居家辦公期間資安防護建議事項

類別	建議事項
居家辦公	**居家辦公前準備:** ☐ 辦公室電腦設備準備： • 進行資料備份等事前準備。 • 無法攜回家之設備、主機相關辦公用品應集中放置管理，避免遺失。 • 加強使用者個人密碼強化，不可使用弱密碼，且建議使用雙因子驗證(若有支援)。 ☐ 居家辦公使用之 PC 或設備整備 • 安裝本院 VPN 軟體，並完成帳號的開通與測試。 • 安裝防毒軟體並更新病毒碼至最新版本。 • 檢查作業系統的安全性更新，並完成更新到最新版本。 • 安裝本院已購置授權之端點防護軟體 (Xensor) 。 • 確認各項軟體使用是否為合法授權。 **居家辦公期間注意事項:** ☐ 以 VPN 連回院內使用本院系統。 ☐ 公務資料可存放在本院 MySpace 空間，避免存放在外部雲端空間。 ☐ 請勿將帳號、密碼記錄於書面或張貼於容易洩漏之處(例如以便條紙書寫個人帳號與密碼貼於電腦螢幕上) 。 ☐ 離開座位應將螢幕鎖定。 ☐ 保持作業系統與防毒軟體更新到最新版本。 ☐ 完成收發信軟體安全性設定(操作方式詳情)。 ☐ 收發信件時，注意防範新冠肺炎社交工程郵件，收到疑似社交工程郵件請循資訊處提供之回報流程。 **居家辦公結束後注意事項:** ☐ 攜回家裡辦公用的文件與設備應全數移回。 ☐ 居家辦公使用之私人 PC 所存放之公務資料需全部清除。 ☐ 若無 VPN 使用需求，可申請取消 VPN 服務。
視訊會議	**與會者:** ☐ 從官方網站下載軟體，並保持應用程式的更新與修補。 ☐ 不要使用 Facebook 帳號及 Google 帳號(Hangouts Meet 除外)的認證方式登入。 ☐ 在自己的電腦，另外開一個只有一般權限的使用者帳號，不給任何 admin 的權限，然後用那個只有一般權限的使用者帳號去參加會議，等會議結束後，刪除該帳號。 ☐ 請勿在會議期間分享機敏資料並避免討論機密議題以防止外洩。 **召集者:** ☐ 視訊會議應全程開啟「點對點加密」(end-to-end encryption) 功能。 ☐ 務必設立高強度的會議密碼與主持人密碼(最好是每場會議都不一樣，且要注意密碼的強度，若有支援，建議密碼至少 8 碼以上，含英數字及英文大小寫，含特殊符號更佳)，且須清點是否有不明人士進入，並依會議屬性適時進行會議鎖定動作。 ☐ 會議室連結與密碼不應以同一封信寄出，若為重要的會議，密碼應該採行其他種方法告知（例如電話通知等）。 ☐ 只向與會者分享會議 ID 和網址。切勿將其分享到社交媒體或公開的網路平台。 ☐ 設定分享螢幕至 「Only Host」，並只在有需要時才開放此功能給與會者。
社交工程攻擊	**注意防範疫情相關社交工程攻擊電子郵件**，例如: 1.聲稱官方釋放之最新消息/冒充政府紓困通知/假冒專家防疫建議/以衛生機構名義詐騙/偽造各企業防疫最新消息。 2.竄改正版 COVID-19 資訊圖。 **避免新冠病毒網路釣魚的方法，可參考以下建議:** 1. 對於來路不明的郵件/社群媒體訊息保持警覺，就算看似來自著名組織或認識的聯絡人也不例外。 2. 收到來路不明的電子郵件，切勿點選信件內的連結/按鈕或下載任何附件。 3. 若該電子郵件要求提供個人資料，直接向寄件者確認，不要點選郵件內容或輸入資料。 4. 向各單位資安人員確認，偵測並封鎖垃圾郵件，封鎖惡意下載內容及網站。 5. 停用 Office 檔案中的巨集 – 駭客經常利用巨集來執行惡意軟體。