慈濟科技大學

資訊安全政策

機密等級：一般

文件編號：TCUST-ISMS-A-001

版　　次：3.0

發行日期：112.06.30

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	99.07.06		賴愛姍	初版
1.1	102.04.16	2,3	賴愛姍	更新目錄，並加入 5.管理指標項目
1.2	104.09.02	封面,1	賴愛姍	更新校名及英文簡稱
1.3	106.07.27	封面,1	賴愛姍	2.1 本政策適用範圍為全校教職員生、委外服務廠商與訪客等。
2.0	108.01.09	封面,1,2	賴愛姍	因應 2016 年教版資通安全規範相關要求事項修訂,修訂 2 適用範圍為 14 項，3.1、3.2、3.3 增加關鍵業務，新增 3.5、3.6 項次，修訂 4.1，刪除 5 管理指標。
2.1	112.01.09	封面,1,2,3	呂家誠	依據教育部 111 年 9 月 5 日臺教資（四）字第 1112703805 號函「111 年全國大專校院資安長會議」紀錄，私立大專校院得參照「國立大專校院資通安全維護作業指引」推動全校落實資通安全管理法相關規定及本校資訊安全暨個人資料保護推動委員會設置辦法進行修訂。
3.0	112.06.30	封面	資訊安全暨個人資料保護推動委員會	將侷限於電子計算機中心的文字刪除，並修訂部分內容，延伸至全校適用規範。於 112.06.13 資訊安全暨個人資料保護推動委員會會議研議通過。

目錄

資訊安全政策					
文件編號	TCUST-ISMS-A-001	機密等級	一般	版次	**3.0**

1 目的

為確保慈濟科技大學（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，並衡酌本校之業務需求，訂定本政策。

2 適用範圍

2.1 本政策適用範圍為全校教職員生、委外服務廠商與訪客等。

2.2 資訊安全管理範疇涵蓋 14 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。

2.2.2 資訊安全組織。

2.2.3 人力資源安全。

2.2.4 資產管理。

2.2.5 存取控制。

2.2.6 密碼學(加密控制)。

2.2.7 實體與環境安全。

2.2.8 運作安全。

2.2.9 通訊安全。

2.2.10 資訊系統取得、開發及維護。

2.2.11 供應者關係。

2.2.12 資訊安全事故管理。

2.2.13 營運持續管理之資訊安全層面。

2.2.14 遵循性。

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 保護本校關鍵業務之安全，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 保護本校關鍵業務之安全，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計畫，以確保本校關鍵業務之持續運作。

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 藉由利害關係者與內外部議題等要求事項，達成下列目標：

3.5.1全景與範圍對應其重要業務流程之要求與維運持續。

3.5.2達成與資安政策一致之預期。

3.5.3透過可量測的規範進行風險管理過程。

3.5.4本校之業務活動執行須符合相關法令或法規之要求。

3.6 組織欲達成目標需決定相關要點：

3.6.1執行事項。

3.6.2所需資源。

3.6.3負責人員。

3.6.4完成時間。

3.6.5成果評估方式。

3.6.6各項量測指標(資安工作目標與計畫)、所需資源、負責人員、達成時間及成果評估方式等資訊，請詳閱「ISMS 有效性量測」。

4 責任

4.1 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。

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以實施本政策。

4.3 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。

4.4 本校全體人員及委外服務廠商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「資訊安全暨個人資料保護推動委員會」通過後，陳請校長核准後公告實施，修訂時亦同。