資訊安全政策

1. 安全管理政策

為了促使本公司ISMS能貫徹執行、有效運作、監督管理、持續進行，維護本公司重要資訊系統的機密性、完整性與可用性，特頒佈資訊安全管理政策。本政策旨在讓同仁於日常工作時有一明確指導原則，所有同仁皆有義務積極參與推動資訊

安全管理政策，以確保本公司所有教職員之資料、資訊系統、設備及網路之安全維運，並期許全體同仁均能了解、實施與維持，以達資訊持續營運的目標。

1.1 落實資訊安全，強化服務品質：由全體同仁貫徹執行ISMS，所有資訊作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資訊安全制度的工作，強化服務品質，提升服務水準。

1.2 加強資安訓練，確保持續營運：督導全體同仁落實資訊安全管理工作，每年持續進行適當的資訊安全教育訓練，建立「資訊安全，人人有責」的觀念，促使同仁瞭解資訊安全之重要性，促其遵守資訊安全規定，藉此提高資訊安全智能及緊急應變能力，降低資訊安全風險，達持續營運之目標。

1.3 做好緊急應變，迅速災害復原：訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資訊系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

2. 資訊安全管理目標

本公司執行ISMS需達成之資訊安全目標，應依據「資訊安全目標管理程序書」之相關規定辦理。

3. 資訊安全責任

3.1 本公司的管理階層負責建立及審查政策。

3.2 資訊安全管理者透過適當的標準和程序以實施本政策。

3.3 所有人員與契約委外廠商均須依照程序以維護資訊安全管理政。

3.4 所有人員有責任通報及處理安全事件和任何已鑑別出的弱點。

3.5 任何蓄意違反資訊安全的行為將受到相關規範或法律行動。

4. 資訊安全管理制度(ISMS)

4.1 一般要求：本公司因應ISO 27001:2013資訊安全管理標準之要求，特制訂本政策作為整體ISMS之建置開發、實施操作、監控審查及持續改善之規範，並依據本公司業務活動與風險，以建立資訊安全管理政策及管理目標。

4.2 組織全景之鑑別：本公司應決定與本公司營運目的相關，且會影響ISMS預期成果之內部與外部議題，鑑別出與本公司所提供服務相關之利害關係者，以及這些利害關係者對本公司的需求與期望，並讓資訊安全長知悉以取得共識，用以客觀決定本公司ISMS之範圍。

4.3 應制定組織全景鑑別管理作業程序，用以系統化地鑑別本公司之核心業務與核心業務相關之利害關係者，以及這些利害關係者對本公司核心業務之需求與期望，並判別若無法達到需求與期望會對本公司造成何種程度之衝擊，並將上述評估及分析結果供資訊安全長用以決策ISMS之導入及驗證範圍。