國立臺東專科學校資訊安全管理作業要點

民國101年9月19日行政會議通過
民國104年03月25日行政會議修正通過
民國112年03月16日擴大行政會議修正通過
民國115年9月17日擴大行政會議修正通過

一、目的

立臺東專科學校（以下簡稱本校）為落實資訊安全暨個人資料保護之管理，強化資訊資產安全，並保障本校教職員工生之權益，特依「個人資料保護法」、「資通安全管理法」及其相關子法、教育部「教育體系資通安全管理規範」及本校「資訊安全暨個人資料保護推動委員會設置辦法」訂定「國立臺東專科學校資訊安全管理作業要點」。

二、通則

（一）本要點應以書面、電子或其他方式告知本校全體教職員工生、連線作業之公私機構及提供資訊服務之廠商共同遵行。

（二）本要點應至少每年評估一次，以順應技術、業務等相關環境之趨勢，確保實務作業之有效性。

（三）本要點實施時如有必要，各單位應訂定說明文件，如管理規範、作業程序、資訊安全控管文件等。

（四）資訊安全應定期或不定期進行稽核。

三、權責分工

於實施本要點時，其權責分工如下：

（一）為統籌、協調、研議本校各項資訊安全暨個人資料保護之政策、計畫及資源調度，成立「資訊安全暨個人資料保護推動委員會」（以下簡稱本委員會）。其設置辦法另定之。委員會下設「資訊安全暨個人資料保護執行小組」（以下簡稱本小組）執行各項相關作業。

（二）各項電腦軟硬體設備、資訊應用系統、網路通訊之安全計畫及技術規範之研議、建置及評估等，由所屬單位之管理人員負責辦理；各單位應推派人員兼任本小組成員，擔任該單位專責人員及聯絡窗口。

（三）各項資料之安全需求、使用管理及保護等事項，由業務承辦單位負責辦理。

四、人員管理

（一）本校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、任務指派及工作時，審慎評估人員之適任性，並進行必要之考核。

（二）各單位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存取特別權限之人員，應加強評估及考核。

（三）各單位應針對管理、業務及資訊等不同工作類別之需求，應要求所屬人員定期參加資訊安全暨個人資料保護教育訓練及研習，建立正確認知，提升單位資訊安全水準。

（四）各單位應加強資訊安全人力之培訓，提升資訊安全管理能力。

（五）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機關（ 構 ）提供顧問諮詢服務。

（六）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。

（七）各相關單位主管應負責督導所屬員工之資訊安全作業，防範不法及不當行為。

五、電腦系統安全管理

（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）各單位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）各單位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）各單位基於實際作業需要，得核發短期性及臨時性之系統辨識碼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。

（五）各單位委託廠商建置及維護重要軟硬體設施時，應在單位相關人員監督及陪同下始得為之。

（六）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。

（七）各單位使用軟體之權利及義務應依著作權法及有關議定之合約辦理。各單位應依據「政府所屬各級行政機關電腦軟體管理作業要點」，建立軟體使用管理制度。

（八）各單位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。

六、網路安全管理

（一）利用公眾網路傳送資訊或進行交易處理，應遵守「台灣學術網路使用規範」；並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。

（二）圖書資訊中心資訊組應針對資料傳輸、撥接線路、網路線路與設備、對外連接介面及路由器等事項，研擬妥適安全控管措施。

（三）本校與外界網路連接之網點，必要時得以防火牆或其他安全設施，控管外界與單位內部網路之資料傳輸及資源存取。

（四）本校開放外界連線作業之資訊系統，必要時得視資料及系統之重要性及價值，採用資料加密、身鑑別、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。

（五）本校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。

（六）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。

（七）各單位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違法或不當之竊取使用。

（八）本校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。

（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，本校應視需要以適當之加密或電子簽章等安全技術處理。

（十）單位業務性質特殊，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。

（十一）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。

（十二）各單位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。

（十三）各單位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。

七、系統存取控制

（一）各單位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教職員工生及使用者之相關權限及責任。

（二）各單位應依資訊安全政策，賦予各級人員必要之系統存取權限；賦予之系統存取權限，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）本校各單位離（休）職人員，應立即取消使用校內各項資訊資源之所有權限，並列入人員離（休）職之必要手續。各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。

（四）各單位應建立教職員工生及使用者註冊管理制度，加強通行密碼管理，並要求定期更新；其通行密碼之更新週期，由各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。

（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，並縮短密碼更新週期。

（六）各單位開放外界連線作業，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。

（七）各單位對系統服務廠商以遠端登入方式進行系統維護者，應加強安全控管，並建立人員名冊，與其相關安全保密責任。

（八）各單位資料需委外建檔者，不論在單位內外執行，均應採取適當及必要之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

（九）本校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。

八、業務永續運作之規劃

（一）各單位應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。

（二）本校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，立即向該單位權責人員通報，於採取反應措施後，並由本校聯繫檢警調機關偵查。

九、其他安全措施

（一）本校應依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及必要之資訊安全措施。

（二）各單位應就設備安置、周邊環境及人員進出管制等，訂定妥善之設備及環境安全管理措施。

十、本要點經擴大行政會議通過，陳請校長核定後實施，修正時亦同。