東南科技大學資訊安全管理矯正與預防措施實施要點

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)

一、本要點之目的在規範本校資訊安全管理系統運作過程中，發現有可改善事項時，實施矯正與預防措施之方式，以確保所實施之改善措施可消除事件發生根本原因，並落實 ISO 27001 標準對於管理系統須持續改善之要求。

二、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，均應依照本要點辦理。

三、電子計算機中心(以下簡稱電算中心)，應指派專人對可改善事項進行案件登記與追蹤等管制工作。

四、電算中心對於所發現之可改善事項進行案件登記時，應對該事項加以具體描述，包含相關之人、事、時、地、物方可成案。

五、為防止可改善事項及同類性質事件再發生，電算中心應依照可改善事項案件之性質，指派人員分析事件發生之根本原因，並針對如何消除根本原因進行改善方案設計，同一改善方案內應至少提供兩種選項以供評估選擇，系統負責人應提交原因分析與改善方案設計結果由電算中心主任審核。

六、改善方案之實施過程應有完整紀錄，並於完成改善方案後，提交檢討與建議之書面資料由電算中心主任審核方可結案。

七、依據「資訊風險評鑑與資訊風險管理實施要點」所產生之相關風險管理改善工作，亦應依照本要點辦理案件登記與追蹤。

八、本要點經電算中心訂定，陳請校長核定後公佈實施，修正時亦同。