					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P32					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	Klawżola 8	
ISO/IEC 27002:2022	Kontrolli 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 sa CP-11	
NIST SP 800-34 Rev.1	Ippjanar ta' kontinġenza	Qafas
ISO 22301:2019		Rekwiżiti tas-Sistema ta' Ġestjoni tal-Kontinwità tan-Negozju
GDPR tal-UE	Artikolu 32	
Direttiva NIS2 tal-UE	Artikolu 21(2)(f)	
DORA tal-UE	Artikolu 10	
COBIT 2019	DSS04	

1. Għan

1.1. Din il-politika tiddefinixxi l-kontrolli u r-responsabbiltajiet obbligatorji biex tiżgura l-kapaċità tal-organizzazzjoni li żżomm jew tirkupra operazzjonijiet kritiċi tan-negozju u s-servizzi ta' appoġġ tal-ICT waqt u wara inċident ta' tfixkil.

1.2. Għandha l-għan li tipproteġi l-ħajja, l-istabbiltà operattiva, l-obbligi legali, l-impenji lejn il-klijenti u r-reputazzjoni tal-organizzazzjoni billi ssaħħaħ ir-reżiljenza permezz ta' ppjanar proattiv u kapaċitajiet ta' rkupru verifikati.

1.3. Din il-politika tipprovdi l-bażi għall-qafas tal-Ġestjoni tal-Kontinwità tan-Negozju (BCM) u tal-Irkupru minn Diżastru (DR) tal-organizzazzjoni, u tiżgura konformità mar-rekwiżiti regolatorji, kuntrattwali u settorjali applikabbli.

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għall-unitajiet organizzattivi kollha, is-sistemi tal-informazzjoni, il-proċessi tan-negozju, il-persunal u s-servizzi ta' partijiet terzi li huma kklassifikati bħala kritiċi jew essenzjali abbażi tar-riżultati tal-Business Impact Analysis (BIA).

2.2. Il-politika tkopri:

2.2.1. Tfixkil naturali u kkawżat mill-bniedem, inklużi attakki ċibernetiċi, ħsarat fl-infrastruttura, qtugħ taċ-ċentri tad-data, pandemiji u interruzzjonijiet fis-servizzi tal-forniturі

2.2.2. L-ippjanar, l-ittestjar u t-titjib kontinwu tal-Pjanijiet tal-Kontinwità tan-Negozju (BCPs) u tal-Pjanijiet tal-Irkupru minn Diżastru (DRPs)

2.2.3. Ir-rwoli u r-responsabbiltajiet għar-rispons ta' emerġenza, il-koordinazzjoni tal-irkupru u l-eskalazzjoni tal-inċidenti

2.3. Il-persunal kollu li għandu responsabbiltajiet marbuta mal-kontinwità jew mal-irkupru, inklużi l-IT, is-sidien tan-negozju, il-maniġers tal-kriżijiet u l-forniturі, huwa suġġett għad-dispożizzjonijiet ta' din il-politika.

3. Objettivi

3.1. Tiġi żgurata l-kontinwità tal-operazzjonijiet u tas-servizzi tan-negozju permezz ta' proċeduri definiti minn qabel u ttestjati, filwaqt li jitnaqqas l-impatt operattiv, reputazzjonali u legali.

3.2. Jiġu rkuprati s-servizzi tal-ICT fi ħdan ir-Recovery Time Objectives (RTOs) u r-Recovery Point Objectives (RPOs) definiti, allinjati mal-livelli ta' tolleranza għar-riskju tan-negozju.

3.3. Tiġi assenjata sjieda għall-ippjanar, l-eżekuzzjoni u l-governanza tal-kontinwità tan-negozju u tal-irkupru minn diżastru madwar l-organizzazzjoni kollha.

3.4. Jiġi żgurat li l-kapaċitajiet ta' kontinwità jiġu ttestjati, miżmuma u mtejba regolarment abbażi ta' xenarji realistiċi u sejbiet tal-awditjar.

