

## 東南科技大學資訊安全稽核實施要點

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電子計算機中心(以下簡稱電算中心)內部自行查核與本校資訊安全稽核之施實方式，以確保內部自行查核與資訊安全稽核之獨立性、客觀性與有效性。
- 二、為確保本校資訊安全管理系統依預期方式運作，本校電算中心每學期應針對本校資訊安全管理系統範圍內之各項作業與控制措施執行一次內部自行查核。
- 三、電算中心內部自行查核應由各組派員交互查核各組所負責之作業與控制措施，所選派之人員應具備 ISO 27001 標準之相關知識或接受過 ISO 27001 標準之相關訓練。
- 四、電算中心執行內部自行查核前應提交查核計畫電算中心主任核准後實施，查核範圍應涵蓋 ISO 27001 標準條文之要求，以及適用性聲明書之所有控制項目。查核計畫應說明查核項目、對應標準條款、時間分配、受查單位及查核人員。
- 五、電算中心執行內部自行查核後，應將查核發現之缺失與改善機會列表追蹤由電算中心主任審查，並提交報告由資訊安全長核備，查核報告應說明查核發現、改善情形以及查核活動之檢討與建議。
- 六、針對本校整體資訊安全狀況，資訊安全長得召集資訊安全稽核小組，依審議通過之稽核計畫執行稽核，並提交報告由計算機發展委員會審議。
- 七、資訊安全稽核小組成員應包括電算中心人員在內；資訊安全稽核計畫應說明查核目的、查核項目、時間分配、受查單位及查核人員；資訊安全稽核報告應說明查核發現與改善建議。
- 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。