優答台灣股份有限公司

營運持續性政策

第一條　　目的

本政策旨在建立一套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，以確保優答台灣股份有限公司（下稱「本公司」）業務活動受到之干擾降至最低，並於發生業務中斷時仍能迅速恢復正常營運，以履行對客戶之義務。

第二條　　適用範圍

本政策適用於本公司全體部門、人員、系統及第三方合作單位，涵蓋所有與本公司業務、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

一、 本政策包括營運持續暨災難復原計畫。本公司應每年進行風險評鑑，據以檢視並更新營運持續暨災難復原計畫及災難復原計畫之相關需求，以反映業務變動、外部環境及技術之演進。此外，營運持續暨災難復原計畫應隨情勢變動而及時更新。

二、 本公司全體人員應受告知並確實瞭解營運持續暨災難復原計畫內容，及其各自所應擔負之角色與職責。

三、 本公司進行至少每年一次之模擬演練或實地測試，以確保營運持續暨災難復原計畫之可行性、及時性與組織應變能力。

第四條　　權責單位

一、 本政策之權責單位分工如下：

(一) 資訊安全主管：

1. 擬定營運持續政策暨災難復原計畫，以及年度測試計

畫，擔任計畫執行與演練推動之協調窗口，辦理文件維護、記錄留存與異常追蹤工作。

2. 負責確保本公司遵循營運持續暨災難復原計畫及相關資訊安全要求，並統籌更新作業與事故應變措施。

(二) 各單位部門主管：確保各單位之營運持續暨災難復原計畫完整納入該單位業務運作所需的實際活動與面向，並確保所進行之測試均達成預期成效。

第五條　　營運持續暨災難復原管理措施

一、 本公司為確保關鍵業務功能於突發事件或重大災難發生時，得維持營運之持續性並迅速復原，特訂定本營運持續暨災難復原計畫（下稱「本計畫」），關於本計畫之重點管理措施包括：

(一) 保管技術及安全性面向：

1. 建置 AWS(Amazon Web Services)Aurora 全球資料庫等備援系統，以確保災難發生時系統之可用性。

2. Amazon 關聯式資料庫(Amazon Relational Database Service，RDS)故障預防與處理：

(1) AWS Aurora 全球資料庫為跨區域部署以因應區域性中斷，並使全球各地的使用者均能以低延遲方式讀取資料。

(2) 復原指標：RTO (Recovery Time Objective) 小於 1 分鐘；RPO (Recovery Point Objective) 小於 5 秒鐘，以減少資料損失。

