

基督教台灣浸會神學院

資訊安全政策

機密等級：一般

文件編號：教 1012G0101 資訊安全政策 0601

版 次：1.0

發行日期：2013.6.1

目錄

1	目的	1
2	適用範圍	1
3	目標	1
4	責任	2
5	審查	2
6	實施	2

1. 目的

為確保基督教台灣浸會神學院（以下簡稱「本校」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並參酌本校之業務需求，訂定本政策。

2. 適用範圍

- 2.1 本政策適用範圍為本校之教職員工生、連線作業之公私機構、提供資訊服務廠商等資訊安全管理事宜。
- 2.2 資訊安全管理範疇涵蓋 11 項領域，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，對本校造成各種可能之風險及危害，各領域分述如下：
 - 2.2.1 資訊安全政策訂定與評估。
 - 2.2.2 資訊安全組織。
 - 2.2.3 資訊資產分類與管制。
 - 2.2.4 人員安全管理與教育訓練。
 - 2.2.5 實體與環境安全。
 - 2.2.6 通訊與作業安全管理。
 - 2.2.7 存取控制安全。
 - 2.2.8 系統開發與維護之安全。
 - 2.2.9 資訊安全事件之反應及處理。
 - 2.2.10 業務永續運作管理。
 - 2.2.11 相關法規與施行單位政策之符合性。

3. 目標

為維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本校全體同仁共同努力以達成下列目標：

- 3.1. 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資訊，以確保其機密性。
- 3.2. 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。
- 3.3. 建立本校業務永續運作作業規範，以確保本校業務服務之持續運作。
- 3.4. 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。
- 3.5. 網路服務服務品質，需達全年上班時間網路正常服務時間可用性 98%。
- 3.6. 資料遭未經授權之異動、毀損、誤植或其他非預期性事件影響資料正確性，已衝擊

業務正常運作之資安事件，全年不得超過三件。

3.7. 校譽傷害、經濟損失、個人權益嚴重受損或犯罪觸法之資安事件，全年不得超過三件。

4. 責任

4.1 本校應成立資訊安全委員會統籌本校資訊安全政策制定；負責資訊安全政策及本校資訊安全管理制度認證事宜之執行工作。

4.2 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序實施本政策。

4.3 本校之教職員工生、連線作業之公私機構、提供資訊服務廠商等皆應遵守本政策。

4.4 本校之教職員工生、連線作業之公私機構、提供資訊服務廠商等均有責任透過適當通報機制，通報資訊安全事件或弱點。

4.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

5. 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本校業務永續運作之能力。

6. 實施

本政策經校長核定後實施，修訂時亦同。