

內政部營建署城鄉發展分署

資訊安全政策

一般文件



編號：TCD-011002

版本：1.0

核准日期：九十二年十一月

核准文號：市資字第0921001388號

一、目的：

避免本分署資訊資產遭受內部、外部、故意或意外的威脅，確保資訊的機密性、完整性與可用性。

二、目標：

強化本分署資訊安全管理，建立安全及可信賴的電子化政府，確保資料、系統、設備及網路安全，保障民眾權益。

三、責任：

(一) 由本分署最高管理階層訂定及審查本政策。

(二) 由資訊安全管理者透過適當的標準、程序及控制措施以實施本政策。

(三) 本分署所有員工、委外服務廠商及第三方人員均需遵守程序以維護本政策之落實。

(四) 任何蓄意危及本分署資訊安全的活動，本分署將採取法律行動。

四、審查：

本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

五、政策：

(一) 為統籌資訊安全管理等事項之協調及推動，應成立跨部門之「資訊安全推動小組」，為本分署最高管理階層。

(二) 依下列分工原則，配賦有關單位及人員權責：

1. 資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由規劃資訊中心負責辦理。

2. 資料及資訊系統之安全需求研議、管理及保護等事項，由各業務單位負責辦理。

3. 資訊機密維護及安全稽核等事項，由政風室會同相關單位負責辦理。

(三) 人員管理及資訊安全教育訓練：

1. 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。各業務主管人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

2. 針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升資訊安全水準。

3. 負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

(四) 電腦系統安全管理：

1. 辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。

2. 對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

3. 依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。

4. 採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

5. 採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。

(五) 網路安全管理：

1. 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
2. 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。
3. 訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。
4. 為避免網路使用者不慎違反本分署相關網路安全規定，網路管理人員可考慮以相關網路技術以不干擾正常網路使用為原則下，主動管制違反本分署相關網路使用規定。

(六) 系統存取控制：

1. 訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。
2. 離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
3. 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼應定期更新。
4. 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

(七) 應用系統開發及維護安全管理：

1. 自行或委外開發系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。
2. 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。
3. 委託廠商建置及維護重要之軟硬體設施，應在本分署相關人員監督及陪同下始得為之。

(八) 資訊資產安全分級管理：

1. 建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。
2. 依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。

3. 已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

(九) 實體及環境安全管理：

1. 就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

(十) 業務永續運作計畫之規劃與管理：

1. 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

2. 建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

3. 依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資訊安全措施。

(十一) 資訊安全稽核：

1. 應就本分署業務性質確立稽核項目及範圍，並訂定相關之稽核計畫或作業程序。

2. 為使資訊安全政策能落實，應定期或不定期進行資訊安全內部及外部稽核作業。