1. 資訊安全風險管理架構：

本公司資訊安全之權責單位為資訊中心，設置資訊主管及專業資訊人員共兩位，負責規劃、執行及推動資訊安全管理政策事項，並推展資訊安全意識。資訊安全監理之查核單位為稽核單位，若每年內部稽核、外部稽核，查核發現缺失，即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。

2. 資通安全政策：

落實資安管理，公司訂有內部控制制度—電腦資訊循環及資訊安全管理政策，藉由全體同仁共同努力期望達成下列政策目標：

①確保資訊資產之機密性、完整性、可用性。

②確保依據部門權限資料存取及防止未經授權之修改或使用資料與系統。

③確保資訊系統之永續運作。

④防止駭客、各種病毒入侵及人為意圖不當及不法使用。

⑤定期執行資安稽核作業，確保資訊安全落實執行。

3. 具體管理方案：

①公司電腦主機、各應用伺服器等設備置放於專用機房，機房採用門禁管制並保留進出紀錄備查。

②機房管理人員應執行機房環境監測，每日填寫機房日誌，並注意機房溫溼度、空調等設備之運轉狀況。

③機房主機配置不斷電設備，避免瞬間斷電造成系統當機，或確保臨時停電不會中斷電腦應用系統的運作。

④建置備份系統，採每日增量、每周完整備份，並於異地儲存，以降低系統毀損所造成的風險及損失。

⑤與外界連線的入口，配置企業級防火牆，阻擋駭客非法入侵。

⑥同仁由遠端登入公司內網存取資料，必須申請相關權限始能登入使用，並留使用紀錄供稽查。

⑦有遠端存取需求的同仁，須經申請後提供 VPN 加密之安全通道連線。

⑧定期宣導，對內部同仁宣導教育相關資訊安全知識，建立並加強資訊安全認知，提升資訊安全水準。

4. 投入資通安全管理之資源：

①配置企業級防火牆，阻擋駭客非法入侵。

②建置備份軟硬體系統，並定期檢視備份資料可用性，保護公司重要系統與資料安全。

③每日各系統狀態檢查、每週定期備份及備份媒體異地存放之執行。

④定期對內部同仁宣導資訊安全管理政策，會計師稽核。

5. 預計投入

防毒軟體，包含郵件防毒、垃圾郵件過濾等，以避免惡意病毒程式之攻擊。

6. 執行狀況：

①本公司目前無重大資安事件導致營業損害之情事。

②續落實資訊安全管理政策目標，並定期實施復原計劃演練，保護公司重要系統與資料安全。