行政院及所屬各機關資訊安全管理要點

行政院八十八年九月十五日台 88 經字第(34735)號函訂頒

壹、目的

一、行政院為推動各機關強化資訊安全管理，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。

貳、通則

二、本要點所稱各機關，指行政院及所屬各部、會、行、處、局、署、院、台灣省政府、台灣省諮議會及其所屬機關（構）。

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、本要點所稱適當及充足之資訊安全措施，應綜合考量各項資產之重要性與價值，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、各機關應就下列事項，訂定資訊安全計畫實施，並定期評估實施成效：

(一)資訊安全政策訂定。
(二)資訊安全權責分工。
(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)系統存取控制管理。
(七)系統發展及維護安全管理。
(八)資訊資產安全管理。
(九)實體及環境安全管理。
(十)業務永續運作計畫管理。
(十一)其他資訊安全管理事項。

六、本要點所稱資訊安全政策，指機關為達成資訊安全目標所訂定之資訊安全管理作業規定、措施、標準、規範及行為準則等。

參、資訊安全政策擬訂

七、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。

八、各機關訂定之資訊安全政策，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。

肆、組織及權責

九、各機關應依下列分工原則，配賦有關單位及人員之權責：

(一)資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。
(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)資訊機密維護及稽核使用管理事項，由政風單位會同相關單位負責辦理。

各機關未設置資訊及政風單位者，由機關首長指定適當單位及人員負責辦理。

機關業務性質特殊者，得由其首長調整第一項分工原則。

十、各機關對所屬機關（構）資訊作業，應進行定期或不定期之資訊安全稽核。

各機關對所屬機關（構）進行外部稽核作業，由資訊單位會同政風單位或稽核單位辦理。

十一、各機關應指定副首長或高層主管人員負責資訊安全管理事項之協調及推動。

各機關得視需要，成立跨部門之資訊安全推行小組，統籌資訊安全政策、計畫、資源調度等事項之協調研議。

前項資訊安全小組之幕僚作業，由資訊單位或首長指定之單位負責。

十二、各機關應視資訊安全管理需要，指定適當人員負責辦理資訊安全相關事宜。

伍、人員管理及資訊安全教育訓練

十三、各機關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。

十四、各機關應針對管理、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，提升機關資訊安全水準。

十五、各機關應加強資訊安全管理人力之培訓，提升資訊安全管理能力。各機關資訊安全人力或經驗如有不足，得洽請學者專家或專業機關（構）提供顧問諮詢服務。

十六、各機關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。

十七、各機關首長及各級業務主管，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。

陸、電腦系統安全管理

十八、各機關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。

十九、各機關對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

二十、各機關應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。

二十一、各機關應採行必要之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。

柒、網路安全管理

二十二、各機關利用公眾網路傳送資訊或進行交易處理，應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求，並針對資料傳輸、撥接線路、網路線路與設備、接外連接介面及路由器等事項，研擬妥適的安全控管措施。

二十三、各機關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。

二十四、各機關與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與機關內部網路之資料傳輸及資源存取。

二十五、各機關開放外界連線作業之資訊系統，必要時應以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

二十六、各機關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。

機關網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭不當或不法之竊取使用。

二十七、各機關應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。

機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各機關應視需要以適當之加密或電子簽章等安全技術處理。

機關業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。

二十八、各機關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，研提資料安全需求，並列入採購規格。

各機關發展及應用加密技術，應採用權責主管機關認可之密碼模組產品。

各機關採購外國產製之密碼模組產品，應請廠商提出輸出許可或相關授權文件，確保密碼模組之安全性，並避免採購金鑰代管或金鑰回復功能之產品。

捌、系統存取控制

二十九、各機關應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。

三十、各機關應依資訊安全政策，賦予各級人員必要之系統存取權限；機關員工之系統存取權限，應以執行法定任務所必要者為限。對被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

三十一、各機關離（休）職人員，應立即取消使用機關內各項資訊資源之所有權限，並列入機關人員離（休）職之必要手續。

機關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。

三十二、各機關應建立系統使用者註冊管理制度，加強使用者通行密碼管理，並要求使用者定期更新；使用者通行密碼之更新周期，由機關視作業系統及安全管理需求決定，最長以不超過六個月為原則。

對機關內外擁有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短密碼更新周期。

三十三、各機關開放外界連線作業，應事簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序及應負之責任。

三十四、各機關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。

三十五、各機關之重要資料委外建檔者，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

三十六、各機關應確立系統稽核項目，建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修改。

玖、系統發展及維護安全管理

三十七、各機關自行開發或委外發展系統，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。

三十八、各機關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。

各機關基於實際作業需要，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。

三十九、各機關委託廠商建置及維護重要軟硬體設施時，應在機關相關人員監督及陪同下始得為之。

拾、業務永續運作之規劃

四十、各機關應訂定業務永續運作計畫，評估各種人為及天然災害對機關正常業務運作之影響，訂定緊急應變與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。

四十一、各機關應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，立即向權責主管單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

四十二、各機關應依相關法規，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。

拾壹、其他

四十三、各機關應就設備安置、周邊環境及人員進出管制等，訂定妥善之實體及環境安全管理措施。

拾貳、附則

四十四、機關業務性質特殊者，得參照本要點另定有關規定。

四十五、直轄市或縣（市）政府未訂定資訊安全管理規定者，得準用本要點。