Artikolu 32 – Jeħtieġ miżuri biex jiżguraw id-disponibbiltà kontinwa u r-reżiljenza tas-sistemi u s-servizzi tal-ipproċessar.

11.4.2 Artikolu 33 – Jattiva obbligi ta' notifika ta' ksur f'każijiet fejn falliment tal-kontinwità jwassal għal kompromess ta' data personali.

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

11.5.1 Artikolu 21(2)(f) – Jeħtieġ kapaċitajiet ta' ppjanar tal-kontinwità u ta' ġestjoni tal-kriżijiet bħala kundizzjoni għat-tħejjija għar-riskju ċibernetiku.

11.6 DORA tal-UE (2022/2554):

11.6.1 Artikolu 10 – Jagħmel obbligatorja l-implimentazzjoni ta' ttestjar tar-reżiljenza operattiva diġitali u ta' kapaċitajiet ta' rkupru, b'mod partikolari għal SMEs tas-settur finanzjarju.

11.7 COBIT 2019:

11.7.1 DSS04 – Ġestjoni tal-Kontinwità: Jipprovdi gwida ta' governanza fil-livell tal-intrapriża għaż-żamma u l-verifika tar-reżiljenza operattiva, inklużi s-sjieda, l-ittestjar, l-integrazzjoni tal-forniturі u r-rieżamijiet wara l-avveniment.