東南科技大學資訊安全管理辦法

96 學年度第 2 學期第 9 次行政會議通過(97.06.10)
100 學年度第 2 學期第 7 次行政會議通過(101.05.15)
103 學年度第 2 學期第 3 次行政會議通過(104.03.17)

第1條　本校為達成維持校務行政系統與校園網路服務之穩定順暢、保障校務行政資料安全、增進資訊安全與個人資料保護認知等資訊安全管理整體目標，特依據行政院頒布之「行政院及所屬各機關資訊安全管理要點」、國家資通安全會報頒布之「政府機關（構）資訊安全責任等級分級作業規定」、教育部頒布之「學術網路保護智慧財產權之相關措施」、「校園網路使用規範」以及「教育體系資通安全管理規範」等相關法令規定，訂定「東南科技大學資訊安全管理辦法」(以下簡稱本辦法)。

第2條　本校對於教職員工生個人資料之蒐集、處理及利用係遵照「個人資料保護法」及教育部所頒布之相關管理辦法，並另訂「東南科技大學教職員生個人資料之蒐集、處理及利用管理辦法」加以規範，對於為達成本辦法第 1 條所述之資訊安全管理整體目標所訂定之各種規定，包括相關要點、程序及作業標準書等，則應以本辦法為依據。

第3條　本校之資訊安全管理系統以校務資料庫、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，其各項管理，皆依據本辦法相關規定辦理。

第4條　本校資訊安全管理工作之推動，應參考國際標準組織所訂定之資訊安全管理標準，建立以流程導向設計規畫之管理系統，並對資訊安全管理工作，訂定可具體衡量之績效指標，且進行持續改善。

第5條　本校由資訊安全長負資訊安全管理之全責，電算中心在資訊安全長指揮監督下，執行資訊安全管理工作之規畫與推動。

第6條　為落實本校資訊安全管理工作，電算中心應定期執行內部查核，並提交報告由資訊安全長審查。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，並提交報告由電子計算機發展委員會審議。

第7條　本校資訊安全管理相關人員的工作職務說明中，應明確定義資訊安全職責與資格，所訂之資格應包括持續在職訓練之要求，以確保相關人員具備執行相關資訊安全管理工作之能力。

第8條　為確保本校資訊資產之機密性、完整性及可用性，本校各單位應鑑別所保管與使用之資訊資產，並依據本校對各類資訊資產所訂之安全防護規定，採取保護措施。

第9條　為確保本校校務行政資料之安全，本校依「限定使用」、「內部使用」及「公開使用」三個等級進行資訊分級標示與保護。相關人員應確實依照資訊機密等級，對資訊進行標示，並於使用、保存、複製、傳輸時，依照該資訊之機密等級，採取保護措施。

第10條　本校資訊安全管理人員應依照「政府機關（構）資訊安全責任等級分級作業

規定」及相關資訊系統分類分之參考指引，鑑別本校各項資訊系統並完成分類分級。對於影響達成本校資訊安全管理整體目標的可能事故，應參考國際標準對於企業風險管理之參考指引，進行風險評鑑，並依照評鑑結果採取必要之風險管理措施。

第11條　本校各單位主管須確保對所屬人員之系統及網路權限配置，以符合該人員之職務與身份為原則，各系統及網路之帳號與權限，應定期清查與覆核，以確保權限配置之適切性。相關人員應遵照密碼管理之規定，妥善設定與保管其帳號密碼，避免遭他人利用進行不當存取。

第12條　為求能確實保障本校校務行政資料安全，並履行個人資料保護法規對於委外管理之義務，本校各單位與委外廠商之契約或協議中應納入資訊安全要求與個人資料保護要求，並確保所訂之資訊安全要求與個人資料保護要求適用於其整體供應鏈。

第13條　本校之建築物及辦公場所應區分安全等級，並依安全等級實施必要之管制措施及安全防護，電腦機房應列為最高等級之安全區域之一。相關人員進出或工作於安全防護區，應遵守實體與環境安全之相關規定，經手機密資訊人員暫時離開座位時，必須啟動螢幕保護裝置並將機密資料上鎖。

第14條　為維護校園網路之安全，連接本校校園網路線路應事先提出申請，並經電算中心評估其風險。透過公眾網路或遠距存取本校校園網路網路設備時，須加強身份認證並採取加密措施。

第15條　本校電算中心所負責之校務行政正式營運環境內之系統及網路，須與測試開發環境區隔，正式營運環境內之系統及網路之變更，應依照組態變更之管制規定進行，新版程式未經測試不得對正式環境進行變更。測試環境如使用正式資料進行測試，其資料存取權限之管制應比照正式環境。電算中心須指派專人負責程式派管與變更管制。

第16條　電算中心應訂定校務資料庫操作與管理之規定，並對校務資料庫結構與內容之異動建立管制措施。校務資料庫伺服器與資料庫管理系統應啟動稽核功能，並透過系統稽核功能或另行開發之稽核工具對大量個人資料之查詢、列印、操作與處理留存稽核紀錄。

第17條　電算中心應依照「政府機關（構）資訊安全責任等級分級作業規定」及相關資訊系統資安防護基準要求，訂定伺服器操作與管理之規定，並對伺服器之安全漏洞修補及軟體授權建立管制措施，各單位應依規定操作與管理所負責之伺服器，並配合實施相關管制措施。

第18條　電算中心應訂定校園骨幹網路設備操作與管理之規定，並對網路異動建立管制措施。

第19條　與本校電算中心機房運作有關之門禁、空調、消防、電力配送設備、不斷電系統及發電機等設備，應定期保養檢測與維修，以確保其設備妥善率。

第20條　為確實掌握本校資訊安全狀況並及時處置可能造成危害之事件，電算中心對於機房實體、校園骨幹網路及校務行政資料庫之安全，應建立安全監控機制，

並定期執行檢測與評估。

第21條　各單位應依照營運衝擊分析及風險評鑑之結果，訂定營運持續計畫，以確保校務行政作業在發生重大災害或異常狀況時仍保持正常運作，電算中心應對機房實體、校園骨幹網路及校務行政資料庫訂定緊急應變與系統災害復原計畫，以確保資訊服務之不間斷或於可忍受之中斷時間前，回復資訊服務作業，營運持續計畫及緊急應變與系統災害復計畫每年至少測試演練一次，並依據演練結果加以檢討與修正。

第22條　本校所有人員應共同努力保護智慧財產權，避免校園網路與電腦遭受病毒、駭客及資訊外洩之威脅，並且應在合理使用範圍內及教學與研究之目的下，使用校園網路或透過校園網路下載程式與資料。

第23條　本辦法應每年評估一次是否須進行修正，以確保其適切性與有效性。

第24條　本辦法經行政會議通過，陳請校長核定後公布實施，修正時亦同。