



商工行政服務e網通系統
資訊安全宣導

ISMS-B07-P02

版本：3.00

機密等級：■一般 □敏感 □密

經濟部商業司

生效日期：中華民國 104 年 01 月 12 日



【文件修訂記錄】

制／修定版本	生效日期	制／修定摘要說明	備註
V1.01	96/08/01	新擬訂文件	
V1.02	96/10/01	改版同步發行	
V1.03	97/12/23	更新電腦使用須知內容	
V2.00	99/08/06	依據內稽建議更新並統一文件版本。	
<u>V3.00</u>	<u>104/01/12</u>	修訂軟體使用之安全管理規範	



一、說明

為提醒員工隨時注意資訊安全並養成安全習慣，以維護個人、客戶及本公司資訊業務相關安全作業，特整理資訊安全相關注意事項，以為宣導。

二、資訊安全責任

資訊安全，人人有責。組織如同一條鍊子，人人皆是鍊子的一環，鍊子的強度取決於其中最弱的一環。人人皆應自我警惕，以維護整體安全強度。

本項資訊安全宣導所涵蓋之相關成員，應至少每半年填寫「ISMS-B07-P03 個人資訊安全檢查表」進行自我檢查。

三、資訊安全要求

（一）法規上的要求

1. 個人資料具有私密性且受法律保護，不可非法隨意查閱或揭露他人個人資料。
2. 提供大眾之公開資訊，須具備完整性，組織並應負資訊錯誤之連帶損害責任。
3. 個人創作及資訊軟體等智慧財產權受法律之保護，不得非法任意使用或引用。
4. 如需使用或複製軟體，需經確認授權問題無違法及安全疑慮後方可安裝及使用。
5. 軟體安裝及使用之權利及義務、須依著作權法及有關議定之契約內容辦理。
6. 安裝使用、複製及修改電腦軟體，應依著作權法相關規定辦理，且嚴禁安裝使用任何非法或未經核准之軟體。
7. 取得軟體公司授權後才可安裝使用其電腦軟體，除非獲得軟體商之許可



或用於光碟備份之用途，否則無權加以複製。

8. 在用戶端、伺服器與網路應用程式方面，應符合授權契約條款使用軟體。

(二) 辦公環境安全：

1. 確保重要文件及其儲存媒體（紙張、隨身碟、磁片、光碟片等）受到應有之保護。
2. 確保不用之紙張文件或報表採取必要的銷毀或廢棄程序。
3. 確保本司資訊設備在無人看管或下班時採取適當之安全保護。

(三) 電腦使用須知

1. 電腦、業務系統或自然人憑證，若超過 30 分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 電腦若疑似受駭時，應立即拔除網路線，停止網路行為並向本部熱線服務通報。
3. 受駭電腦重整後，應立即變更曾於該受駭電腦登入之所有系統密碼(如部內服務網、電子郵件系統、自然人憑證等)。
4. 禁止私自安裝點對點檔案分享軟體(Peer-to-Peer 簡稱 P2P)及未經合法授權軟體
5. 連網電腦應隨時配合更新作業系統，應用程式漏洞修補程式及防毒病毒碼等。
6. 筆記型電腦應定期上網以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
7. 應變更管理者（Windows Administrator）密碼。
8. 應關閉 IE 瀏覽器記憶密碼功能。



9. 下班時應關閉電腦及螢幕電源。
10. 如發現資安問題，請主動向本部熱線服務專線：666 通報。

(四) 網際網路使用須知

1. 禁止於辦公室內私裝電腦及網路通訊等相關設備。
2. 禁止使用網路芳鄰共享資料夾。
3. 不隨意下載或安裝不明軟體。
4. 連網電腦禁止瀏覽非法或不當之網站。
5. 應將經常性必要瀏覽之網站設定成我的最愛。
6. 應考量安全性網站以進行必要之網路交易或登錄註冊。
7. 因業務特性需上網瀏覽大陸網站者，須經單位主管核可後，向本部資訊中心提出申請後使用。
8. 機敏場所如非業務需要，禁止安裝網路攝影機等視訊會議設備。

(五) 實體隔離作業須知

1. 處理密級以上或各單位認定需保護之敏感性資料(以下簡稱機敏資料)時，須使用專屬實體隔離電腦設備處理及列印。
2. 儲存機敏資料之專屬隨身碟、磁片等儲存媒體須上鎖保管，並僅限於實體隔離電腦讀取、繕打及列印。
3. 實體隔離電腦不得私自連接網路並不得與上網電腦共用印表機。
4. 實體隔離電腦製妥之文件如需網路傳輸或從連網電腦下載文件複製至隔離電腦使用時，須先將文件複製至隨身碟、磁片等儲存媒體，再移至目的電腦。此等儲存媒體僅當作兩部電腦間檔案傳送之「載具」，使用前、後應以格式化方式刪除所有檔案。



(六) 電子郵件使用須知

1. 本部預設之垃圾電子郵件過濾機制，勿擅自刪除。
2. 電子郵件收發軟體(如本部 Web 版電子郵件系統、Microsoft Outlook 或 Outlook express)之「預覽窗格」及「下載圖片」功能應取消。
3. 非公務相關電子郵件及其附檔(含 Word、網頁連結、圖檔等)請勿開啟，並立即刪除不明郵件。
4. 可疑郵件須先求證後方可開啟。
5. 不得假冒單位內外其他人員的電子郵件帳號。
6. 電子郵件社交工程演練不合格同仁，須依規定接受本部安排之資安訓練。

(七) 資料保護須知

1. 機敏資料須加密後儲存於實體隔離電腦、隨身碟或磁片等，不可存放於連網電腦。
2. 密級以上資料須以國安單位認可之加密機制於實體隔離電腦加密後，方可透過網路傳送。
3. 敏感性資料須於實體隔離電腦啟動其編輯軟體設定密碼保護功能後，方可透過網路傳送。
4. 密碼長度至少須 12 碼(採文數字、特殊符號混合使用原則)且不得採用電腦自動記憶方式、明文書寫、張貼或交予他人使用。
5. 使用隨身碟或磁片等存放資料時，機敏資料及一般資料應分開儲存，不得混用並妥善保管。
6. 禁止在家中等辦公室以外場所使用連線電腦處理機敏公務。
7. 各項重要業務資料均應妥善定期備份，並經檢視以確保備份資料之可用性。