

持續營運性計畫

最新修訂日期：2025/06/16

壹、前言

一、目的說明：

本營運持續計畫（Business Continuity Plan, BCP）的主要目標在於確保萃科科技股份有限公司（下稱交易所）遭遇各類突發事件（例如：網路攻擊、系統故障、自然災害、政策變動等）時，能夠維持核心業務的正常運作，並以最小的中斷時間保護用戶資產與維護市場信心。此計畫旨在建立一整套系統化、標準化的應急處理與復原流程，涵蓋從風險預防、應急響應到後續復原的全階段管理，並確保所有相關單位和合作夥伴能夠在突發情況下迅速協調行動。

二、適用範圍：

本計畫適用於交易所內所有關鍵系統與運營流程，涵蓋範圍包括但不限於：IT 基礎設施、資金流轉、用戶數據安全、交易撮合、錢包管理、客戶服務、法令遵循以及與第三方合作商的合作。計畫同時涉及內部各單位與外部合作夥伴，目的在於在任何可能導致業務中斷的事件發生時，確保運營系統能夠迅速切換到備援方案並順利恢復正常狀態。

貳、風險評估與業務影響分析 (BIA)

一、風險識別

(一) 網路安全風險：

- 各類駭客攻擊（如 DDoS、惡意軟件、釣魚攻擊、SQL 注入等）可能導致系統癱瘓或資料洩漏。
- 外部攻擊與內部不合規操作均可能對交易數據與用戶資產構成威脅。

(二) 系統故障：

由硬體故障、軟體缺陷、電力中斷或網路連線問題等引起的服務中斷，可能造成交易所核心系統暫停運作。

(三) 自然災害：

包括地震、火災、洪水等天災，這類事件可能直接破壞數據中心及辦公場所，導致長時間運營中斷。

(四) 市場流動性與金融風險：

異常市場波動、流動性危機及突發的金融事件可能引起交易異常或資金調度上的壓力。

(五) 監管政策與法律風險：

政府新法規、監管政策變更或跨國法律衝突，均可能影響交易所的運營模式及法律合規性。

(六) 內部管理與操作失誤：

包括內部人員的操作失誤、資訊誤傳或內部欺詐行為，這些均會對交易所的正常運營帶來不可預測的影響。

二、業務影響分析：

(一) 關鍵業務功能識別：

詳細列舉交易撮合、錢包管理、用戶身份認證（KYC/AML）及數據庫管理等核心系統，分析各系統在不同風險情境下可能受到的影響。

(二) 影響範圍與優先級排序：

根據各類風險的發生概率及其對系統運作的影響，確定各業務模塊的重要性與優先保護順序，並制定相應的緊急應對方案。

(三) 財務與聲譽風險評估：

預估每一風險可能引發的經濟損失和品牌聲譽受損的程度，為各項復原措施提供決策參考。

參、組織架構與指揮系統

一、緊急指揮團隊組成

(一) 組織結構：

由執行長、技術單位、風險控制單位、財會單位、法令遵循單位與行銷單位組成緊急指揮中心，形成一個跨單位協作體系。

(二) 職責與分工：

1. 每個單位均需指定一名緊急負責人，明確在危機情況下的決策、協調與執行職責。
2. 制定詳細的行動指南，規定指揮中心在接到警報後的各項步驟與工作流程。

二、應急聯絡清單建立

(一) 內部聯絡：

整理全體員工及單位負責人的聯絡資訊（電話、電子郵件、即時通訊工具等），並定期進行測試，確保信息傳遞通暢。

(二) 外部聯絡：

編制第三方服務商、法律顧問、主管機關與媒體聯絡人名單，並保持 24/7 可用的聯絡渠道。

(三) 聯絡方式更新：

建立定期更新機制，確保所有聯絡資訊均為最新狀態，並在突發事件發生前進行快速核對。

肆、營運持續策略

一、資訊系統與網路安全保障

本公司除按本公司之《資訊安全作業規範》之內容辦理外，應透過以下方法達成資訊系統之營運持續性：

(一) 多區域備援與冗餘設計：

1. 在不同地理位置設置備援數據中心，實施冗餘架構，確保在單點失效時能迅速切換。
2. 建立雙主架構或多主架構系統結構，保證任一數據中心故障時，其他中心能立即承擔業務負載。

