東南科技大學資通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)
107學年度第1學期第2次圖書資訊處會議通過(107.09.18)
107學年度第2學期第5次圖書資訊處會議通過(108.06.26)
112學年度第2學期第10次行政會議通過(113.06.25)

一、本校之資通安全管理系統(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、校園骨幹網路及圖書資訊處(以下簡稱圖資處)機房為範圍，並遵照「個人資料保護法」、「資通安全責任等級分級辦法」附表六資通安全責任等級C級之特定非公務機關應辦事項之要求，訂定相關規定。為確保管理系統之運作符合ISO 27001與相關法規之要求，特訂定本要點(以下簡稱本要點)。

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

三、本管理系統之文件管制與紀錄管制依照本校「文件管制辦法」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、本校校園資通安全宣導，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「資通安全宣導與教育訓練實施要點」之規定辦理。

六、本管理系統由圖資長執行ISO 27001 所要求之管理審查。管理審查每年至少舉行一次，審查結果由資通安全長進行核備：

(一) 先前資通安全管理審查結果追蹤。

(二) 與資通安全管理系統有關之外部及內部議題的變更。

(三) 與資通安全管理系統相關關注方之需要及期望的變更。

(四) 資通安全績效之回饋：

1. 矯正措施之狀況
2. 監測與衡量結果
3. 內部與外部資通安全稽核結果
4. 資通安全目標達成狀況

(五) 關注方之回饋：

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。

(六) 風險評鑑結果與風險管理實施情況。

(七) 持續改善的機會。

七、本管理系統由圖資處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，資通安全長得視需要對與本校資訊安全有關之事項，另行召集資訊安全暨個人資料保護稽核小組執行稽核工作。有關圖資處內部自行查核與本校資通安全之實施方式，依照本校「資通安全稽核實施要點」之規定辦理。

八、本管理系統之運作過程，經內部自行查核、資通安全稽核、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「資通安全管理矯正與預防措施實施要點」採取改善措施。

九、本要點經圖資處訂定，陳請校長核定後公布實施，修正時亦同。