資訊安全指引

1. 適用範圍及管理責任

本指引適用於總會電郵、網站、雲端硬碟、網上表格、會員及賽事系統、官方社交媒體帳戶，以及用於存取上述系統的裝置。總會須指定系統負責人，維護平台清單，記錄管理人、授權使用者、復原途徑及備份安排。

2. 帳戶及存取權限

1. 按工作需要授權。有個人帳戶或角色分工功能的平台，應為每位使用者獨立授權。管理員權限只授予有管理需要的人員。
2. 官方電郵、雲端管理帳戶、網站後台及社交媒體管理帳戶，凡平台支援，均須啟用多重驗證。每個帳戶應使用獨立強密碼。復原電郵、電話及備用驗證碼須由總會指定人員安全保管。
3. 委員、職員、義工或承辦人員離任、調職或完成工作時，系統負責人須撤除或調整其帳戶、群組和檔案權限，處理相關共用憑證，並確認官方帳戶仍可由總會接管。重要帳戶權限應在委員交接及平台管理人更換時覆核。

3. 檔案、裝置及備份

1. 會員資料、付款紀錄、健康資料、投訴檔案及運動員名單須存放於總會指定位置。共享檔案應指定接收帳戶及權限。使用電郵發送前，須核對收件人、附件及連結權限。公開賽程及賽果應由獨立公開版本發布。
2. 用於處理總會資料的裝置須設螢幕鎖、保持系統及軟件更新。工作需要下載個人資料時，使用者須保護本機副本，並在用途完成後刪除。經私人即時通訊收到的個人資料，如須保留為正式紀錄，應轉存至總會指定位置並清理多餘副本。
3. 總會須備份重要會務、財務、會員及賽事紀錄，限制備份存取權限，並測試能否復原。賽事報名及賽果管理人員須在關鍵階段確認資料可供授權人員取用及復原。

4. 資訊安全事故處理

步驟	處理要求
通報	發現誤寄、公開分享、裝置遺失、可疑登入或帳戶遭盜用時，立即向指定資訊安全負責人報告。涉及個人資料，同時通知私隱負責人。
控制及保全紀錄	視情況撤回分享連結、暫停帳戶、終止可疑登入或隔離裝置，並保留相關電郵、截圖及系統紀錄。
評估及通知	確認事故涉及的資料、受影響人士及可能損害。總會須記錄是否通知受影響人士、私隱專員公署及其他相關機構的決定。決定通報後，應盡快進行。
復原及跟進	確認系統安全後恢復服務，記錄事故成因、補救措施及負責人，並覆核相關權限或流程。