# 法務部及所屬機關資訊安全作業基本認知　97.03.26

## 一、 資訊安全政策

■ 資訊安全方針：資訊安全，人人有責。

■ 資訊安全目標

- 非法存取資訊之事件，各機關每年發生次數不得超過5次。
- 因資安事件導致服務停頓，各機關每半年小於3次(含)以下，每次不得超過36小時。
- 每年至少需執行2次「營運持續管理計畫」之情境演練，並於2年內完成計畫內所有情境之演練。所屬機關每年至少執行1次演練。
- 每人每年至少應接受3小時以上的資訊安全教育訓練。
- 本部每年至少進行2次內部稽核。所屬機關則每年至少進行1次內部稽核。

## 二、 資訊設備使用

■ 應設定螢幕保護程式(須設定開機密碼，時間最長不得超過20分鐘)或是其他控制措施保護；離開座位致所使用資訊設備有遭入侵之虞者，應於離開前將螢幕鎖定。

■ 可攜式設備及媒體（如筆記型電腦、行動硬碟、隨身碟等）應妥為保管，非因公務需要不得攜出辦公處所，攜回時應進行掃毒或系統還原。

■ 因處理業務保有敏感性、機密性電腦資料或檔案者，應加強安全保護措施，如下班時應該上鎖或以其他方法妥為收存。

■ 定期備份個人重要檔案。

## 三、 電腦軟體使用

■ 個人電腦原則僅安裝業務所需軟體，安裝前應確認取得合法授權。

■ 不得將授權軟體轉借或給予未經授權人員使用。

■ 使用私有、免費或共享軟體時應考量系統安全性，避免危及本部電腦或網路的安全。

■ 如發現使用非授權的軟體，由使用者自行負相關法律責任。

■ 軟體版權基本認知：

- 版權軟體：非取得版權不得安裝使用。
- 共享軟體(Shareware)：可因測試之目的進行安裝及試用，但應於試用到期時立即移除。
- 免費軟體(Freeware)：可免費下載、安裝使用，但仍受著作權法之保護，且亦受著作權人所定之條件限制，不得用於謀利。
- 自由軟體(Free Software)：鼓勵複製、散佈，允許研究、改良。英文中的 Free 代表的是自由軟體可自由傳遞的開放性，而非成本上的「免費」。
- 公開軟體(Public Domain)：著作權已因放棄而消滅，無任何限制。

## 四、 網路使用

■ 不得任意更改個人電腦IP 位址與網路卡。

■ 個人電腦不得安裝數據機或架設無線網路等相關對外連線設備。

■ 非經本部同意不得自行與外界網路相連結；未經核准不得於本部網路私自架設網站。

■ 不得在上班時段利用網路收聽音樂、廣播等，或使用MSN或SKYPE等軟體進行視訊、語音交談等，避免浪費網路頻寬，影響正常業務運作。

■ 除因公務需要且經本部核可外，不得使用點對點（Peer-to-Peer, P2P）分享軟體。

■ 機密檔案不得在網路上傳送。

## 五、 密碼管理

■ 不得將識別碼或密碼張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。

■ 所配發之使用者識別碼及密碼，應妥善保管，不得交付他人使用。

■ 密碼設定最少應由8位英數字組成，最好包含特殊字元，並避免使用與個人有關資料（如生日、身份證字號、單位簡稱、電話號碼等）。

■ 密碼應最少每六個月更換一次。

## 六、 病毒及駭客防範

■ 個人電腦(筆記型電腦、伺服器)應關閉USB儲存裝置自動執行設定(Auto Run)，以防駭客藉由USB儲存裝置植入後門程式。

■ 隨時注意個人電腦防毒軟體之病毒碼是否為最新版本（日期最長不得超過一週，如有問題立即連絡機關資訊人員）。

■ 不得利用SKYPE 等軟體進行檔案傳送，避免成為病毒入侵途徑。

■ 取消郵件預覽，預設為純文字讀取模式，不明來路之電子郵件不宜打開，不隨意開啟或下載附件，以避免木馬或病毒植入。

■ 非必要不設定自動傳送電子郵件之讀取回條。

## 七、 防範電子郵件社交工程的小提示

■ 注意可疑電子郵件之特徵：過於聳動的主旨與緊急要求、不正常的發信時間、陌生人或少往來對象來信、認識的人來信但主旨或內容與其習性不符、要求輸入私密資料送出等。

■ 可疑電子郵件之自我保護措施

- 非必要閱讀之郵件逕行刪除。
- 於該信件按滑鼠右建，或點選【郵件選項】(Outlook)確任發信者電子郵件帳號，惟發信者電子郵件帳號仍有被偽冒的機率，必要時直接與寄信者連絡確認是否來信。
- 設定為純文字讀取模式再開啟郵件閱讀。
- 開啟郵件內含之超連結時先確認連線網址之網域名稱(Domain Name)是否足以識別？若為數字IP之網址勿輕易開啟。
- 不隨意輸入資料送出，傳送私密資料時確認是否有啟動加密機制。