法務部及所屬機關資訊安全作業基本認知

一、 資訊安全政策

■ 對民眾承諾因公務蒐集取得之個人資料，依個資法規定保障隱私、依法使用，並強化各項資訊安全管控措施，以確保資料安全；對內部同仁要求遵守各項資訊安全規定，並落實「資訊安全，人人有責」之資訊安全方針。

二、 資訊安全方針：資訊安全，人人有責。

三、 資訊安全目標

■ 核心資通系統因資安事故導致之服務中斷時數，不得超過年度總運作時數之 0.1%。

■ 每年電子郵件社交工程演練之郵件開啟率：
-機關電子郵件帳號數大於 20 者：郵件開啟率年度平均數不得高於 5%。
-機關電子郵件帳號數 20 以下者：每次演練之郵件開啟人數不得超過 1 人。

■ 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。

四、 資訊設備使用

■ 辦公環境內必須使用機關提供之資訊設備、網路，及規定之軟體，非經核准，不得使用個人私有設備及中國廠牌產品，公務設備亦不得連結個人私有手機上網。

■ 個人電腦應設定螢幕保護程式，等候啟動時間不得超過二十分鐘，且須以密碼保護；另離開座位前應將螢幕鎖定。

■ 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，下班時應將電腦之電源關閉，以維護資訊及用電安全。

五、 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。

■ 為避免公務機敏資料被不當竊取，個人電腦非經核准，不可安裝非公務用軟體，包括即時通訊軟體(如 Line 等)。如因業務需要簽奉機關首長核准使用即時通訊軟體，應遵循以下注意事項：
- 不得使用即時通訊軟體傳輸公務機密、涉及資訊安全及個人隱私之事項，或其他非機密，但若不當公開或外洩，可能造成決策困擾、個人或機關信譽非必要損害等負面效應之事項。
- 未確認傳遞者身分及訊息內容真實性前，不隨意點選訊息內超連結，以免落入釣魚、惡意或高風險網站陷阱。

六、 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；未經核准不得於內部網路私自架設網站。

■ 上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站；且不得在上班時段利用網路收聽音樂、廣播等，或使用即時通訊等軟體進行非公務視訊、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。

■ 傳送公務資訊應有適當保護，如加密傳送；機密檔案不得在網路上傳送。

七、 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，如有外洩疑慮，除儘速更換密碼外，並應通知資安窗口。

■ 密碼設定最少應由 8 位英文字、阿拉伯數字、英文字大小寫、特殊符號，以上四取三項之複雜性原則組成，並避免使用與個人有關資料（如生日、身分證字號、單位簡稱、電話號碼等）。

■ 密碼應最少每六個月更換一次。

八、 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）。

■ 公務資料傳遞及聯繫應使用公務電子郵件帳號；且不得使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。

九、 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

- 取消郵件預覽，不明來路之電子郵件不隨意開啟或下載附件，以避免木馬或病毒植入，非必要閱讀之郵件逕行刪除。
- 確認發信者電子郵件帳號，若使用 Outlook 2010 以後版本，請先將【郵件選項】功能新增至「快速存取工具列」上（可請貴機關單位資訊主兼辦同仁協助），以滑鼠左鍵選取該信件後，點選快速存取工具列之【郵件選項】，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。
- 非必要不設定自動傳送電子郵件之讀取回條、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。

■ 雲端郵件軟體、行動裝置種類繁多且更版快速，安全性設定方式互異（如 Thunderbird、iOS 郵件軟體之「隱私權保護」等），應留意並落實所用軟體、裝置相關安全設定。

十、 事件通報

■ 如有發現資安疑慮或異常時，應即時通報資安窗口。

十一、資訊安全法遵事項及規定

■ 應遵守個人資料保護法、資通安全管理法及機關資訊安全行政規則等規定(資安訊息位址：法務部內部網站/資通安全/資訊安全行政規則)。

■ 未遵守機關資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。