桃園市政府資訊安全管理要點

中華民國 104 年 5 月 26 日府研資字第 1040133526 號函頒訂

一、桃園市政府（以下簡稱本府）為強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，保障民眾權益，特訂定本要點。

二、本要點適用於本府及所屬各機關(以下簡稱各機關)。

三、各機關應依有關法令，考量施政目標，進行資訊安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施，確保各機關資訊蒐集、處理、傳送、儲存及流通之安全。

四、前點所稱適當及充足之資訊安全措施，應綜合考量各項資訊資產之重要性及價值，以及因人為疏失、蓄意或自然災害等風險，致機關資訊資產遭不當使用、洩漏、竄改、破壞等情事，影響及危害機關業務之程度，採行與資訊資產價值相稱及具成本效益之管理、作業及技術等安全措施。

五、各機關應依實際業務需求，訂定機關資訊安全政策，並以書面、電子或其他方式告知所屬員工、連線作業之公私機構及提供資訊服務之廠商共同遵行。

六、各機關應就下列事項訂定資訊安全管理相關規定，並定期評估實施成效：

（一） 資訊安全組織。

（二） 資訊安全責任。

（三） 人員管理及資訊安全教育訓練。

（四） 電腦系統安全管理。

（五） 網路安全管理。

（六） 系統存取控制。

（七） 應用系統開發及維護安全管理。

（八） 資訊資產安全管理。

（九） 實體及環境安全管理。

（十） 業務永續運作計畫之規劃與管理。

(十一)資訊安全稽核。

七、各機關資訊安全分工、權責及組織相關規定如下：

（一） 資訊單位應負責推動、協調及督導機關資訊安全相關事宜；業務單位應督導所屬之資訊作業安全事宜。

（二） 資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。

（三） 資訊單位應成立跨單位資通安全處理小組，推動機關資訊安全作業。

（四） 資訊機密維護及稽核使用管理事項，由資訊單位及政風單位會同相關單位負責辦理；未設置資訊單位及政風單位者，由機關首長指定適當單位及人員負責辦理。

八、各機關人員資訊安全權責相關規定如下：

（一） 資通安全處理小組召集人：資訊安全政策、資訊重大計畫之核定及各項資訊業務推動之督導。

（二） 資訊業務承辦人：辦理資訊設備及應用系統管理維護，確保設備及應用系統正常運作，參加各式資安訓練、提升資安認知，配合及執行各種資安演練、資安事件通報及處理，並對所管理之機密性或敏感性資訊負有維護及保密之責。

（三） 資訊業務主管：各項資訊安全相關業務之審核，並對所經手之機密性或敏感性資訊負有維護及保密之責。

（四） 一般使用者：確實遵守本府資訊安全相關規定，正確合法使用網路、電子郵件、設備及系統等，對於被授與之權限、帳號密碼等負有保密之責。

九、各機關人員資訊安全管理及教育訓練相關規定如下：

（一） 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。

（二） 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。

（三） 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。

（四） 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。

十、各機關電腦系統安全管理相關規定如下：

（一） 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。

（二） 對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

（三） 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。

（四） 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。

（五） 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。

十一、各機關網路安全管理相關規定如下：

（一） 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。

（二） 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。

（三） 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。

十二、各機關系統存取控制相關規定如下：

（一） 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。

（二） 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。

（三） 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。

（四） 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。

十三、各機關應用系統開發及維護安全管理相關規定如下：

（一） 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。

（二） 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。

（三） 委託廠商建置及維護重要之軟硬體設施，應在各機關相關人員監督及陪同下始得為之。

十四、各機關資訊資產安全分級管理相關規定如下：

（一） 建立與資訊系統有關資訊資產目錄，訂定資訊資產項目、擁有者及安全等級分類等。

（二） 依據國家機密保護、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，以及相對應保護措施。

（三） 已列入安全等級分類之資訊及系統輸出資料，應標示適當安全等級以利使用者遵循。

十五、各機關應就設備安置、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。

十六、各機關業務永續運作計畫之規劃與管理相關規定如下：

（一） 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。

（二） 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。

（三） 建立資訊安全事件緊急處理機制，在發生資訊安全事件時，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，若有需求聯繫檢警調單位協助偵查。

（四） 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。

十七、各機關資訊安全稽核相關規定如下：

（一） 就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。

（二） 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。

（三） 設有資訊單位之一級機關對所屬機關資訊作業，應由資訊單位會同政風單位或相關稽核人員進行定期或不定期之資訊安全稽核。

十八、本要點未規定事項，依行政院及所屬各機關資訊安全管理要點之規定辦理。