



# 建國科技大學

## 資訊安全政策

第 1.0 版

112 年 12 月 06 日 頒行

## 目 錄

|               |   |
|---------------|---|
| 壹、 目的 .....   | 3 |
| 貳、 適用範圍 ..... | 3 |
| 參、 名詞定義 ..... | 3 |
| 肆、 權責 .....   | 3 |
| 伍、 要求事項 ..... | 3 |
| 陸、 修訂 .....   | 4 |
| 柒、 施行 .....   | 5 |

## 壹、目的

本政策規範本校資訊安全管理制度，以確保本校管轄資訊資產之機密性、完整性、可用性符合相關法規之要求，進而保障全校教職員工生之權益。

## 貳、適用範圍

本校員工、接觸本校業務資料之外機關人員、委外服務提供廠商人員及訪客。

## 參、名詞定義

- 一、機密性(Confidentiality):使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。
- 二、完整性(Integrity):保護資產的準確度(Accuracy)和完全性(Completeness)的性質。
- 三、可用性(Availability):經授權個體因應需求之可存取及可使用的性質。
- 四、資訊安全:係避免因人為疏失、蓄意或自然災害等風險，運用系統化之控制措施，包含政策、實施、稽核、組織結構和軟硬體功能等，以確保本校資訊資產受到妥善保護。
- 五、資訊資產:凡本校作業流程中使用之資訊資產，如內部人員、外部人員、紙本文件、電子文件、網路服務、電腦應軟體、應用系統、電腦硬體、網路設備、環控系統、建築保護設施與便利設施等皆屬之。
- 六、資訊安全管理系統:Information Security Management System (ISMS)整體管理系統的一部份，乃根據風險管理的辦法所制訂，用來建立、執行、操作、監控、審查、維護與改進資訊安全。

## 肆、權責

設置本校「資訊安全暨個人資料保護推動委員會」，負責政策之核定及監督、資訊安全預防及危機處理。

## 伍、要求事項

### 一、資訊安全目標

- (一) 本校每年無發生教職員工生密級資料外洩。
- (二) 本校每年無發生教職員工生資料(如:學生成績或使用個人資料)遭竄改。
- (三) 確保本校關鍵業務系統資訊機房維運服務達全年上班時間 96.9%以上之可用性，並確保：
  1. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每年不得超過 8 次。
  2. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 8 工作小時。
- (四) 本校關鍵業務系統服務達全年上班時間 98.4%以上之可用性，中心關鍵業務系統因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。

## 二、資訊安全管理事項

避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校帶來各種可能之風險及危害。資訊安全管理應涵蓋下列管理事項：

- (一) 資訊安全政策。
- (二) 資訊安全組織。
- (三) 人力資源安全。
- (四) 資產管理。
- (五) 存取控制。
- (六) 密碼學(加密控制)。
- (七) 實體與環境安全。
- (八) 運作安全。
- (九) 通訊安全。
- (十) 資訊系統取得、開發及維護。
- (十一) 供應者關係。
- (十二) 資訊安全事故管理。
- (十三) 營運持續管理之資訊安全層面。
- (十四) 遵循性。

## 三、資訊安全管理原則

在資訊安全管理系統中，建置蒐集前述安全指標的機制，以確認執行成效。蒐集資料的安控機制包括下列各項：

- (一) 重要之資訊資產應定期清查、分類分級與進行風險評鑑，並據以實施適當的防護措施。
- (二) 重要資訊資產存取權限應予以區分，考量人員職務授予相關權限，必要時得採行加解密(例 zip/rar)及身分鑑別機制，以加強資訊資產之安全。
- (三) 對於資訊安全事件須有完整的通報及應變措施，以確保資訊系統、業務的持續運作。
- (四) 應訂定營運持續計畫並定期演練，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。
- (五) 相關人員應依規定接受資訊安全教育訓練與宣導，以加強資訊安全認知。
- (六) 定期執行資訊安全稽核作業，檢視存取權限及資訊安全管理制度之落實。
- (七) 違反本政策與資訊安全相關規範，依相關法規或本校懲戒規定辦理。
- (八) 本政策每年至少評估一次，依業務變動、技術發展及風險評鑑的結果修訂。

## 陸、修訂

管理階層審查：確保「資訊安全管理系統」實務運作之可用性、安全性及有效性。本政

策每年依業務變動、技術發展及風險評鑑的結果或配合政府資訊安全管理要求、法令、技術及最新業務發展現況至少評估或修訂一次。

## 柒、施行

本政策須經「資訊安全暨個人資料保護推動委員會」審核，核定後依據「文件暨紀錄管理辦法」公告或傳達給本校各單位人員與相關外部單位實施，修訂時亦同。