3.5. Jiġu ssodisfati l-obbligi ta' konformità skont l-ISO, NIST, GDPR, DORA u NIS2, b'appoġġ għad-diliġenza dovuta fir-reżiljenza operattiva u fid-disponibbiltà.

4. Rwoli u responsabbiltajiet

4.1. Tmexxija Eżekuttiva

4.1.1. Tapprova l-Politika dwar il-Kontinwità tan-Negozju u l-Irkupru minn Diżastru u tiżgura l-allinjament strateġiku.

4.1.2. Talloka baġit u riżorsi biex tappoġġa l-kontinwità tan-negozju, ir-rispons ta' emerġenza u l-eżerċizzji ta' rkupru.

4.2. Maniġer tal-Kontinwità tan-Negozju (Responsabbli BCM)

4.2.1. Huwa responsabbli għall-iżvilupp u ż-żamma tal-BCPs fil-livell tal-organizzazzjoni kollha u għall-koordinazzjoni tal-ittestjar tal-kontinwità.

4.2.2. Iżomm l-iskeda tal-BIA, jiffaċilita t-taħriġ u jiżgura li d-dokumentazzjoni tissodisfa l-istandards ta' konformità.

[... 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 trid tiġi rieżaminata kull sena mill-Maniġer tal-Kontinwità tan-Negozju u mill-Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni biex jiġi żgurat l-allinjament ma':

9.1.1. Bidliet fl-operazzjonijiet tan-negozju, fis-sistemi kritiċi jew fl-infrastruttura

9.1.2. Lessons learned minn inċidenti, awditi, tabletop exercises jew testijiet tad-DR

9.1.3. Obbligi regolatorji jew kuntrattwali aġġornati (eż. DORA, GDPR, rekwiżiti tal-klijenti dwar RTO/RPO)

9.1.4. Bidliet fl-aptit għar-riskju tal-organizzazzjoni jew fl-istrateġija ta' kontinwità

9.2. Ir-rieżamijiet iridu jinkludu:

9.2.1. Verifika tar-rilevanza tal-pjanijiet u tad-dettalji ta' kuntatt

9.2.2. Rivalutazzjoni tal-RTOs, RPOs u tal-klassifikazzjoni fil-livelli tal-irkupru

9.2.3. Evalwazzjoni tal-kapaċità tas-servizz tal-backup u tad-DR

9.2.4. Feedback mill-partijiet interessati li eżegwew pjanijiet jew testijiet ta' rkupru reċenti

9.3. Il-bidliet kollha fil-politika jridu jkunu:

9.3.1. Taħt kontroll tal-verżjoni b'raġuni dokumentata u approvazzjoni formali tal-partijiet interessati

9.3.2. Ikkomunikati lill-persunal u lit-timijiet ewlenin b'responsabbiltajiet aġġornati

9.3.3. Riflessi fit-taħriġ, fil-materjal ta' sensibilizzazzjoni u fil-proċeduri operattivi aġġornati

9.4. Għandhom jinħarġu aġġornamenti interim ta' emerġenza jekk ikun hemm bidla organizzattiva maġġuri, obbligu legali jew sejba kritika li tagħmel il-pjanijiet jew il-politika attwali mhux vijabbli.

10. Politiki relatati u rabtiet

10.1. Din il-politika taħdem f'koordinazzjoni mad-dokumenti ewlenin li ġejjin:

10.1.1. P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi r-rekwiżit għal operazzjonijiet reżiljenti u bbażati fuq ir-riskju taħt il-kundizzjonijiet kollha.

10.1.2. P5 – Politika tal-Ġestjoni tat-Tibdil: Tiżgura li kull bidla fil-konfigurazzjoni jew fl-infrastruttura relatata mal-irkupru ssegwi flussi tax-xogħol dokumentati u approvati.

10.1.3. P14 – Politika taż-Żamma u r-Rimi tad-Data: Tirregola ċ-ċiklu tal-ħajja tal-mezzi tal-backup u tad-data rkuprata użata fl-operazzjonijiet ta' kontinwità.

