資訊安全管理政策程序

最新修訂日期：2025/06/16

第一條　目的

一、本政策旨在確保交易所之資訊資產安全，維護資訊系統的機密性、完整性及可用性，並符合相關法令與監管要求。

二、本政策亦確保交易所具備完善的資訊安全架構，以應對日益增加的網路攻擊與內部風險。

第二條　適用範圍

本政策適用於交易所內所有資訊系統、設備、員工及第三方合作夥伴，並涵蓋所有與資訊安全相關之作業，包括但不限於資訊存取、數據處理、風險評估及事件應變。

第三條　最高管理層承諾

董事（會）與執行長應將資訊安全納入公司治理架構，確保資安政策之落實與持續改善，並提供適當的資源與預算，以確保資安計畫的有效執行。

第四條　資訊安全架構

一、交易所應設立資訊安全委員會（下稱資安委員會），由資訊安全單位主管負責召集，並定期檢討資安政策與風險管理計畫。

二、資安委員會應定期召開會議，確保各單位落實安全機制並有效應對新興威脅。

第五條　合規與標準遵循

確保符合 ISO27001、FATF 等標準，並應定期進行第三方資安稽核，以確保資訊安全管理系統的完整性及符合最新法規。

第六條　資安單位主管遴選與資格限制

一、遴選標準：

（一） 資安單位主管應具備至少三年資訊安全相關經驗，並曾直接或間接參與資安風險評估、事件應變與監管合規等工作。

（二） 需具備國內外公認的資訊安全專業證照，如 CISSP（Certified Information Systems Security Professional）、CISM（Certified Information Security Manager）或 CEH（Certified Ethical Hacker）等。

（三） 具備良好的溝通與管理能力，能夠協調內部資安事務並應對外部主管機關之要求。

二、資格限制：

（一） 資安單位主管與該單位人員不得有金融詐欺、內部交易或其他不誠信行為之紀錄。

（二） 不得兼任可能產生利益衝突之職務，例如財務主管、開發人員或系統管理員。

（三） 任職期間須定期接受資安相關進修課程，確保專業能力與時俱進。

第七條 最小權限原則

一、所有存取權限應遵循最小權限原則，並對高權限帳戶實施強化存取控制。
二、使用者權限應定期審查，確保符合業務需求並杜絕權限濫用。

第八條 多重驗證（MFA）

所有管理員與用戶必須啟用 MFA，對較高風險操作（如大額轉帳、API 設定變更）需額外身份驗證，如生物辨識技術或動態安全密碼。

第九條 帳號與密碼管理

一、應強制使用高強度密碼（至少 12 碼，包含大小寫字母、數字與特殊符號），並定期變更密碼。
二、異常登入應自動觸發額外驗證機制，並向帳號持有者發送安全警示。

第十條 防火牆與入侵防禦系統

一、應部署次世代防火牆（NGFW）並搭配 IDS/IPS 監測並阻擋惡意攻擊。
二、所有外部網路存取應透過安全通道（VPN）並受到嚴格監控。

第十一條 流量監控與日誌管理

一、 應使用 SIEM 監控異常流量與日誌，並實施行為分析機制（UEBA），以即時偵測可疑活動。
二、 日誌應至少保存 12 個月，以供稽核及資安事件調查。

第十二條 分區安全架構

一、應區分開發、測試與正式環境，並採用零信任架構（Zero Trust Architecture）。
二、內部網路應限制跨區域存取，並針對不同使用者角色設置不同的存取控制策略。

第十三條 數據分類與存取控制

依據 CIA 原則分類數據，並限制存取權限。所有敏感數據應透過角色為基礎的存取控制（RBAC）機制進行管理。

第十四條 數據加密與保護

一、靜態數據應採用 AES-256 加密，並儲存於受管控的資料中心。
二、傳輸數據應透過 TLS 1.3 加密，防止數據在傳輸過程中被攔截。
三、API 金鑰應透過 HSM 管理，私鑰存儲於冷錢包並使用多重簽名機制。

第十五條 資安事件回應流程

一、應建立資安事件應變計畫（IRP），並設立 24/7 SOC 監控與即時通報。
二、事件發生時，應依據標準作業程序（SOP）進行應變處理，確保風險最小化。

第十六條 取證與事後分析

一、所有資安事件應完整記錄，進行取證分析，並採取補救措施。
二、所有事件應納入風險評估機制，並提出具體的改進計畫。

第十七條　員工資安培訓

一、應定期對所有員工進行資安意識培訓，提高對釣魚攻擊、社交工程的警覺性。
二、針對不同職能的員工，制定專屬培訓內容，以確保有效應對相關資安風險。

第十八條　用戶教育與保護

提供安全使用指南，提高用戶資安意識，並透過多種管道（包括但不限於電子郵件、網站公告）提醒用戶常見資安風險與防範措施。

第十九條　法令遵循

應確保交易所符合相關法規，並定期進行第三方資安稽核，確保符合最新監管要求。

第二十條　內部資安稽核

內部資安稽核應每年至少進行一次完整稽核，並即時檢討政策。所有稽核發現的問題應即時整改，並定期跟蹤改善情況。

第二十一條　災難復原機制（DRP）

應建立完整的災難復原計畫（DRP），確保系統迅速恢復；並定期進行災難演練，以驗證應變機制的有效性。

第二十二條　營運持續性管理（BCM）

一、制定業務持續計畫（BCP），確保關鍵業務能在災害情境下持續運行。
二、應建立異地備援機制，並確保關鍵業務具備自動故障轉移（Failover）能力。