

慈濟大學

資訊安全政策

機密等級：一般

文件編號：TCU-ISMS-A-001

版 次：V1.1

發行日期：2026.01.09

資訊安全政策					
文件編號	TCUST-ISMS-A-001	機密等級	一般	版次	V1.1

目錄

1 目的 1

2 適用範圍 1

3 權責 1

4 名詞定義 1

5 作業說明 2

6 修訂 4

7 實施 4

資訊安全政策					
文件編號	TCUST-ISMS-A-001	機密等級	一般	版次	V1.1

1 目的

為確保慈濟大學（以下簡稱「本校」）所屬之資訊資產的機密性、完整性、可用性，以符合「資通安全管理法」等相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，以保障全校教職員之權益，特訂定本政策。

2 適用範圍

本校全體同仁、委外服務廠商、資料使用者(含保管者)與訪客等。

3 權責

- 3.1 設置本校「資通安全暨個人資料保護推動委員會」，負責政策之督導，下設「資訊安全執行小組」，負責政策之擬定、執行、監督、稽核、資訊安全預防及危機處理。
- 3.2 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以實施本政策。
- 3.3 任何存取本校資訊資產之組織、人員等皆應遵守本政策，且均有責任透過本校適當管道，通報與本校有關之資訊安全事件或弱點。
- 3.4 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。

4 名詞定義

- 4.1 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。
- 4.2 完整性 (Integrity)：保護資產的準確度 (Accuracy) 和完全性 (Completeness) 的性質。
- 4.3 可用性 (Availability)：經授權個體因應需求之可存取及可使用的性質。
- 4.4 法律遵循性 (Legal Compliance)：符合目的事業主管機關之要求並避免違反有關資訊安全之法律、法令、法規或契約義務，以及任何安全要求

資訊安全政策					
文件編號	TCUST-ISMS-A-001	機密等級	一般	版次	V1.1

事項。

4.5 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。

4.6 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。

5 作業說明

5.1 資訊安全目標

為維護本校資訊資產之機密性、完整性、可用性與法律遵循性，並保障使用者資料隱私之安全，期藉由本政策之實施以達成下列目標：

5.1.1 建立安全及可信賴之資通作業環境，確保本校電腦資料、系統、設備及網路之安全，以保障本校業務永續運作。

5.1.2 保護本校業務服務之安全，確保資通系統及相關資訊需經授權人員才可存取資訊，以確保其機密性。

5.1.3 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。

5.1.4 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。

5.1.5 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。

5.1.6 保護本校業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。

5.1.7 依循 ISO 27001 要求，進行風險管理，落實品質管理循環（PDCA）精神，以持續改善資訊安全管理系統（ISMS）之有效性。

5.1.8 保護本校業務服務之安全，確保已授權的使用者在需要時能夠存取

資訊安全政策					
文件編號	TCUST-ISMS-A-001	機密等級	一般	版次	V1.1

與使用資訊與系統，以確保其可用性。

5.2 管理指標

5.2.1 依循本校核心價值及資訊安全目標建立「組織全景評鑑表」並以其分析內外部利害關係者之期待與議題。

5.2.2 藉由利害關係者與內外部議題等要求事項，達成下列目標：

5.2.2.1 全景與範圍對應其重要業務流程之要求與維運持續。

5.2.2.2 達成與資安政策一致之預期。

5.2.2.3 透過可量測的規範進行風險管理過程。

5.2.2.4 本校之業務活動執行須符合相關法令或法規之要求。

5.2.3 由「資通安全暨個人資料保護推動委員會」下轄資訊安全執行小組擬定本校資安年度量測指標，校內依量測指標項目匯整資安資訊產出「資安管理指標暨有效性量測表」，於年度結束前交付「資通安全暨個人資料保護推動委員會」進行量測指標追蹤管控，檢討調整量測指標項目，以確保資訊安全管理制度運行。

5.3 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。資訊安全管理應含括四大主題（組織、人員、實體及技術）並落實於本校 14 項管理事項中，各管理事項分述如下：

5.3.1 資訊安全政策。

5.3.2 資訊安全組織。

5.3.3 人力資源安全。

5.3.4 資產管理。

5.3.5 存取控制。

5.3.6 密碼學(加密控制)。

資訊安全政策					
文件編號	TCUST-ISMS-A-001	機密等級	一般	版次	V1.1

5.3.7 實體與環境安全及監控。

5.3.8 運作安全(含雲端運作安全)。

5.3.9 通訊安全。

5.3.10 資訊系統取得、開發及維護。

5.3.11 委外服務與供應者關係安全管理(含雲端管理與監督)。

5.3.12 資訊安全事故管理(含情資管理)。

5.3.13 營運持續管理。

5.3.14 遵循性。

6 修訂

6.1 管理階層審查

6.1.1 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。

本政策每年應適時審查，順應組織或業務發生重大改變進行調整，以確保有效性，並符合相關法規、主管機關及本校資訊安全要求。

6.1.2 資通安全組織、主管機關(或法令、法規要求)、或專家學者等利害關係人如有資通安全相關回饋事項，應將其列入管理審查會議之討論議題。

7 實施

本政策須經「資通安全暨個人資料保護推動委員會」審核，核定後依據「文件管理程序書」公告實施，修訂時亦同。