(二) 數據備份與災難恢復：

1. 制定每日、每周及每月不同級別的數據備份計畫，並採用異地存儲與雲端備份技術。
2. 定期進行災難恢復演練，驗證數據備份的完整性與恢復流程的可行性。

(三) 安全監控與防禦措施：

1. 部署先進的入侵檢測與防禦系統，實時監控網路流量及安全事件。
2. 定期進行漏洞掃描、滲透測試，及時修補潛在風險。

二、資金與資產保護措施

本公司應按本公司之《資產管理政策》與相關法規之規定，嚴格實踐以下目標：

(一) 用戶資產與交易所自有資產分離管理：

1. 設立獨立的用戶資產隔離帳戶，將用戶存放的資金與交易所自有運營資金分開管理，確保在風險事件或資產糾紛發生時，用戶資金能夠獨立保護，不受其他資金運作的影響。
2. 建立專門的清算流程與監控系統，確保用戶資產在日常運作中始終保持獨立性，並能夠在需要時快速調用或凍結，防範資金挪用風險。
3. 制定嚴格的內部管理與操作規範，並定期進行內部審核與第三方風險評估，確保用戶資產與自有資產分離管理制度落實到位，並符合最新監管要求與安全標準。

(二) 冷熱錢包分離管理：

1. 嚴格區分線上熱錢包與私鑰離線存儲之冷錢包，依法令之規定按比例將用戶之資產分別存放在熱錢包與冷錢包之中。
2. 建立專業的資金管理流程與審核制度，確保資金流動的每一環節都有多重驗證。

(三) 多重簽名與權限控制：

1. 實施多重簽名機制，對涉及大額交易的操作進行多重審核，防止單一內部人員濫權。
2. 定期審查用戶權限，防止未經授權的訪問或操作。

三、供應鏈及第三方協作策略

(一) 供應商風險評估：

評估所有第三方供應商與外部合作夥伴的營運持續能力，確保其具備應對突發事件的方案。

(二) 應急合作協議：

與關鍵合作夥伴簽訂具體的應急合作協議，明確在發生突發情況下的權責分配與支援流程。

(三) 聯合演練與溝通機制：

定期與外部合作夥伴進行聯合應急演練，測試跨組織協同應對能力，並在演練後進行評估與改進。

伍、應急響應程序

一、啟動條件與觸發機制

(一) 明確的觸發標準：

1. 根據系統異常、資金異常流動、網路攻擊或自然災害等事件設定具體的啟動條件。
2. 利用自動化監控系統，當檢測到符合預設條件的異常時，立即發出警報並啟動應急響應流程。

