【政風宣導-公務機密宣導】AI 與雲端時代的保密防諜觀念

廉政檢舉專線：0800-286-586

「保密防諜、人人有責」這句標語，過去常見於校園、軍營及公共場所。在早期兩岸情勢緊張年代，保密防諜主要著重於實體文件、軍事情資與人員滲透。然而，隨著網際網路、智慧型手機及人工智慧（AI）快速發展，現今的機密外洩方式已與過去大不相同，資安威脅更從傳統間諜行為，演變為網路攻擊、社交工程、資料竊取與 AI 資訊外流等新型態風險。

過去電影中的情報員，可能需要透過特殊照相設備、暗號或秘密接頭來傳遞情報；但在現代科技環境下，一支智慧型手機、一台平板電腦，甚至一個雲端帳號，即可能成為資料外洩的媒介。現今文件多已數位化，資料傳輸速度極快，只需透過電子郵件、即時通訊軟體、社群平台或雲端空間，即可能在短時間內大量傳送敏感資訊，造成難以彌補的損害。

尤其近年生成式 AI 工具盛行，許多民眾與企業習慣利用 AI 協助撰寫文件、整理資料與分析內容。然而，若將尚未公開的公務資料、個資、標案內容、內部會議紀錄或機敏文件直接輸入 AI 平台，便可能產生資訊外洩風險。因此，使用 AI 工具時，應遵守機關資訊安全規範，不得任意上傳涉密資料或公務資訊，以維護機關及民眾權益。

目前常見的資訊外洩管道，包括：

一、即時通訊軟體

現代人普遍使用 LINE、WhatsApp、Messenger、Telegram 等通訊軟體進行聯繫，雖然提高溝通效率，但若透過私人群組傳送公務文件、帳號密碼或敏感資料，可能因帳號遭盜用、設備遺失或群組管理不當而導致資料外流。因此，公務資料應依規定使用安全且經核可之通訊平台傳遞。

二、電子郵件與網路釣魚

駭客常利用假冒政府機關、銀行或熟人名義寄送釣魚郵件，誘導使用者點擊不明連結或下載惡意附件。一旦點擊，可能造成帳號遭竊、電腦中毒或內部資料被竊取。對於來路不明郵件，應提高警覺，並避免開啟可疑檔案。

三、雲端儲存與檔案共享

雲端硬碟與線上文件雖方便協作，但若權限設定不當，可能導致資料遭未授權人員存取。使用 Google Drive、Dropbox、OneDrive 等雲端服務時，應確認分享對象與權限設定，避免將機敏資料設為公開。

四、USB與可攜式設備

隨身碟、行動硬碟及個人裝置仍是資料外流的重要媒介。部分惡意程式甚至會透過USB裝置進行感染，因此，不應任意使用來源不明之儲存裝置，並應依規定執行掃毒與資料管制作業。

五、社群媒體與公開資訊

許多人習慣於 Facebook、Instagram、Threads 等社群平台分享工作日常或照片，但若不慎拍攝到公文、電腦畫面、門禁資訊或辦公環境配置，也可能成為有心人士蒐集資訊的來源。因此，於社群平台發文時，應留意是否涉及公務機密或敏感資訊。

六、遠端辦公與公共網路

近年遠距辦公逐漸普及，部分人員會在咖啡廳、公共場所使用免費 Wi-Fi 處理公務，但公共網路存在較高資安風險，容易遭攔截或竊取資料。處理公務時，應優先使用安全網路環境及 VPN 等保護措施。

為強化資訊安全與機密維護，政府機關與企業除建置防火牆、防毒系統、多因素驗證(MFA)及資安監控機制外，也持續加強員工資安教育訓練，提升對網路攻擊與假訊息的辨識能力。

此外，民眾亦應建立正確資安觀念，包括：

- 不任意點擊不明連結。
- 定期更新密碼並啟用雙重驗證。
- 不使用未授權軟體。
- 不隨意分享個人或公務資訊。
- 發現異常時立即通報資訊單位。

在數位與 AI 科技快速發展的時代，資訊安全已不只是政府或資訊人員的責任，而是每一位使用科技設備者都應重視的重要課題。唯有提高保密意識與資安警覺，才能有效防止機密外洩，共同維護國家安全、機關信譽及民眾權益。

資料來源：綜整數位資安與資訊安全觀念編修 AI

115.06.

新北市八里區公所政風室