國立臺灣科技大學資通安全暨個人資料保護政策

114.12.03 資通安全暨個人資料保護委員會會議通過

壹、 目的

國立臺灣科技大學(以下簡稱本校)為健全資訊安全架構及落實個人資料妥適之保護，因應資訊技術之變遷及作業環境之風險，特訂定本政策。

貳、 適用對象及範圍

一、 適用對象

本校教職員工、學生、校友、相關委外及合作廠商等。

二、 適用地區

本政策之適用地區包括臺灣地區（含澎湖、金門、馬祖等地區）、本校締結之海外姊妹校地區。

三、 日常作業中應確實遵守「資通安全管理法」、「個人資料保護法」、「電子簽章法」及「著作權法」等相關法令法規，以確保適當使用本校資源與保護隱私資訊。

四、 如經查明確有違反本政策之情事，將依相關法規或本校懲戒規定辦理。

參、 資訊安全準則

為確保適用對象其使用的資訊資料、應用系統、硬體設備及網路設施安全，避免因人為疏失、蓄意破壞或自然災害等風險，遭致資訊資產不當使用、洩漏、竄改、破壞等情事，期藉由管理系統之運作以及本校全體同仁共同努力，以達成機密性、完整性、可用性與法律遵循性，並保障使用者資料隱私之資訊安全目標。

一、 本校成立「資通安全暨個人資料保護委員會」負責本校資通安全與個人資料保護管理相關政策、目標及核心業務。

二、 本校資訊安全管理系統控制技術相關措施，由「資通安全暨個人資料保護委員會」執行小組負責協助辦理。

三、 本校各單位執行資訊業務委外服務時，應於事前審慎評估可能影響，並納入契約或計畫書條款；委外廠商應遵循本政策以及相關程序之規定，不得未經授權使用或濫用本校之各類資訊資產，若涉及限制使用等級以上業務，應簽署保密同意書。

四、 應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，促使教職員工生瞭解資訊安全的重要性及各種可能的安全風險，以提高教職員工生資訊安全意識並熟悉工作中之資訊安全職責，促其遵守資訊安全規定。

五、 應使用具合法版權軟體，避免上網下載來路不明之軟體。

六、 凡領取使用者代碼後，應立即自行設定密碼，個人電腦及主機或網路設備之密碼須遵循本校密碼安全管理設定，使用者不得將自己的使用者代碼與密碼交付他人使用。

七、 各電腦應安裝防毒軟體，如發現無法刪除病毒或病毒造成破壞時，應通報電子計算機中心，協請電子計算機中心派員協助處理。

八、 對於資訊安全事件須有通報及應變措施，以確保資訊系統及重要業務的持續運作。

九、 電子計算機中心應訂定與維護核心資通系統業務持續計畫，每年應至少進行乙次測試演練，確保資訊服務於資訊安全事件發生時，能於預定時間內恢復作業。

十、 重要系統及應用程式每年應至少進行乙次備份，其系統日誌至少保留六個月紀錄，以確保系統資料的安全性；個人電腦中之重要資料備份應由個人自行進行備份，並應選擇安全之環境進行保管。

肆、 個人資料保護準則

一、 處理含個人資料時，應依據「個人資料保護法」及相關規定審慎處理，不私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。

二、 為界定個人資料之範圍，應清查持有之個人資料檔案並建立清冊，且定期執行作業流程檢視及個資盤點作業。

三、 建立個人資料之風險評估及管理機制，藉由資料安全管理及人員管理，以確保本校業務範圍內各項個人資料檔案獲得安全保護。

四、 制定個資蒐集、處理及利用管理程序，並符合個人資料保護相關法令及主管機關之要求。

五、 制定業務終止後個人資料處理方法，以因應個資相關業務終止後，須移轉或銷毀之個人資料的處理方式及程序。

六、 建立個資遭竊取、竄改、毀損、滅失、洩漏或其他不合理或違法利用時之事故預防、通報及應變機制。

七、 定期規劃及舉辦有關個資保護之教育訓練及宣導課程，以提升本校所有同仁對於個資保護之知識與認知。

八、 就個人資料之蒐集、處理、利用所產生之使用紀錄、軌跡資料及證據加以保存。

九、 設置聯絡窗口，以供當事人行使個資法賦與之權利或提出相關之申訴與諮詢。

十、 要求涉及蒐集、處理或利用本校個資之往來廠商遵循本政策及相關規定。本校如有委託個資蒐集、處理及利用作業時，應妥善監督受託機關。

十一、 查核個人資料保護管理制度落實狀況及矯正預防結果追蹤，以確保個人資料檔案之安全。

伍、 審查與宣導

一、 本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本校業務永續運作之能力。

二、 本政策得以書面、電子郵件（E-MAIL）、公告於網站、或其他等方式公告周知。

陸、 頒布與修訂

本政策經「資通安全暨個人資料保護委員會」決議通過後公告實施，修正時亦同。