宜蘭縣頭城鎮公所資訊安全管理要點

中華民國99年07月12日頭鎮行字第0990006043號函頒布施行

壹、目的

宜蘭縣頭城鎮公所（以下簡稱本所）為強化資訊安全管理，建立安全及可信賴之電子化環境，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、依據

本要點依據「行政院及所屬各機關資訊安全管理要點」規定，並考量本所業務需求所訂定。

參、定義

資訊安全即為了避免因人為疏失、蓄意或自然災害等風險，運用一套適當的安全控制措施，亦能視影響及危害業務之程度，迅速進行必要之應變處置，並在最短時間內回復正常運作，來確保本所的資訊資產受到妥善的保護。

肆、目標

確保資訊的機密性、完整性、可用性、資訊設備與網路系統的可靠性以及員工對資訊安全之認知，以保護本所資訊資產免遭不當使用、干擾、入侵、洩漏、竄改、破壞或任何不利行為與企圖等情事發生，並確保資訊蒐集、處理、傳送、儲存及流通之安全。

伍、適用範圍

本要點適用於本所各項資訊資產及其資訊使用者，資訊使用者係包含本所員工、建置維護廠商及其他經授權使用資訊資產之人員。

陸、實施要點

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。

柒、實施內容：

一、資訊安全政策

（一）建立安全可信賴之資訊化環境，確保資料、系統、設備及網路之安全。
（二）明定有關人員在資訊安全作業應扮演之角色，責任分配，以作為各單位之權責分工依據。
（三）加強宣導資訊安全政策及相關作業規定，並視實際需要辦理資訊安全教育訓練。
（四）建立各項系統及網路服務之安全控管機制，並防止未經授權的系統存取。
（五）提昇電腦網路防禦技術，適時阻絕外界之入侵、破壞，加強電腦網路系統之安全及品質，以確保網路傳輸資料的正確性及安全性。
（六）在發展應用系統時，應有效防範不當軟體及電腦病毒等危害系統安全之情況發生。
（七）建立安全防護措施，避免資訊設施遭誤用或人為破壞，並防止業務目的以外或超出授權範圍之使用。
（八）確保與維護資訊業務之正常運作，嚴禁惡意攻擊或傳送等不當行為，避免人為或意外因素可能導致的威脅，並建立備援及緊急應變處理機制。
（九）本政策以書面、電子或其他方式告知本所員工、業務往來之公私機構及提供資訊服務之廠商共同遵行。如有違反資訊安全相關規定者，依本所紀律及相關法規辦理。
（十）本政策應至少每年評估一次，並視需求修正，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可行性及有效性。

二、資訊安全權責分工

（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，由本所行政室負責辦理。
（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，由本所各業務單位與行政室負責辦理。
（三）資訊機密維護及稽核使用管理事項，由本所政風室會同相關單位負責辦理。
（四）本所之資訊作業，應視實際業務需求定期或不定期進行資訊安全稽核。上述之資訊安全稽核作業，由政風室會同行政室及受稽核單位辦理。
（五）資訊安全管理事項，由本所主任行政負責協調及推動。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。

三、人員管理及資訊安全教育訓練

（一）對資訊相關職務及工作人員，視實際業務需求，進行安全或適任性評估。

（二）針對管理、業務及資訊等不同工作類別之需求，視實際需要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。

（三）本所各單位主管人員，須負責督導所屬員工之資訊作業安全，防範不法及不當行為。

四、電腦系統安全管理

（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。

（二）系統管理人員，應隨時注意及觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存、印表機及其他輸出設備及通信系統之使用狀況；管理人員應隨時注意上述設備的使用趨勢，尤應注意系統在業務處理及資訊管理上的應用情形。

（三）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侵入，確保系統正常運作。

（四）應保護本所重要的電腦系統、軟體及資料檔案，以防止遺失、毀壞、被偽造或竄改。

五、網路安全管理

（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）與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。

（三）利用網際網路及全球資訊網公布及流通資訊，針對機密性、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。

（四）機密性資料及文件，不得以電子郵件或其他電子方式傳送。

（五）為避免使用者不慎違反本所相關網路安全規定，網路管理人員可以使用網路相關技術，在不干擾正常網路使用原則下，主動管制違反規定之使用者。

六、系統存取控制管理

（一）依資訊安全政策，賦予各級人員必要的系統存取權限；員工之系統存取權限，應以執行法定任務所必要者為限。

（二）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。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；使用者通行密碼之更新周期，最長以不超過六月個為原則。

七、系統發展及維護安全管理

（一）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。

（二）對廠商之軟硬體系統建置及維護人員，應限制其可接觸之系統與資料範圍，並於廠商使用完畢後，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，應在本所相關人員監督及陪同下始得為之。

八、資訊資產安全管理

（一）本所資訊資產分為：資訊資產（如資料庫及資料檔案、系統文件、使用者手冊等）、軟體資產（如應用軟體、系統軟體等）、實體資產（如電腦及通訊設備等）、技術服務資產（如通信服務、電源及空調等）。

（二）本所之資訊資產應予保護及審慎使用，以防止因自然災害或人為因素而遭致之損壞。

（三）各單位使用有智慧財產權的軟體，應遵守相關法令及契約規定，不應保有及使用未取得授權的軟體，亦不得使用盜版之軟體。若發現有使用非法軟體之情事時，應自行或請資訊相關人員協助移除。

（四）應依據電腦處理個人資料保護法等相關規定，審慎處理及保護個人資訊。

九、實體及環境安全管理

（一）電腦機房的安全保護，應以事前劃定的各項周邊設施為基礎，並以設置必要的障礙（例如：鑰匙、使用身分識別卡之安全門等），達成安全控管的目的。

（二）為防斷電時造成系統毀損或資料流失，電腦機房須配置不斷電系統，以便斷電時有足夠時間做存檔與正常關機。

（三）電腦機房應安裝適當的安全偵測及防制設備，例如熱度及煙霧偵測設備，火災警報設備、滅火設備及火災逃生設備等。

（四）個人電腦及電腦終端機不使用時，應以關機、登出、設定螢幕密碼或是其他控制措施保護。

（五）非資訊相關人員或維修人員，不得自行拆卸電腦機殼及更換內部零件；且未經同意，不得增設或移除電腦資訊等設備，亦不得擅自修改相關設定。

十、業務永續運作計畫管理

（一）評估各種人為及天然災害對本所正常業務運作之影響，訂定緊急應變及回復作業程序，並視實際狀況調整更新計畫。

（二）建立本所緊急應變及回復作業程序，遇重要電腦（網路）系統發生當機、中斷時，由資訊相關人員評估影響情形，立即進行電腦（網路）系統之復原或備援作業，並於問題解決後，向行政室主任回報處理結果。

（三）建立本所資訊安全事件緊急處理機制，在發生資訊安全事件時，迅速通報本所行政室或資訊相關人員立即處理，並於事件解決後，向行政室主任回報處理結果；或視危機狀況向國家資通安全會報通報網站進行通報，採取反應措施，必要時並聯繫檢警調單位協助偵查。

捌、本資訊安全管理要點奉　鎮長核可後實施，修正時亦同。