1 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、可用性及符合相關法規之要求，進而保障全校教職員工生之權益。

2 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。

3 名詞定義

3.1 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。

3.2 完整性（Integrity）：保護資產的準確度（Accuracy）和完全性（Completeness）的性質。

3.3 可用性（Availability）；經授權個體因應需求之可存取及可使用的性質。

3.4 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。

3.5 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。

4 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。

5 要求事項

5.1 資訊安全目標

5.1.1 本校每年無發生教職員生密級資料外洩。

5.1.2 本校每年無發生教職員生資料遭竄改。

5.1.3 保護本校業務服務之安全，確保資訊需經授權，人員才可存取，以確保其機密性。核心業務系統遭非法存取之事件，每年發生次

數不得超過 1 次。

5.1.4 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。核心業務系統資料異動經查核異常案件應為 1 件。

5.1.5 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。提供核心業務系統之平台因資安事件導致服務停頓，每次不得超過 8 小時，每年中斷服務率不得超過 4% 以上（計算方式：全年中斷服務之總工作小時／一年總工作小時）。

5.1.6 每年依本校全體人員之工作職務、責任，適當授與資訊安全相關訓練。

5.1.7 確保本校各項業務服務之執行須符合相關法令或法規之要求。

5.2 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 14 項管理事項：

1. 資訊安全政策。
2. 資訊安全組織。
3. 人力資源安全。
4. 資產管理。
5. 存取控制。
6. 密碼學(加密控制)。
7. 實體與環境安全。
8. 運作安全。
9. 通訊安全。
10. 資訊系統取得、開發及維護。
11. 供應者關係。
12. 資訊安全事故管理。

13. 營運持續管理之資訊安全層面。

14. 遵循性。

5.3 資訊安全管理原則

5.3.1 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。

5.3.2 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)及身分鑑別機制，以加強資訊資產之安全。

5.3.3 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。

5.3.4 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。

5.3.5 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。

5.3.6 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。

5.3.7 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。

5.3.8 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。

6 修訂

6.1 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。

7　施行

7.1　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「資訊安全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。

承辦人/專責人員　　單位主管　　校長