X-FORT

ISO 27001:2022 實務說明

防止資訊外洩是防止和偵測個人或系統，在未經授權狀況下資訊被揭露和存取的過程。對於處理、儲存或傳輸敏感資訊的系統、網路和任何其他設備，採取相對應預防控制措施，包含 Data Leakage Prevention 與 User Activity Monitoring 等。

對照 ISO 27002 控制措施與 X-FORT 控管

透過 X-FORT 控制措施，讓 ISO 27001 的導入能更事半功倍。

編號	ISO 27002 控制措施	X-FORT 功能說明
5.12	資訊之分類與分級 Classification of Information	• 在各種行為出口前，對檔案內容進行過濾，對有疑慮之檔案予以阻擋
5.13	資訊之標示 Labelling of Information	• 出口放行，備份檔案加註分類標籤
5.14	資訊傳送 Information Transfer	• 管控與備份寫出至外接式儲存媒體，包含禁用、唯讀、寫出明文/密文檔案 • 管控與記錄各種網路行為，包含網頁瀏覽、即時通訊軟體、郵件 • 限制檔案傳送的目的地，如雲端硬碟、網頁、即時通訊軟體等
5.15	存取控制 Access Control	• 限制存取外接式儲存媒體、MTP裝置、印表機、光碟、藍牙等 • 禁止使用非授權應用程式 • 限制存取內部伺服器、無線基地台，原則禁止、例外允許
6.7	遠端工作 Remote Working	• 遠端連入工作環境，套用專屬安全政策，限縮使用權限 • 使用私人電腦RDP連入受控電腦時，限制遠端連線分享本機資源 (如：RDP分享本機磁碟)
8.1	使用者端點裝置 User Endpoint Devices	• 管理端點電腦連接周邊裝置、網路行為 • 避免私人裝置，透過網芳或其他通訊協定(如：MTP)帶走資料 • 管理用戶端的本機帳號管理，可新增、修改、刪除本機帳號，亦可啟用或停用本機帳號
8.7	防範惡意軟體 Protection Against Malware	• 禁用未經授權的軟體 • 管理電腦Windows Hotfix安裝現況，執行Hotfix安裝/移除 • 資料夾存取控制，限制電腦中特定資料夾內的檔案只能被「指定程式」存取，確保資料夾內的資料，不被其他非允許的程式存取
8.12	資料洩漏預防 Data Leakage Prevention	• 監控資料外洩管道，包含外接式儲存媒體、行動裝置、檔案傳輸、電子郵件、通訊軟體等 • 檔案出口端進行內容過濾，未包含關鍵字內容予以放行 • 針對特定應用程式，禁止複製到剪貼簿、滑鼠拖曳資料、螢幕截圖，記錄與備份上傳檔案 • 線上主管審核機制，審查檔案傳送
8.15	存錄 Logging	• 記錄各式使用者操作，包含事件、日期、電腦名稱、IP、使用者等 • 違規事件發送警示通知管理者與用戶端 • 僅系統稽核員可查詢記錄及審視權限內容，但不能變更任何記錄與設定
8.16	監視活動 Monitoring Activities	• 使用應用程式、裝置控管黑白名單 • 使用儀表板監看各種行為記錄，快速找出異常行為 • 透過偵測監視和記錄端點活動，檢測可疑行為、評量安全風險，自動回應切換控管政策
8.23	網頁過濾 Web Filtering	• 禁止瀏覽指定HTTP/HTTPS網址 • 監測網路流量，超過流量時警示管理者 • 限制檔案上傳至網站
8.24	密碼技術之使用 Use of Cryptography	• 寫出檔案至外接式儲存媒體，自動加密保護 • File Locker將完整資料內容加密保護，無論編輯、複製或保存，確保始終對特定資料夾中檔案維持加密狀態