東南科技大學資訊風險評鑑與資訊風險管理實施要點

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 6 次電算中心會議通過(98.06.11)

一、本要點之目的在於規範本校資訊安全管理系統之資訊風險評鑑與資訊風險管理實施方式，以確保本校之資訊安全管理系統之規劃符合 ISO 27001 標準之要求，有效控制本校資訊安全管理系統範圍內的資訊資產所面臨之資訊安全風險。

二、本校之資訊風險評鑑應依照以下步驟執行，由電算中心主任審查，並提交資訊安全長核備，相關之執行步驟內容由本校電子計算機中心(以下簡稱電算中心)另訂程序書加以規範:

(一) 鑑別資訊資產

(二) 分析營運衝擊

(三) 鑑別威脅與弱點

(四) 鑑別現有控制

(五) 鑑別風險發生可能性與影響程度

(六) 決定風險等級

三、本校對於資訊風險的控制所採取之風險管理措施，應以杜絕重大問題發生並減少一般性問題發生的可能性為目標，進行資訊風險評鑑時，風險等級之判定原則由電算中心主任審查，並提交資訊安全長核備。

四、本校之資訊風險管理應依照以下步驟執行，並提交風險管理計畫由資訊安全長審核，相關之執行步驟內容由電算中心另訂程序書加以規範:

(一) 評估風險管理建議

(二) 決定風險管理方案

(三) 彙整風險管理計畫

(四) 執行風險管理計畫工作事項

(五) 追蹤風險管理計畫工作事項進度

五、電算中心應依據現有控制與風險管理計畫，更新資訊安全管理系統之適用性聲明書，並由電算中心主任審查，並提交資訊安全長核備。

六、電算中心應每年提交資訊環境與風險變動情形之評估報告，並對是否須重新執行資訊風險評鑑與資訊風險管理提出建議，由電算中心主任審查，並提交資訊安全長核備。

七、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。