國立臺灣科技大學　資訊安全政策

100.4.8 資訊安全委員會議通過制訂
102.10.25 資訊安全委員會議修訂通過
111.07.21 資訊安全委員會議修訂通過

壹、 目的

為健全國立臺灣科技大學(以下簡稱本校)之資訊安全架構，提供安全效率之服務，特訂定本政策。

貳、 資訊安全準則

為確保本校教職員工生及使用本校資訊資產或執行資訊業務委外服務之廠商人員其使用的資訊資料、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，期藉由資訊安全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「資訊安全委員會」負責本政策之審核及資訊安全管理制度推動事宜。

二、 本校資訊安全管理系統控制技術相關措施，由電子計算機中心負責協助辦理。

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」等其他資訊安全相關之法令。

四、 應遵守本校相關資訊安全規定，確保適當使用本校資源。

五、 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。

六、 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。

七、 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。

八、 應使用具合法版權軟體，避免上網下載來路不明之軟體。

九、 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。

十、 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。

十一、 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。

十二、 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。

十三、 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。

十四、 違反本政策與本校之資訊安全相關規範，依相關法規或本校懲戒規定辦理。

參、 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。

肆、 頒布與修訂

本政策經「資訊安全委員會」審議通過後，陳請校長核定後施行，修正時亦同。