國立臺北科技大學計算機與網路中心

資訊安全政策
CCSG-001_N11

安全等級：　□機密　　□敏感　　□一般

發行日期：　109　年　10　月　27　日

目　　錄

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、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)。

第三章、聲明

健全資訊安全管理架構，提供安全信賴資訊服務。

第四章、目標

一、在資訊安全的考量下提供完整的服務，並維持業務持續運作。

二、符合主管機關與國家法律規章之要求。

三、保護資訊資產，防止人為意圖不當或不法使用，遏止駭客、病毒等入侵及破壞之行為。

四、建立標準作業程序，避免人為作業疏失及意外，加強同仁資訊安全意識。

第五章、內外部議題與溝通

一、組織應每年評估一次影響資訊安全管理系統運作的議題，包括：

(一) 會影響達成資訊安全管理系統運作的內部與外部議題。內部議題包含：與組織策略目標結合、組織文化、責任、合約關係的形式、作業流程、資源、知識和內部利害相關者感知與價值等。外部議題包含：國際趨勢、社會文化、法令規章、

競爭環境、外部利害相關者目標與關切事項等。

(二) 利害相關團體對資訊安全的要求事項(包含法令法規要求和契約義務)。

二、應規劃影響資訊安全管理系統執行所須溝通的事項、溝通時機、溝通的對象、協助執行溝通人員及溝通方式。

第六章、資訊安全管理系統有效性評估

一、應制訂「有效性量測表」，量測內容由資安推動小組審核後執行。

二、每年追蹤與評估資訊安全管理系統各項活動之執行成效，並將追蹤情形記錄於「有效性量測表」。

三、應於管理審查會議中報告資訊安全管理系統活動執行有效性量測結果。

第七章、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。

第八章、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。

第九章、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。

第十章、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。

第十一章、 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。

第十二章、 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。

第十三章、 紀錄

一、(附表 1)有效性量測表