(3) 自動化的儲存資料複寫機制：確保當主要系統故障時，備援區域能在 1 分鐘內接手所有讀寫工作。

(4) 每日自動備份可保存 7 日。

3. 關鍵管理服務(Key Management Service，KMS)故障預防與處理：

(1) 建置多區域 KMS 架構以確保持續運作，避免整體系統之中斷。

(2) 刪除之私鑰可於 7 日內復原，並由資訊安全部門持續監控。

4. 區塊鏈節點管理：

(1) 區塊鏈節點運作時，系統應定期建立快照，記錄節點運行時之狀態，以於發生災難或異常時，可利用快照影像將節點復原至正常狀態。

(2) 當虛擬機器(Virtual Machine，VM)發生故障時，應透過可插拔式儲存裝置切換至備援環境，以確保節點服務之持續運作與資料完整性。

5. 存取及安全性：採用多因子驗證、稽核日誌及即時監控，以維護資訊安全

6. 資料備份：每日自動執行資料備份，並建立快照復原機制，以確保於系統故障或資料遺失時，能即時將資料還原至備份時之狀態。

7. 災難情況模擬：定期進行災難復原模擬，以確保復原機制之可行及有效性

(二) 產品面向：

1. 版本控制：使用 GitLab 及 Docker 系統進行程式碼版本管控，以確保產品完整及可溯及性。

2. 關鍵基礎設備：

(1) 程式碼版本主要儲存於 GitLab，並於 Docker 儲存庫中登錄備份副本。

(2) 開發人員應每日執行離線備份作業，確保資料安全與可復原性。

(3) 系統管理權限應採至少兩位管理人共同管理之制度，以防止單一人員操作錯誤或故障造成系統中斷。

(4) 雲端服務之 root 帳號應以群組電子郵件建立，以確保帳號備援機制。

(5) 當服務或系統元件發生故障時，應依既有備份版本執行復原。

(三) 市場及供應商管理面向：

1. 於系統中斷時提供替代營運平台及工具，確保市場活動在中斷期間仍能無縫接軌進行。

2. 市場資料應加密並採取嚴格之接觸存取控制措施。

3. 與第三方供應商間之契約與相關合作文件應進行妥善備份及保存。

(四) 法律面向：

1. 所有法律文件應存放於雲端倉儲，並僅限授權人員存取。

2. 定期稽核本公司內部法律相關程序，以確保一致性及合法性。法律作業應集中使用 legaltaiwan@lmnl.app，避免造成單一窗口聯繫失敗之情況。

3. 委任營運當地法律顧問以確保本公司營運活動符合當地法律規範。

(五) 財務管理面向：

1. 採用 Xero 會計系統管理財務紀錄，並實施定期備份及備援措施。本公司每週及每月定期檢視財務紀錄以確保真實及完整性。

2. 本公司培訓多名人員熟悉財務作業，避免仰賴單一人員；如關鍵人員無法履職，總經理應持續掌握財務狀況。

3. 共用信箱：

   財務作業應集中使用 finance@lmnl.app，以確保作業備援與持續性。

(六) 公司行政事務面向：

1. 應建置自動化行事曆機制，以確保相關法律規定申報作業之正確性與及時性。

2. 公司治理文件應進行安全備份，並得於業務中斷期間內持續順利存取。

3. 應指定並培訓具跨部門職能之人員，於必要時得代理相關職責，以確保業務運作之持續性。

(七) 客戶服務面向：

1. 客戶服務應提供多重管道，並確保該等客戶服務能透過電子郵件、電話及即時聊天等平台同時運作，以提升服務可及性與回應效率。

2. 建立分層化之升級處理機制，明確界定各層級之職責與權限，以確保客戶之問題得以即時回應與妥適解決。

3. 應確保備援人員接受充分訓練，於主要人員缺席或無法執行職務時，能即時承接並處理客戶需求，確保服務之持續性。

(八) 其他營運事項

本公司營運流程應以各種 SaaS (Software as a Service)訂閱制平台進行管理，並透過共用電子信箱控管存取權限，以確保整體營運作業之持續性。

第六條　　營運持續暨災難復原計畫之測試及維護

一、 為確保營運持續暨災難復原程序之穩健性，降低營運中斷之風險，本公司應就該計畫進行週期性測試、檢討及維護。內容包括：

(一) 年度測試與更新

1. 本公司應每年維護、測試及更新營運持續暨災難復原計畫，並得視需要進行臨時測試，以確保其可行性與穩健性。

2. 資訊安全主管負責協調和進行營運持續暨災難復原管理措施的年度演練。

3. 測試過程及結果均應完整紀錄，並提交總經理審視，作為持續改進之依據。測試發現之缺失或不足，應即納入改進計畫，並於合理期限內完成修正。

(二) 針對虛擬資產（VAs）及分散式帳本（DLT）之特殊考量

1. 網路故障：應建立偵測與應變程序，迅速發現並緩解網路中斷情形，以維持資料完整與客戶信任。

2. 資料遺失或完整性受損：營運持續暨災難復原計畫應訂定明確程序，以防範虛擬資產及分散式帳本環境中

可能發生之資料遺失，並確保於任何中斷期間，關鍵營運資料受到完整保存。

二、 所有事故均應完整紀錄，並保存相關文件，以備稽核及追蹤。事故處理後，資訊安全主管應召開檢討會議，分析事故原因、影響範圍及改進措施，並納入後續控制程序。

第七條　　資通安全事件內部通報機制

一、 內部通報機制：

(一) 本公司應建立資通安全事件通報與升級機制，並依據分層式通報機制進行（詳細分層機制與人員資訊請參本條第二項）。

(二) 發生資安或營運中斷事件時，第一層人員應立即通報並採初步應變措施；若事件涉及重大系統中斷、資料洩漏或潛在法遵風險，應即升級至第二層，並由資訊安全主管指揮後續應對。

(三) 各層級通報人員之姓名、職稱、聯絡方式應定期檢視與更新，以確保通訊暢通及應變即時。

二、 分層通報機制表及關鍵人員聯絡資訊：

通報層級	職稱	姓名	電子郵件
第一層通報	各單位部門主管	郭姿吟 張正昕 鍾文政	lesleykuo@lmnl.app andrewchang@lmnl.app allenchung@lmnl.app
第二層通報	資訊安全主管	張仲霖	johnny@lmnl.app

第八條　　違規處分

一、 違反本政策的員工可能面臨與其違規行為相稱的懲處後果。

二、 本公司各權責單位主管將決定員工的違規行為的嚴重程度，並

採取適當的行動。對於輕微違規，員工可能僅接受口頭警告；對於較嚴重的違規（例如，未依本政策進行營運持續管理活動），員工可能面臨嚴重的紀律處分，包括終止聘僱契約。

第九條　　附則

本政策未盡事宜，悉依主管機關法令及本公司相關規定辦理。

第十條　　核決層級

本政策經提報總經理核准後實施，修正時亦同。

版本修訂紀錄表

版次	修訂日期	修訂內容
1.0	**2026.4.10**	**新制定**