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 保護公司與客戶資訊資產之機密性、完整性、可用性。
② 透過全員認知，達成資訊安全人人有責的共識。
③ 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。
④ 「確保公司業務之永續營運」為指導準則，建立防火牆、入侵偵測、防毒等系統，以提升公司在防禦攻擊的能力，防止駭客、各種病毒入侵及人為意圖不當及不法使用。
⑤ 不斷地進行「計劃 - 實施 - 查核 - 行動」(PDCA, Plan-Do-Check-Act) 循環以持續改善。

「計劃階段」著重資通風險管理，建立資通安全風險識別，包括核心資產、應修補而未修補的漏洞等，定期檢視與更新。

「執行階段」建構多層資安防護機制，強化資訊及網路安全，以維護公司重要資產。

「查核階段」定期執行資安稽核作業，確保資通安全政策落實執行。

「行動階段」以檢討與持續改善為本，落實監督、稽核確保資安規範持續有效，並持續進行全員資安教育訓練以提升資安意識。

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 定期檢視與更新資通安全風險識別，並追蹤未修補漏洞的風險等級，確保及時採取防護與應變措施。
⑥ 與外界連線的入口，配置企業級防火牆，阻擋駭客非法入侵。
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 員工應遵守資安規定，遵循資安政策，並不斷地進行 PDCA 循環以持續改善。
⑨ 進行全員資安教育訓練與不定期社交工程釣魚郵件測試，以提升資訊安全水準。

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 配置端點偵測與回應(EDR)，增進網路、端點及應用安全。
⑤ 依據 CVSS（通用漏洞評分系統）優先排序修補漏洞。
⑥ 所有新進員工到職時皆完成資訊安全教育訓練。
⑦ 定期對內部同仁宣導資訊安全管理政策，定期會計師稽核。
⑧ 114 年度投入資源：

- 資通安全相關人力投入 2 人。
- 資通安全相關軟硬體採購 $766,200。
- 資通安全相關會議 1 次。
- 資通安全相關教育訓練 12 hr。

5. 預計投入

① 垃圾郵件過濾，以避免惡意病毒程式之攻擊。
② 防火牆更新。
③ 弱點掃描測試。

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 持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。