彰化縣溪湖鎮公所維護資訊安全實施要點

107年7月訂定

壹、依 據

行政院及所屬各機關資訊安全管理要點擬訂適當之資訊安全管理措施。

貳、目 的

本要點所定資訊安全措施，綜合考量各項資訊資產之重要性與價值，及因人為疏失、蓄意破壞或自然災害等風險，致本所資訊資產遭不當使用、洩漏、竄改、破壞等情事，影響及危害業務之程度，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。

參、評估實施成效：

一、資訊安全政策訂定:

（一）所訂定之資訊安全管理政策，以書面、電子或其他方式告知本所所屬員工、連線作業之公私機構及提供資訊服務之廠商共同遵行。

（二）資訊安全管理政策實施後，資訊單位須每年評估一次，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。

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。

（四）資訊安全稽核作業，由行政室會同政風單位每半年定期辦理一次，並視實際狀況得不定期進行資訊安全稽核。

（五）資訊安全管理事項由主任秘書或高層主管人員負責協調及推動，得視實際需要，成立資訊安全推行小組，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，應進行安全評估，並依其任務之適任性進行必要之考核。

（二）對可存取機密性與敏感性資訊或系統之人員，及因工作需要須配賦系統管理權限之人員，應加強評估及考核。

（三）資訊單位得依業務及資訊等不同工作類別，視實際需要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。

（四）應加強資訊安全管理人力之培訓提升資訊安全管理能力。

（五）對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，並視需要建立人力備援制度。

（六）各級業務主管，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，須明定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）對於系統變更作業或更新功能，由資訊單位執行控管並詳細紀錄，以備查考。

（三）系統伺服器所存放之機房須由資訊單位專人專責管理，並嚴禁無關人員進出。

五、網路安全管理：

（一）各系統伺服器與外界網路連接之網點，須設立防火牆以控管外界與內部網路之資料傳輸及資源存取，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）各單位使用電子郵件傳輸公務文件及資料須加密碼保護，機密性資料及文件，不得以電子郵件或其他電子方式傳送。

（三）開放外界連線作業，須由資訊單位事前與連線單位簽訂契約或協定，限制系統可運作之權限，並明定應遵守之資訊安全規定、程序及應負之責任。

六、系統存取控制管理：

（一）登入各作業系統時，依各級人員執行法定任務所必要之系統存取權限，由資訊單位系統管理人員設定應賦予權限之帳號與密碼，並於六個月內須更換一次。

（二）對離（休）職人員，須立即取消使用各項資訊資源所有權限，並列入人員離（休）職之必要手續。

（三）對機關內外擁有系統存取特別權限之人員，由資訊單位建立使用人員名冊，加強安全控管，並縮短密碼更新周期為兩個月。

（四）各機關之重要資料如需委外建檔者，不論在機關內外執行，均由資訊單位與委外廠商簽訂適當之安全管制合約，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

七、系統發展及維護安全管理：

（一）各單位自行開發或委外發展系統，須在系統開發初期階段，即將資訊安全納入考量；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）對委外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，並嚴禁資訊單位核發長期性之系統辨識碼及通行密碼。

（三）對委外廠商或系統維護人員基於實際作業需要，資訊單位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。

（四）各單位委託廠商建置及維護重要軟硬體設施時，應在機關系統管理人員與資訊單位人員監督及陪同下始得為之。

八、資訊資產安全管理：

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

（二）不使用來源不明之磁片。

（三）不使用非經許可之軟體程式。

（四）電腦設備須裝置防毒軟體，並開啟於即時掃瞄狀態。對所收電子郵件之附加檔案更須先經過掃瞄確定安全後始得開

啟。

（五）網路主機須設置防火牆。

（六）個人電腦密碼應定期更新，文件檔案存檔時須養成加密保護習慣，若檔案需提供網路共享則必須加密保護。

九、實體及環境安全管理：

（一）資訊單位就系統伺服器主機設備安置於主機房，並由資訊單位專責管理，並管制非相關人員隨意進出。

（二）主機房須設置空調恆溫控制，並配置適量之化學消防設施。

（三）若非資訊單位人員或維修人員，不得自行拆卸電腦機殼及更換內部零組件。

十、業務永續運作計畫管理：

（一）為因應各種人為及天然災害造成業務運作受影響，資訊單位須於系統中安裝救援回復軟體並每天定期作備份。

（二）各單位在發生資訊安全事件時，應立即向資訊單位系統管理人員通報，並聯繫檢警調單位協助偵查。

十一、其他未盡事項以「行政院所屬各機關資訊安全管理規範」及相關規定規範之。