10.1.4. P15 – Politika dwar il-Backup u r-Restawr: Tapplika kontrolli fuq il-frekwenza tal-backup, is-sigurtà u l-verifika tar-restawr.

10.1.5. P18 – Politika tal-Kontrolli Kriptografiċi: Tiżgura li l-proċessi ta' rkupru jżommu l-istandards tal-iċċifrar u tal-kunfidenzjalità.

10.1.6. P22 – Politika tal-Illoggjar u l-Monitoraġġ: Tappoġġa s-sejbien u l-eskalazzjoni ta' avvenimenti li jaffettwaw il-kontinwità.

10.1.7. P30 – Politika dwar ir-Rispons għall-Inċidenti: Tiddefinixxi l-proċessi ta' trażżin, eskalazzjoni u analiżi tal-kawża ewlenija allinjati mal-attivaturi tal-kontinwità.

10.1.8. P33 – Politika dwar il-Monitoraġġ tal-Awditjar u l-Konformità: Tivverifika l-integrità u l-effettività tal-prattiki tal-kontinwità u tal-irkupru fis-sistemi u l-proċessi kollha.

11. Standards u oqfsa ta' referenza

11.1. Din il-politika hija allinjata ma' standards internazzjonalment aċċettati dwar il-kontinwità tan-negozju u l-irkupru minn diżastru, b'appoġġ għall-awditabbiltà, ir-reżiljenza u l-konformità legali.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.29 tal-Anness A – Sigurtà tal-Informazzjoni waqt Tfixkil: Jeħtieġ il-kontinwità tal-kontrolli tas-sigurtà taħt kundizzjonijiet avversi.

11.2.2. Kontroll 5.30 tal-Anness A – Tħejjija tal-ICT għall-Kontinwità tan-Negozju: Jobbliga l-preparazzjoni, l-ittestjar u l-verifika tal-kapaċitajiet ta' rkupru tal-ICT.

11.3. ISO 22301:2019 – Sistemi ta' Ġestjoni tal-Kontinwità tan-Negozju

11.3.1. Tipprovdi l-qafas biex jiġu stabbiliti, implimentati u miżmuma prattiki ta' BCM allinjati mal-objettivi organizzattivi u mal-limiti tar-riskju.

11.4. NIST SP 800-34 Rev.1 – Gwida għall-Ippjanar ta' Kontinġenza

11.4.1. Tiddeskrivi l-aħjar prattiki għall-pjanijiet ta' kontinġenza tas-sistemi tal-IT, inklużi l-iżvilupp tal-istrateġija ta' kontinwità, l-analiżi tal-impatt u l-ittestjar tal-pjanijiet.

11.5. GDPR tal-UE (2016/679)

11.5.1. Artikolu 32 – Sigurtà tal-Ipproċessar: Jeħtieġ ir-reżiljenza tas-sistemi tal-ipproċessar u r-restawr f'waqtu tad-disponibbiltà u tal-aċċess għad-data personali wara inċident.

11.6. Direttiva NIS2 tal-UE (2022/2555)

11.6.1. Artikolu 21(2)(f): Jobbliga miżuri ta' kontinwità tan-negozju u ta' ġestjoni tal-kriżijiet biex jappoġġaw is-sigurtà tan-network u tas-sistemi tal-informazzjoni.

11.7. DORA tal-UE (2022/2554)

11.7.1. Artikolu 10 – Kontinwità tan-Negozju tal-ICT: Jeħtieġ li entitajiet finanzjarji jiżviluppaw u jittestjaw pjanijiet ta' kontinwità tal-ICT, inklużi RTO/RPO bbażati fuq ir-riskju u kapaċitajiet ta' failover.

11.8. COBIT 2019

11.8.1. DSS04 – Ġestjoni tal-Kontinwità: Ikopri l-aspetti kollha tal-ippjanar tal-kontinwità, inklużi l-identifikazzjoni tat-theddid, l-analiżi tal-impatt, l-istrateġija ta' rkupru u l-ittestjar regolari.