南投縣政府資訊安全管理要點

壹、目的

一、南投縣政府（以下簡稱本府）為強化本府資訊安全管理，建立安全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、本要點所稱各單位，係指縣長辦公室、副縣長辦公室、秘書長辦公室、參議及秘書辦公室、採購中心及依本府組織自治條例第五至八條設置之處。

三、各單位應依有關法令，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，確保各單位資訊蒐集、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，致單位資訊資產遭不當使用、洩漏、竄改、破壞等情事，影響及危害單位業務之程度，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、本要點所稱資訊安全政策，指單位為達成資訊安全目標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

六、各單位應依實際業務需求，訂定單位資訊安全政策，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。

七、各單位訂定之資訊安全政策，應適時評估，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

八、本府應設置資通安全處理小組，統籌本府資訊安全政策、計畫及資源調度等事項之協調與研議。

九、本府資訊安全相關政策、計畫、措施及技術規範之研議與資訊安全技術之研究、建置及評估相關事項，由本府計畫處負責辦理。

十、資料及資訊系統安全需求之研議、使用管理及保護等事項，由各業務單位負責辦理。

十一、資訊機密維護及稽核使用管理事項由本府政風處主管，並進行定期或不定期之資訊安全稽核。

十二、各單位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。

十三、引進及啟用軟體、硬體、通信及管理措施等新資訊科技，應於事前進行安全評估，瞭解新資訊科技之安全保護措施及水準，並依行政程序經主權人員核准，始得引用，以免影響既有的資訊安全措施。

伍、人員管理及資訊安全教育訓練

十四、各單位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。

十五、各單位應針對管理、業務及資訊等不同工作類別之需求，定期或不定期辦理或配合本府計畫處進行資訊安全教育訓練及宣導，建立員工資訊安全認知，提升單位資訊安全水準。

十六、各單位應加強或配合本府計畫處進行資訊安全管理人力之培訓，提升資訊安全管理能力。各單位資訊安全人力或經驗如有不足，得洽請學者專家或專業單位（構）提供顧問諮詢服務。

十七、各單位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。

十八、各單位主管及各級業務主管人員，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。

陸、電腦系統安全管理

十九、各單位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、各單位應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。

柒、網路安全管理

二十一、各單位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，研擬妥適的安全控管措施。

二十二、各單位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。

二十三、各單位與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與單位內部網路之資料傳輸與資源存取。

二十四、各單位開放外界連線作業之資訊系統，必要時得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。

二十五、各單位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。

二十六、各單位自己建置或維護之網站如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、各單位網路使用者應遵循南投縣政府網路使用規範，並確實瞭解其應負之責任；如有違反網路安全情事，應依資訊安全規定，限制或撤消其網路資源存取權利，並依紀律規定及相關法規處理。

二十八、電子郵件使用之安全管理，應依南投縣政府使用電子郵件作業規定辦理；機密性資料及文件，不得以電子郵件或其他電子方式傳送。

二十九、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，各單位應視需要以適當的加密或電子簽章等安全技術處理。

三十、各單位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。

捌、系統存取控制

三十一、各單位使用之資訊系統應訂定相關作業手冊，以確保員工正確及安全地操作使用。

三十二、各單位應依資訊安全政策，賦予各級人員必要的系統存取權限；單位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。

三十三、對離（休）職人員，應立即取消使用單位內各項資訊資源之所有權限，並列入單位人員離（休）職之必要手續。單位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。

三十四、各單位如有其權責業務之資訊系統，應依各單位業務之特性，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，由單位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。

三十五、對單位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。

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

三十七、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。

三十八、重要資料委外建檔，不論在單位內外執行，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。

三十九、單位如有其權責業務之資訊系統，得依各單位業務之特性及視資訊安全管理需要，建立資訊安全稽核制度，定期或不定期辦理或配合有關單位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

四十、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訂定相關之作業手冊，以確保人員正確之操作及使用。

四十一、各單位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。

四十二、各單位資訊系統應將正式作業環境及測試環境獨立分開，建立完整適當之變更控制程序，並嚴格執行，以降低可能的安全風險。

四十三、各單位對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

四十四、各類程式版本之更換，應訂定作業程序，據以辦理；核定使用之程式，不得擅自變更，如有變更之必要時，應獲得權責主管人員核准使得為之。

四十五、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。

四十六、委託廠商建置及維護重要之軟硬體設施，應在單位相關人員監督及陪同下始得為之。

壹拾、資訊資產之安全管理

四十七、資訊資產應包括以下項目：

（一）資訊紀錄：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支

援程序、業務永續運作計畫、預備作業計畫、合約等。

（二）軟體資產：套裝軟體、應用軟體、系統軟體、發展工具及公用程式等。

（三）實體資產：電腦、通訊及儲存設備、磁性媒體等。

（四）技術服務資產：不斷電系統、發電機、空調設備、門禁設備、消防設施等。

四十八、資訊系統應建立資訊資產目錄，並建立各項目之管理人員名冊。

壹拾壹、實體及環境安全管理

四十九、資訊系統相關設備應置於適當地點並予以保護，以降低因環境不安全引發之危險及避免未經授權之存取發生。

五十、重要資訊系統相關設備應建立維護制度，以確保設備之完整性及續用性。資訊主機系統應安裝不斷電設備，並得設置預備電源。

五十一、個人電腦及終端機使用者離座或不再使用時，應予上鎖、離線、設定密碼或其他控制措施。

五十二、資訊相關設備、資料或軟體，禁止帶離辦公室。但經單位主管許可者，不在此限。

壹拾貳、業務永續運作之規劃

五十三、各單位如有其權責業務之資訊系統，應依各單位業務之特性，訂定業務永續運作計畫，評估各種人為及天然災害對單位正常業務運作之影響，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。

五十四、各單位於資訊系統發生重大資通安全事件或其他災害涉及資通安全事件時，應立即依南投縣政府資通安全緊急應變計畫暨作業處理程序辦理。

五十五、各單位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先行處理。

五十六、各單位應依各單位業務之特性及相關法規，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。

壹拾參、附則

五十七、本要點未盡事宜，依其他相關法令規定辦理。