資訊安全政策

維護資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。

責任

1. 本院管理階層建立及審查此政策。
2. 資訊安全管理者透過適當的標準和程序以實施此政策。
3. 所有人員和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，包含行動設備、存取、帳號密碼、供應商管理、系統安全開發、、等。
4. 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
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之相關規定進行懲處。

目標

期藉由全體同仁共同努力來達成下列目標：

1. 保護業務活動資訊，避免未經授權的修改，確保其正確完整。
2. 建立跨部門之資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保具備可供業務持續運作之資訊環境。
3. 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
4. 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
5. 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。
6. 業務活動執行須符合相關法令或法規之要求。

為評量資訊安全政策達成情形，訂定資訊安全目標執行計劃，其量測目標如下：

1. 確保維運之關鍵業務及網路服務可用率達 99%。
2. 確保因資通安全或其他異常事件，所造成系統故障而中斷業務服務之情事，每次最長不得超過 4 小時。
3. 關鍵業務因資安事件造成癱瘓事件次數每年不超過 3 次。
4. 發生資安事件影響等級為 3 級以上的次數，每年不得超過 1 件。
5. 為保護資訊資產之機密性與完整性，每年進行風險評鑑及處理不得少\於一次。
6. 為確保資訊安全措施或規範，符合法令、法規要求，每年至少需進行稽核一次。
7. 每年需進行 1 次以上業務持續運作計劃及維護，以確保資訊業務服務得以持運作。

本政策最後審視日期：106 年 6 月 9 日