輔仁大學

資訊安全政策

機密等級：一般

文件編號：IS-A-001

版　　次：1.0

發行日期：97.11.06

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	97.11.06		潘東名	初版

資訊安全政策					
文件編號	IS-A-001	機密等級	一般	版次	1.0

目錄

資訊安全政策					
文件編號	IS-A-001	機密等級	一般	版次	1.0

1 目的

本政策訂定之目的在於確保輔仁大學（以下簡稱本校）所屬資訊資產之機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

2 適用範圍

資訊安全管理涵蓋下列事項，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：

2.1 資訊安全政策訂定與評估。

2.2 資訊安全組織。

2.3 資訊資產分類與管制。

2.4 人員安全管理與教育訓練。

2.5 實體與環境安全。

2.6 通訊與作業安全管理。

2.7 存取控制安全。

2.8 系統開發與維護之安全。

2.9 資訊安全事件之反應及處理。

2.10 業務永續運作管理。

2.11 相關法規與本校政策之符合性。

本校人員、委外服務廠商與訪客皆應遵守本政策。

3 目標

維護本校資訊資產之機密性、完整性及可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

3.1 保護本校業務活動資訊，避免未經授權的存取。

3.2 保護本校業務活動資訊，避免未經授權的修改，確保其正確完整。

3.3 建立資訊業務永續運作計畫，確保本校業務之持續運作。

3.4 本校之業務執行須符合相關法規之要求。

4 責任

4.1 本校之管理階層建立及審查本政策。

4.2 資訊安全管理者應透過適當之標準和程序以實施本政策。

4.3 本校所有人員及委外服務廠商均須依照相關安全管理程序以維護資訊安全政策。

4.4 本校所有人員有義務報告資訊安全事件和任何已鑑別出之弱點。

4.5 有任何危及資訊安全之行為者，應依法負擔民事、刑事及行政責任，並依本校相關規定進行懲處。

5 審查

本政策應至少每年審查乙次，以配合相關法令、技術及業務之發展，並確保本校永續運作及提供學術網路服務之能力。

6 實施

6.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

6.2 本政策經「資訊安全委員會」通過後實施，修訂時亦同。