



國立臺北科技大學計算機與網路中心

資訊安全政策 CCSG-001_V16

安全等級： 機密 敏感 一般
發行日期： 106 年 07 月 01 日

© 版 權 說 明 ©

本文件為國立臺北科技大學計算機與網路中心專有之財產
未經許可，不得以任何形式使用、引用或公開等

目 錄

第一章、目的	3
第二章、範圍	3
第三章、責任	4
第四章、聲明	4
第五章、目標	4
第六章、教育訓練	4
第七章、文件紀錄管理	4
第八章、內部稽核	4
第九章、管理階層審查	5
第十章、資訊資產暨風險管理	5
第十一章、政策措施	5

第一章、目的

為增進資訊科技的使用，達成「e化校園」的服務目標，建構完整資訊安全管理措施，以確保國立臺北科技大學(以下簡稱本校)資訊資產免於來自內部或外部、蓄意或意外各種威脅與破壞，保障本校教職員工及學生權益，特建立資訊安全管理制度(以下簡稱本制度)。

第二章、範圍

一、適用範圍

本校「計算機與網路中心」(以下簡稱本中心)的作業活動，其範圍包括：

- (一) 本中心「校務資訊服務系統」與「校園網際網路應用服務」等核心業務。
- (二) 本中心擁有之各項資訊資產。
- (三) 本中心之各辦公處所、建築、機房設備及校園網路之設備。
- (四) 執行作業之人員、系統、手冊、工具、基礎設施。

二、驗證範圍

本中心的作業活動，其範圍包括：

- (一) 資訊機房營運管理
- (二) 主幹網路服務
- (三) 電子郵件系統
- (四) 教師評鑑系統維護作業
- (五) 校園入口網站
- (六) 網路加退選系統
- (七) 學校網頁系統
- (八) 會議及活動簽到系統

第三章、責任

所有本中心人員及維護廠商與業務往來者，及使用本中心服務之使用者，只要涉及任何本制度所涵蓋的範圍，都有責任來實施或配合資訊安全政策(以下簡稱本政策)。

第四章、聲明

健全資訊安全管理架構，提供安全信賴資訊服務。

第五章、目標

- 一、在資訊安全的考量下提供最完整的服務。
- 二、符合主管機關與國家法律規章之要求。
- 三、以 CIA 為基準，訂定相關安全目標與標的，並於管理階層審查會議時裁定之。

第六章、教育訓練

本校教職員工應每學年接受資訊安全相關教育訓練或宣導，且本制度適用範圍內之人員應具備工作所需之相關技能，以提昇資訊安全認知觀念與防護能力，降低因人為因素而造成之資訊安全漏洞。

第七章、文件紀錄管理

- 一、本制度相關文件應經適當審查後，頒布實施。
- 二、本制度相關文件與紀錄之管制方式，應依業務需要，訂定存取權限與保存方式。

第八章、內部稽核

為檢視資訊安全規範之落實度與適切性，以持續改進本制度，每年應至少實施一次資訊安全內部稽核。稽核結果屬優點者，應予以表揚；稽核結果屬缺點者，應做出適度的反應與改善。

第九章、管理階層審查

本制度適用範圍內之主管級以上人員應每學年至少執行一次管理審查，評估本政策修訂之必要性，以反映政府法令、技術及業務等最新發展現況，並檢視各項業務於資訊安全面之落實度，以確保本制度持續運作的適用性、適切性及有效性，其職責如「資訊安全組織暨管理階層審查作業程序」所示。

第十章、資訊資產暨風險管理

應至少每年執行一次資訊資產盤點與風險評鑑，且依據風險評鑑結果，以風險角度，並考量法規遵循性，規劃資源之分配，及時進行風險處理與改善。

第十一章、政策措施

為達成本政策目標，所採取之控制措施如「適用性聲明」內之適用項目。