東南科技大學資訊安全管理系統實施要點

96 學年度第 2 學期第 5 次電算中心會議通過(97.05.15)
97 學年度第 2 學期第 5 次電算中心會議通過(98.06.03)
103 學年度第 2 學期第 6 次電算中心會議通過(104.07.13)

一、本校之資訊安全管理系統(以下簡稱本管理系統)係採用國際標準組織所訂定之資訊安全管理標準(ISO 27001)為架構，以校務資料庫、校園骨幹網路及電子計算機中心(以下簡稱電算中心)機房為範圍，並遵照「個人資料保護法」、「行政院及所屬各機關資訊安全管理要點」之要求，訂定相關規定。為確保管理系統之運作符合 ISO 27001 之要求，特訂定本要點(以下簡稱本要點)。

二、本管理系統以本校「資訊安全管理辦法」為 ISO 27001 所要求之資訊安全管理系統政策與資訊安全政策。

三、本管理系統之文件管制與紀錄管制依照本校「文件製作標準程序書」規定辦理。

四、本管理系統之風險評鑑與風險管理係依照本校「資訊風險評鑑與資訊風險管理實施要點」辦理。

五、本校校園資訊安全宣導，以及與本管理系統運作相關人員，其人員指派、資訊安全職責、資格及教育訓練，依照本校「資訊安全宣導與教育訓練實施要點」之規定辦理。

六、本管理系統由電算中心主任執行 ISO 27001 所要求之管理審查。管理審查每年至少舉行一次，審查結果由資訊安全長進行核備：

（一）資訊安全管理改善提案。

（二）先前資訊安全管理審查結果追蹤。

（三）內外部環境可能影響資訊安全管理系統的改變。

（四）資訊安全績效之回饋：

1. 矯正措施之狀況
2. 監測與衡量結果
3. 內部與外部資訊安全稽核結果

（五）資訊安全目標達成狀況

（六）利害相關者之回饋：

1. 外部相關單位的意見。
2. 內部有關資訊安全管理之意見或提案。

（七）風險評鑑結果與風險管理實施情況。

（八）持續改善的機會。

七、本管理系統由電算中心定期對本管理系統範圍內之各項作業與控制措施執行內部自行查核以符合 ISO 27001 對於內部稽核之要求。內部稽核每半年舉行一次，資訊安全長得視需要對與本校資訊安全有關之事項，另行召集資訊安全稽核小組執行稽核工作。有關電算中心內部自行查核與本校資訊安全稽核之實施方式，依照本校「資訊安全稽核實施要點」之規定辦理。

八、本管理系統之運作過程，經內部自行查核、資訊安全稽核、外部稽核、風險評鑑、

緊急應變與系統災害復原演練、資訊安全事件處理及管理審查等活動，發現有可改善事項時，應依照「資訊安全管理矯正與預防措施實施要點」採取改善措施。

九、本要點經電算中心訂定，陳請校長核定後公布實施，修正時亦同。