HOYA BIT

營運持續性之政策

權責單位：	技術資訊處
版次：	V1.0
本文件著作權屬本公司所有，未經本公司許可不准引用或翻印。	

文件修訂沿革

發行/修訂版次	發行/修訂生效日期	發行與變更說明	發行/修訂人員	核准人員
V1.0	2025/03/13	新版文件發行	技術資訊人員	董事長

第一條　　政策目的（Purpose）

本政策旨在建立一致性與制度化的營運持續性管理架構，透過系統性評估、計畫制定、測試演練與持續改進機制，以降低潛在災害對本公司關鍵營運活動之衝擊，確保資訊安全、法遵合規、客戶信任與業務永續性，並支援組織在各種突發事件中之復原能力與韌性。

第二條　　政策適用範圍（Scope）

本政策適用於本公司全體部門、關鍵人員、系統及第三方合作單位，涵蓋所有與關鍵業務、資訊系統、資訊資產、營運地點、人力資源及供應鏈相關之營運持續性計畫、程序與應變措施。

第三條　　政策聲明（Policy Statement）

一、營運持續性為企業治理之核心要素，公司管理階層須主動承諾並支持建立跨部門、具前瞻性之營運持續性管理架構。

二、本公司應每年執行營運衝擊分析（BIA）與風險評鑑，識別關鍵業務流程、資訊資產、RTO 與 RPO 要求。

三、各部門應依據風險評鑑結果，訂定具體、可操作之營運持續計畫（BCP），包含緊急應變、系統復原及資訊回復程序。

四、所有營運持續計畫應納入文件化管理、定期測試、教育訓練與異地備援機制，並符合資訊安全與合規性要求。

五、必須進行至少每年一次之模擬演練或實地測試，以確保計畫之可行性、及時性與組織應變能力。

六、任何重大演練異常、實際事件或營運中斷應於法定或監理要求時間內通報並追蹤改善。

七、本公司應持續評估與改善營運持續性計畫，以反應業務變動、外部環境及技術演進。

第四條　　角色與責任（Roles and Responsibilities）

單位／職責	主要職責內容
董事會／高階主管	確保營運持續性為企業治理目標之一，核定相關政策與資源配置。
資訊安全工作小組	擬定營運持續政策與年度測試計畫，統籌 BIA、BCP 設計與審查，監督演練與改善進度。
各業務部門主管	協助識別關鍵流程、風險點，負責本部門BCP建置、演練參與與應變落實。
資訊安全處理分組	擔任營運持續計畫執行與演練推動之協調窗口，執行文件維護、記錄留存與異常追蹤。
系統管理與基礎設施	確保關鍵系統符合復原標準，負責異地備援、資料備份、RTO/RPO 達成能力之實施與維運。
稽核／法遵單位	監督與評估整體營運持續性管理制度合規性，對演練與實際應變進行獨立性審查與回饋。

第五條　　治理原則與實施要求（Governance & Implementation Requirements）

一、文件化與版本控管：所有BIA、BCP、演練報告與通報紀錄應設有文件控制編號並定期更新。

二、資訊分類與保護等級考量：依據資訊資產之敏感性、可用性與業務依賴度，決定異地備援與備份頻率。

三、關鍵資源調度與通報機制：建立應變通報流程、內外部聯絡清單、資源動員程序，以支援即時回應。

四、供應鏈與第三方整合：營運持續性政策應涵蓋對外部服務供應商之契約要求與SLA（Service Level Agreement）驗證。

五、教育訓練與意識提升：每年至少辦理一次針對關鍵人員之BCP教育訓練與測驗。

六、演練評估與持續改善：每次演練應完成檢討報告並納入改善項目，追蹤至完成為止。

七、合規性與監理配合：營運持續性制度應符合主管機關、產業標準（如 ISO 22301）與內部稽核標準。

第六條　　核定層級

本政策經提報董事長核定後施行，修正或廢止時亦同。