

壹、目的

外交部領事事務局（以下簡稱本局）之主要業務為提供護照核發、簽證及文件證明等各項服務，是外交部為民服務工作的窗口，對於提供服務之資訊系統，特別著重於機密性、完整性及可用性之保護，因此期望透過本政策之制定，做為資訊安全工作之指導方針。

貳、範圍

資訊安全政策涉及之範圍如下：

- 一、資訊作業使用之相關設備與資產，例如資料庫及各項設備、資訊服務作業流程中之書面文件及電子紀錄等。
- 二、本局所有員工、聘僱人員以及承包本局各項作業之廠商。
- 三、使用本局設備或資料之其它機關人員。

參、權責

本政策由資訊安全委員會通過後施行，每半年評估檢討一次。

肆、要求事項

一、資訊安全聲明

機密資料保護好，完整正確不可少，持續服務為首要，永永遠遠沒煩惱。

二、資訊安全責任及組織

- （一）本局設置資訊安全委員會，負責資訊安全管理系統相關事項之計畫、執行及協調溝通，由副局長擔任主席，各單位主管為委員會之成員。
- （二）資訊安全委員會下設資訊安全防護暨作業組及資訊安全稽核組，資訊安全防護暨作業組負責執行本局資訊安全例行作業；資訊安全稽核組負責評估本局資訊安全管理制度之落實與遵行情形。
- （三）資訊安全防護暨作業組設資訊安全執行秘書一人，以及副執行秘書一人，除協助推動資訊安全委員會決議事項外，並負責督導資訊安全防護暨作業組，對本局資訊安全狀況進行預警及監控，並依資訊安全委員會的授權對資訊安全狀況與事件進行處置。
- （四）本局員工之資訊安全職責在工作職位說明書中明確描述，對各工作角色須符合適當的權責區分，基於本局運作之需要，所負責之各項工作應訂定該項工作之代理人。
- （五）有關資訊安全組織的細部設計及運作方式，另訂於「資訊安全組織作業程序」。

三、資訊資產分類分級

- （一）本局之資訊資產應指派其保管者及使用者，並依照資訊資產分類分

級作業程序維持資訊資產清冊的正確性。

- (二) 本局資訊資產分為電子類資產、文件類資產、軟體類資產、硬體類資產、服務類資產及人員類資產等六類，並依據資訊資產清冊之分級制定管理方式。
- (三) 有關各類別的資訊資產管理原則另訂於「資訊資產分類分級作業程序」。

四、存取控管及委外管理

- (一) 應針對使用者所能存取的資料、程式、系統、網路及實體區域環境設定存取與進出權限，存取權限之開放依據員工職務所需最少資訊為原則，人員若有職位變動立即變更其存取權限。
- (二) 為確保存取權限之適當及有效性，各單位主管應定期覆核其員工之存取權限。
- (三) 為提高委外作業之安全性，採購契約中應明訂建置或維護廠商需簽署保密協議書，審慎開放專案人員或駐點人員之權限，並建立名冊管理之。
- (四) 有關資訊系統存取及委外作業之安全管理原則，另訂於「護照製發管理系統存取安全控制作業程序」及「委外安全管理作業程序」。

五、風險評估及風險管理

- (一) 應建立風險評估及管理之機制，並識別所面臨之風險，決定應採行動。
- (二) 本局營運組織或營運環境變遷致作業程序有重大變更時，應重新進行風險評估及風險管理作業。
- (三) 有關風險評估及風險管理之要求，另訂於「資訊安全風險評估暨風險管理作業程序」。

六、實體安全

- (一) 本局應採取適當的門禁管制，以防止對本局之資訊資產不當存取或造成損害，重要的資訊處理設施（如傳真機、影印機、主機電腦等）應設置於有適切門禁管制之場所。
- (二) 辦公區域及機房應置放適當之消防滅火設備(如手提式滅火器、煙霧偵測器等)。
- (三) 個人電腦或伺服器應設定螢幕保護程式及密碼保護，並於電腦暫時無人使用時啟動螢幕保護程式。
- (四) 業務承辦人於列印、影印或接收密級或具敏感性資料時，於接獲通知或列印完畢後，立即取走該資料。

- (五) 有關實體安全之細部要求，另訂於「機房環境安全作業程序」及「辦公環境安全作業程序」。

七、網路安全

- (一) 本局應採取適當的網路防護措施，以防止本局之電腦系統遭受不當存取或損害，重要之主機系統與網路設備應有適切之防護措施。
- (二) 網路設備安裝、維護時，設備密碼不得交予維護廠商，如須輸入密碼，應由管理者輸入後方可操作。
- (三) 如欲使用本局之網路資源，應填具申請單，經核可後送交資訊小組處理。
- (四) 使用者不得私自安裝數據機或無線網路，如有特殊需求須提出申請。
- (五) 有關網路安全及之具體要求，另訂於「網路安全管理作業程序」。

