國立臺南護理專科學校資訊安全管理計畫

99.01.15資訊發展委員會會議訂定通過
99.06.22行政會議通過

壹、依據

本計畫依據行政院88年9月15日台88經字第34735號函訂頒「行政院及所屬各機關資訊安全管理要點」、88年11月16日行政院研考會（88）會訊字第05787號函頒「行政院及所屬各機關資訊安全管理規範」及98年6月19日教育部台電字第0980095040A號函「98年度教育機構C、D級資安稽核—綜合意見」訂定。

貳、實施計畫

一、資訊安全政策

資訊安全政策文件包括資訊安全定義、目標、涵蓋範圍、執行組織、權責分工、員工責任及應遵守的安全規則、事件通報程序、處理流程、委外契約相關規定（資料保密、智慧財產權、事件處理方式等條款），並定期評估及以書面、電子或其他方式告知本校所屬教職員工生、連線作業之公私機構及提供資訊服務之廠商共同遵行。

二、資訊安全權責分工

（一）資訊安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項，由圖書資訊中心資訊組(以下簡稱資訊組)辦理。

（二）資料及資訊系統之安全等級研議、使用者權限需求等事項，由業務相關單位會同資訊組辦理。

（三）資訊機密維護及稽核使用管理事項，由人事室(政風)會同相關單位辦理。

（四）人員進用之安全評估，由用人單位會同人事室辦理。

（五）資訊資產安全及管理、緊急應變處理程序演練及測試，由秘書室會同資訊組辦理。

（六）資訊安全稽核作業，由資訊組會同人事室(政風)定期辦理，並視實際狀況得不定期進行資訊安全稽核。

（七）資訊安全管理事項由副校長(或圖書資訊中心主任)負責協調及推動，得視實際需要，成立跨部門之資訊安全推動小組，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）對處理敏感性、機密性資料之人員及因工作需要須賦於系統管理權限之人員，應妥適分工，分散權責並建立評估及考核制度，及視需要建立人員相互支援制度。

（二）對離（休、停）職人員，依據人員離（休、停）職之處理程序辦理，並立即取消使用各項系統資源所有權限。

（三）依角色及職能為基礎，針對不同層級人員，視實際需要辦理資訊安全教育訓練及宣導，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

（四）各業務主管，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）建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理資訊安全事件。

（二）建立資訊設施及系統的變更管理通報機制，以免造成系統安全上的漏洞。

（三）依據電腦處理個人資料保護法之相關規定，審慎處理及保護個人資訊。

（四）建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以便發生災害或儲存媒體失效時，可迅速回復正常作業。

五、網路安全管理

（一）機關與外界網路連接之網點，須設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。

（二）機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中，機密性文件不得以電子郵件傳送；敏感性資訊如有電子傳送之必要，需經加密或電子簽章等安全技術處理後傳送。

（三）審慎評估開放外界連線及機關間資料傳送作業，必要時簽訂契約或協定，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。

（四）建立警示系統，讓網路系統管理人員在特定的網路安全事件發生時，及時獲得警示性的訊號，俾利採取有效的防範措施，減少網路安全事件的發生。

六、系統存取控制管理

（一）視作業系統及安全管理需求訂定通行密碼核發及變更程序並作成記錄。

（二）登入各作業系統時，依各級人員執行任務所必要之系統存取權限，由資訊組系統管理人員設定賦予權限之帳號與密碼，並定期更新。

（三）各單位之重要資料如需委外建檔者，不論在校內或校外執行，均須與委外廠商簽訂適當之安全管制條款，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

七、系統發展及維護之安全管理

（一）在資訊系統規劃之需求分析階段，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）資訊業務委外時，應於事前審慎評估可能的潛在安全風險，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。

（三）對於委外建置之軟硬體系統及維護人員，應規範及限制其可接觸之系統與資料範圍，並於使用完畢後立即取消其使用權限。

（四）依據智慧財產權之相關規定，規範各種軟體之使用。

八、資訊資產安全管理

（一）建立一份與資訊系統有關之資產目錄，並訂定資訊財產攜出辦公處所管理規則。

（二）為防止可能的不當行動，應禁止未經授權的人員在辦公室單獨作業。

（三）電腦設備須裝置防毒軟體並即時更新病毒碼，並公告有關病毒最新資訊。

（四）個人文件檔案存檔時須養成安全保護習慣，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）系統伺服主機、設備應安置於主機房，並由資訊組專責管理，並管制非相關人員隨意進出。

（二）主機房應安裝適當的安全偵測及防制設備，各項安全設備應依廠商的使用說明書定期檢查。

（三）備援作業用的設備及備援媒體，應存放在安全距離以外的地點。

（四）訂定資訊安全緊急應變處理程序並定期演練及測試。

十、業務永續運作計畫管理

（一）評估各種人為及天然災害對正常業務運作之影響，訂定緊急應變及回復作業程序，並視需要調整更新計畫。

（二）建立資訊安全事件之正式通報程序及管道。

（三）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。

十一、其他

（一）訂定資訊安全作業稽核計畫(含稽查內容、範圍、程序、人員)，並定期稽查資訊安全事項辦理情形。

（二）有關資訊安全之細部作業規範由相關資訊組參考「行政院及所屬各機關資訊安全管理規範」辦理。

參、計畫立法

本計畫經資訊發展委員會及行政會議通過，陳校長核定後施行，修正時亦同。