遠距工作資安防護管控

因應疫情衝擊，許多企業減少出差與大型活動，除實體辦公室人員需分區、分組、分流辦公，部分員工居家遠距辦公等措施降低衝擊，但也帶來新的資安危機。由於遠距辦公時，使用的網路環境及電腦設備，已非平常組織所建置安全保護網之下；甚至使用非公司的制式配備。

調整控管建議

- 多層存取：導入跳板機制，外部遠端連線僅限連入組織的中繼主機，並強化身份認證
- 網路監控機制：啟動連線存取記錄、連線活動記錄、辦公區操作記錄、上網行為記錄
- 限制存取連結裝置：限制遠端連線分享本機資源、防止外流到遠端存取設備 (如：RDP 分享本機磁碟)

Case 1　使用安裝 X-FORT 設備遠距工作

- 使用 VPN：直接存取公司內部環境與服務，如同在公司內工作。連入時依網段不同，套用 X-FORT 專屬政策。
- 未連 VPN：X-FORT 自動切換成離線政策，如通訊埠控管，只允許連結 VPN 通訊埠。

Case2　使用私人電腦，連結安裝 X-FORT 設備

- 使用 RDP 連線：限制使用 RDP 遠端桌面工具存取內部資源。中繼電腦須安裝 X-FORT，政策與平時工作相同。
- 使用 VDI：X-FORT 自動啟動使用者工作階段防護，政策與平時工作相同。

X-FORT 擁有多項活動監視及存取控管手段，適用遠距工作架構變化，不論內外一起保護。

模組	說明	Case1	Case2
儲存裝置控管	● 外接式儲存裝置防護，控管包含禁用、唯讀、寫出加密、寫出明文等	⊘ ✓ 🕓 💾	⊘
光碟裝置控管	● 禁用燒錄軟體	✓	⊘
列印裝置控管	● 控管本機、網路、分享及虛擬印表機	⊘ ✓	✓
操作記錄	● 軟體執行記錄：執行軟體，或軟體視窗標題名稱變動時，記錄活動內容 ● 網頁瀏覽記錄：當瀏覽器視窗標題變動時，記錄視窗標題名稱與網址 ● 檔案操作記錄：檔案總管對檔案的操作，包含本機、網路芳鄰、外接式儲存裝置等；建立、刪除、更名、移動、複製檔案，掛載、移除磁碟機	🕓	🕓
進階操作記錄	● 記錄使用者複製/貼上剪貼簿的文字內容	🕓	🕓
共用資料夾控管	● 詳實記錄/備份網路芳鄰寫出/寫入檔案	⊘ ✓ 🕓 💾	⊘
通訊控管	● 允許/禁止使用的通訊埠，限定使用VPN通訊埠	✓ 🕓	⊘ ✓ 🕓
傳輸控管	● 即時通訊軟體可禁止執行、禁止傳檔；記錄傳訊內容、備份傳送檔案	🕓 💾	🕓 💾
軟體安控	● 禁用遠端連線軟體	⊘	⊘
特殊軟體安控	● 管制特定功能， 禁止列印/複製到剪貼簿/鍵盤/另存新檔/滑鼠拖曳資料 ● 執行特定軟體時，啟用螢幕浮水印	✓	✓
畫面擷取	● 擷取視窗切換、使用剪貼簿、Microsoft Office操作時的畫面 ● 執行特定軟體(如啟用VPN Client)、網頁清單時，固定間隔連續擷取	🕓 💾	🕓 💾

⊘禁止 / ✓控管 / 🕓記錄 / 💾備份