資訊安全政策及管理方案

一、資訊安全風險架構

- 本公司資訊安全之權責單位為行政服務部，負責統籌資訊安全及相關事宜，擬定相關內部控制程序管理，並定期進行內部資訊安全檢查。
- 本公司稽核室為資訊安全監理之督導單位，負責督導內部資安執行狀況，若有查核發現缺失，立即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。
- 組織運作模式是採用 PDCA（Plan-Do-Check-Act）循環式管理，確保目標之達成且持續改善。

二、資訊安全政策

(一) 目的：

為建置本公司安全及可信賴的資訊運作環境，維持業務持續運作，降低資訊作業風險，保障資訊服務使用者之權益，建立資訊安全管理系統，規範本程序為最高指導方針，以達成資訊安全管理的目標。

(二) 範圍：

包括本公司所屬各據點資訊作業之相關人員、管理制度、應用程式、資料、文件、媒體儲存、硬體設備及網路設施。

(三) 目標：

避免資訊系統遭受來自內、外部人員不當使用或蓄意破壞，或當已遭受不當使用、蓄意破壞等緊急事故時，公司能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之經濟損害及營運中斷。

(四) 程序：

執行資訊機房、網路安全、系統開發及程式修改、資料安全、資訊保密、智慧財產權、資訊委外等管理。

三、資訊安全管理措施

資訊安全管理措施		
類型	**說明**	**相關作業**
權限管理	人員帳號、權限管理與系統操作行為之管理措施	●人員帳號權限管理與審核
外部威脅	內部潛在弱點、中毒管道與防護措施	●主機/電腦弱點檢測及更新措施 ●病毒防護與惡意程式檢測
系統可用性	系統可用狀態與服務中斷時之處置措施	●系統網路可用狀態監控及通報機制 ●資訊備份機制 ●定期災害復原演練

資訊安全事件依循事前預防、事中處理、事後檢討三大階段辦理

事前預防	事中處理	事後檢討
• 環境管理	• 環境回復	• 記錄過程
• 資料管理	• 資料復原	• 保留證據
• 人員管理	• 快速處理	• 教育訓練

(一)事前預防控制：

(1)環境管理：強化資訊環境安全管理、加強防火牆系統。

(2)資料管理：應用資料加密系統、權限管控系統、加強管理管制資料存取。

(3)人員管理：定期辦理資訊安全教育訓練，不定期推播及宣導資訊安全。

(二)事中問題處理：

(1)環境回復：透過復原計畫，逐步回復服務。

(2)資料復原：透過備份系統，將資料復原。

(3)快速處理：透過短期對策，縮短影響時間。

(三)事後檢討：

(1)紀錄過程：事件處理過程詳細紀錄，並作成長期對策，防止再發。

(2)保留證據：保留證據，調查事件始末。

(3)教育訓練：藉由資安事件可加強員工資安及風險管理。

四、具體資訊安全強化方案

(一)陸續導入多項資安措施，提升整體資訊安全：

(1)提升資訊防禦能力：升級防毒防駭系統、加強防火牆系統。

(2)降低資料損失風險：建立異地備份機制。

(3)建立軌跡紀錄功能：導入資料存取稽核系統。

(二)未來資訊安全規劃：

(1)定期執行系統安全漏洞掃描。

(2)持續強化基礎資訊環境。

(3)建立備份資料異地存放機制自動化。