二、初步評估與決策流程

(一) 迅速成立緊急指揮中心：

一旦觸發條件滿足，迅速召集相關單位負責人，成立臨時緊急指揮中心，進行第一時間的情況評估。

(二) 影響範圍與風險判斷：

詳細評估事件對交易撮合、錢包管理、用戶數據及其他關鍵系統的影響，並根據影響程度決定後續處理方案。

(三) 決策發布與指令下達：

緊急指揮中心根據初步評估結果，迅速做出決策，並向全體相關人員下達明確的行動指令與後續應急步驟。

三、立即行動與現場處理

(一) 啟動備援系統：

根據預先制定的備援計畫，立即將系統運營切換至其他數據中心或冗餘系統，保證服務不中斷。

(二) 內外部資訊同步：

快速通知內部技術團隊、運營團隊及外部合作夥伴，同時根據預先準備的公告模板向主管機關及用戶發布初步資訊。

(三) 事件記錄與監控：

詳細記錄事件發生的時間、性質、初步處理措施及各項反饋資訊，並持續更新事件進展，為後續復原工作提供依據。

陸、復原計劃

一、分階段復原策略

(一) 核心業務優先恢復：

在確保安全前提下，第一時間重啟交易撮合、錢包管理與用戶認

證等核心系統，並逐步恢復輔助業務與其他系統。

(二) 設定恢復目標：

根據不同系統的重要性，制定明確的恢復時間目標（RTO）及數據恢復點目標（RPO），並在復原過程中實時跟蹤進度。

(三) 模擬復原測試：

定期進行模擬恢復測試，驗證各項復原流程的準確性與有效性，並根據測試結果不斷優化復原方案。

二、資源調度與協同

(一) 技術與人力資源整合：

指定專責團隊負責復原作業，確保有充足的技術支持、緊急工具及外部專家協助。

(二) 專案預算資金支持：

為可能發生的臨時支出準備預算，確保復原過程中資金與物資能夠及時到位。

(三) 復原進度監控：

實時監控各系統復原進度，並建立反饋機制，確保所有環節均符合預期標準，必要時迅速調整資源分配。

柒、溝通計劃

一、內部溝通機制

(一) 多渠道即時通知：

建立簡訊、電子郵件、即時通訊與專用緊急通知系統，確保所有員工在發生突發事件時能夠迅速接收到訊息與指令。

(二) 標準化資訊報告流程：

制定內部資訊報告的格式與頻率，各單位必須定期向緊急指揮中心上報情況進展，確保資訊流動順暢。

(三) 內部培訓與演練：

定期對所有員工進行緊急溝通與協同工作的培訓，提高全體人員在危機時的反應速度與協作能力。

二、外部溝通策略

(一) 統一公關發言：

指定專業公關團隊及發言人統一對外發布資訊，避免因資訊不一致引發混亂或市場恐慌。

(二) 公告模板與媒體溝通：

預先準備多種情境下的公告模板（包括初步通報、最新狀況更新及事件結束報告），並與主要媒體建立穩定的溝通管道。

(三) 用戶服務與疑慮回應：

通過客服熱線、官方網站、社群媒體等多種渠道主動回應用戶疑

問，解釋處理措施，維持用戶信任與市場穩定。

三、危機溝通與媒體應對

(一) 常見問答 (FAQ)：

編製詳細的 FAQ 文檔，涵蓋常見疑問與標準回應策略，供第一線客服與媒體參考。

(二) 透明與即時訊息發布：

確保所有對外發布的訊息均經過內部多層審核，並在事件進展中持續更新，避免資訊斷層或不實傳言。

捌、測試與訓練

一、定期演練與模擬

(一) 全面應急演練計畫：

每年至少組織一次全規模的應急演練，模擬包括桌面演練、實地模擬及跨單位聯合演練，覆蓋各種突發事件情境。

(二) 情境多樣性設計：

根據實際運營風險，設計包括網路攻擊、硬體故障、數據滅失、自然災害、政策變動等不同情境的模擬演練，確保演練內容全面且針對性強。

(三) 演練後評估與反饋：

演練結束後，組織全面評估會議，記錄各環節表現與不足，制定改進措施並形成書面報告，為下一次演練提供參考。

二、員工培訓與技能提升

(一) 定期專項培訓：

為各單位制定專門的培訓計畫，包括技術操作、緊急處理與危機溝通，並定期進行測試與考核。

(二) 模擬演練與實戰演習：

結合實際操作，進行模擬演練與實戰演習，提高員工在真實突發情況下的應對速度與協調能力。

(三) 持續技能更新：

根據最新技術與風險趨勢，持續更新培訓內容，確保員工掌握最新的應急處理方法與工具。

玖、計劃維護與審查

一、定期審查與更新

(一) 年度審查與調整：

制定明確的年度審查計畫，根據最新風險環境、技術進步與監管要求，定期檢討與更新營運持續計畫。

(二) 跨單位協同討論：

定期召開跨部門會議，徵求各單位對現行計畫的意見與改進建議，

確保計畫內容能夠切實反映實際運營狀況。

(三) 風險環境監控：

持續關注市場及技術的變化，並及時調整風險評估結果與應急措施，確保計畫始終保持前瞻性與有效性。

二、文件管理與版本控制

(一) 文件集中管理：

建立集中管理的文件資料夾，對所有營運持續計畫相關文件進行歸檔與版本控制，確保每次修改均有詳細記錄。

(二) 內部審核與流程：

設立內部審核流程，所有文件更新必須經過董事（會）確認，並在發布新版後向所有相關人員進行通知。

三、合規性審視與稽核

(一) 定期合規審查：

組織團隊定期對計畫內容進行合規性檢查，確保所有措施均符合當前國內外監管標準與法律法規。

(二) 定期稽核機制：

建立定期稽核制度，對營運持續計畫的執行狀況進行審核，發現偏差及時糾正，並記錄稽核結果以供後續改進參考。

壹拾、附錄

一、緊急聯絡清單

- (一) 詳細列出內部應急指揮團隊成員、各單位負責人及其最新聯絡方式（電話、電子郵件、即時通訊工具等）。
- (二) 編制並定期更新外部合作夥伴、供應商、法律顧問、主管機關窗口及媒體聯絡人的詳細清單。
- (三) 設置備用聯絡方式，確保在主要聯絡渠道失效時能夠迅速取得聯繫。

二、關鍵資產清單

- (一) 詳細列出所有對交易所運營至關重要的硬體設備、網路設施、軟體系統及資料庫。
- (二) 包括交易撮合系統、錢包管理系統、用戶數據庫及其他業務支撐系統，並指定每項資產的責任人與備援方案。
- (三) 建立資產更新與檢查機制，確保清單內容符合最新實際情況。

三、技術文件與操作手冊

- (一) 提供完整的技術操作手冊，包括數據備份、系統恢復、網路安全維護及故障排查指南。
- (二) 詳細描述各系統操作流程、緊急處理指引與常見問題解決步驟，並定期更新。
- (三) 確保所有文檔均存檔於安全的內部系統，並隨時可供緊急處理人員查閱。

四、 備援資源列表

- (一) 列出所有關鍵外部資源，包括雲端服務平台、第三方技術支援、緊急供應商及其他緊急資源。
- (二) 詳細記錄各資源的服務範圍、聯絡資訊、緊急調用流程，確保在突發情況下能迅速調用。
- (三) 定期測試備援資源的可用性，並將測試結果作為評估資源有效性的依據。