八、系統開發與變更

- (一) 本局對於資訊系統之新增及變更，應有適當之測試確認其設計滿足本局資訊安全之要求，並經適當層級的人員核准後上線。
- (二) 系統開發須於測試環境進行，測試環境應與線上環境隔離，測試用的資料如含有個人資訊，其存取紀錄應予以監控。
- (三) 有關系統開發之具體要求，另訂於「系統開發維護操作變更作業程序」。

九、病毒及惡意軟體之防護

- (一) 本局之電腦系統須建置防範電腦病毒及惡意軟體之機制，並依照規定更新電腦病毒碼與系統漏洞。
- (二) 除了本局所核准並經合法授權之系統及應用軟體外，禁止使用其它軟體，各單位主管應確保所屬之電腦系統是否合於規定並定期清查。
- (三) 對來路不明的電子郵件或檔案，應立刻刪除，不宜隨意打開電子郵件。
- (四) 使用者如發現電腦病毒入侵或系統異常，應立即通報予資通安全防护暨作業組。
- (五) 有關病毒及惡意軟體防治之具體要求，另訂於「電子郵件及電腦病毒控制作業程序」。

十、人事安全及訓練

- (一) 本局所有人員有義務接受與職務相關之資訊安全教育訓練，以確保員工有足夠之資訊安全認知。

- (二) 人員進用時，應詳查其學歷、工作資格及身份證明文件。
- (三) 應不定期對人員或由第三者派駐在局內服務之人員，進行資訊安全教育訓練。
- (四) 有關人員進用及安全訓練，另訂於「人事安全管理作業程序」。

十一、個人電腦及儲存媒體使用

- (一) 本局之個人電腦及儲存媒體（如磁帶、磁片等）僅供員工處理公務使用，禁止非公務用途之使用。
- (二) 私人電腦設備因業務需要而攜至局內使用時，應填具申請單經權責主管審核後送至資訊小組執行。
- (三) 有關本局人員使用網路及個人電腦，另訂於「個人電腦及儲存媒體安全作業程序」。

十二、資訊安全事件通報及其它機關資訊交換處理

- (一) 若發現可能會對本局之資訊資產之機密性、完整性、可用性造成損害的事件應立即依照程序通報並研判發生原因、損害程度及可能影響範圍，採取適當之控制對策，降低其可能發生之風險。
- (二) 本局提供其它機關個人資料或軟體前，應建立適當控管機制（如簽署保密協定），如有任何異常狀況應立即通報至相關單位主管，以維護本局之權益。
- (三) 有關資訊安全事件通報及處理及其它機關資訊交換之具體執行步驟及要求，另訂於「資訊安全事件通報及危機處理作業程序」及「其它機關資訊交換作業程序」。

十三、營運持續管理

- (一) 應制定業務持續運作計劃，確保本局之服務能持續運作不受重大災難、人為破壞或設備故障的影響。
- (二) 業務持續運作計劃應定期進行演練，以確保計畫中所有人員皆熟悉在該計畫中所負責之工作內容及執行步驟。
- (三) 有關本局護照製發業務持續管理作業，另訂於「護照製發管理系統業務持續運作管理作業程序」。

十四、資訊安全稽核

- (一) 各單位應定期對資訊安全管理系統之實際運作進行自行評估，自行評估之結果應由資訊安全委員會複核。
- (二) 資訊安全稽核組或第三方稽核人員應依照本局對資訊安全管理的符合性及自行評估的有效性執行稽核。
- (三) 有關資訊安全稽核之細部要求另訂於「資訊安全稽核作業程序」。

十五、資訊安全管理審查

- (一) 資訊安全委員會須對本局資訊安全管理制度之完整性及有效性執行審查，以確保資訊安全管理制度達成本局資訊安全目標。
- (二) 有關審查項目及審查頻率，另訂於「資訊安全管理審查作業程序」。

十六、法規遵循及懲處

- (一) 本局人員須遵守資訊安全相關法令之規範，特別對於電腦處理個人資料保護法、智慧財產權、及電子簽章法的規定應嚴格遵守。
- (二) 本局員工均應依據相關之規定簽署相關資訊安全保密協議，以確保員工均了解遵循上述法令規範之義務。
- (三) 違反本局資訊安全政策相關規定之人員，視情節重大程度依相關人事規章議處，發生上述情節之個人所屬部門主管負有行政督導之連帶責任。