壹、目的

為確保嘉南藥理大學（以下簡稱本校）之資訊系統、主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致資訊資產之機密性、完整性、可用性遭受破壞等風險，導入資訊安全管理制度（以下簡稱 ISMS），落實「資訊安全，人人有責」的觀念，建立全方位資訊安全防護措施，以提供本校之資訊業務持續運作之資訊環境，符合相關法規及內、外部關注方之資訊安全期望與要求，特訂定資訊安全政策（以下簡稱本政策）以茲遵循。

貳、依據

一、資訊安全管理系統要求事項 ISO/IEC 27001：2013。
二、資訊安全管理系統作業規範 ISO/IEC 27002：2013。
三、教育體系資通安全暨個人資料管理規範
四、本校「資訊安全組織全景管理規範」。

參、適用範圍

本校教職員工、接觸本校業務資料、系統、設備之委外服務提供廠商、外機關人員、訪客，及使用本校資訊系統之使用者，均適用之。

肆、定義

一、機密性：確保被授權之人員才可使用資訊。
二、完整性：確保使用之資訊正確無誤、未遭竄改。
三、可用性：確保被授權之人員能取得所需資訊。

伍、政策聲明

一、本校各項資訊安全管理規定必須遵守政府及教育部頒布資訊安全相關法令法規。
二、成立資訊安全管理組織，負責資訊安全制度之建立及推動事宜。

三、依國際標準(ISO/IEC 27001：2013)或教育體系資通安全暨個人資料管理規範，建立、管理、 實作與運作、 監視與審查、 維持與改進「資訊安全管理系統(ISMS)」，並通過國際或教育部資訊安全驗證。

四、依據個人資料保護法、個人資料保護法施行細則及本校個人資料保護管理辦法、個人資料檔案安全維護計畫，並參酌國際及國家個資標準，建立與實施個資管理制度，使個資保護政策得以落實。

五、實施資訊安全教育訓練、精實人員安全考核及發佈之資訊安全規範，以深植本校教職員工對資訊安全之意識與強化其對相關責任之認知，使得本校教職員工及第三方，均能充份遵循本政策及措施。

六、重要之資訊資產應定期清查、分類分級與進行風險評鑑，並據以實施適當的安全控制措施。

七、建立主機及網路使用之管理機制，以統籌分配、運用資源。

八、新系統、設備建置前，須將風險、安全因素納入考量，防範危害系統安全之情況發生。

九、建立資訊機房實體及環境安全防護措施，並定期施以相關保養。

十、明確規範網路系統之使用權限，防止未經授權之存取動作。

十一、 對於資訊安全事件應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。

十二、 訂定 ISMS 內部稽核計畫，定期檢視本校推行 ISMS 範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正措施。

十三、 訂定與維護營運持續計畫並定期測試演練，確保本校核心資訊服務運作不中斷。

十四、 本校所有人員負有維持資訊安全之責任，且應遵守資訊安全管理相關之法律及規範，如有違反或有危害本校資訊

安全之虞時，應立即採取適當措施並辦理人員懲處，有觸犯法律之嫌疑者，逕送司法機關調查。

十五、 為確保上述政策目標實務作業的可行性及有效性，應訂定「ISMS 目標有效性量測表」，每年針對各項政策目標實施有效性量測乙次。

十六、 本政策以書面、電子（E-MAIL、網頁公告）或其他方式通知本校教職員工及接觸本校業務之公私機關（構）、廠商、使用者共同遵行。

陸、審查

本政策應至少每年審查乙次，以反映政府資訊安全管理政策、法令、技術、利害相關團體資訊安全期望與要求，及本校業務之最新狀況，並確保本校資訊安全政策的可行性及有效性。

柒、實施

本政策經資訊安全長核定後公告實施，修訂時亦同。