資訊安全風險管理架構

本公司總經理召集成立「資通安全處理小組」，由總經理、資訊部門主管及組員共四名成員組成，負責主導及規劃本公司資訊安全，由各行政業務相關單位配合執行，以確認本公司資訊安全管理運作之有效性。本小組每月定期召開會議檢討執行情形，以確保本公司營運業務持續運作，並確認本小組提供的資訊服務可穩定使用。

資訊安全政策

本公司資訊安全管理政策由資通安全處理小組負責制定並定期檢討修正，目前本公司已訂定之資訊安全政策如下:

- ✓ 內部控制制度-資訊循環
- ✓ 資通安全檢查規範
- ✓ 資訊系統管理程序
- ✓ 資訊系統災害防制與緊急應變處理程序

資訊安全具體管理方案

資訊安全管理類型	相關作業
資產盤點	定期盤點資訊資產清單
系統可用性	監控系統、網路之使用狀態 資料異地備援以確保完整復原資訊 定期演練災害發生以及系統還原程序 中斷資訊服務應變措施
外部威脅	偵測病毒與惡意程式攻擊，防範資訊受損 電腦主機弱點檢測及更新 個人電腦安裝防毒軟體且定期更新病毒碼
權限管理	員工帳號及權限之設定管理 定期檢查盤點帳號及必要業務之使用權限 重要機房出入權限管理
存取控管	管制資訊檔案存取 資料存取記錄 重要資料加密
教育宣導	不定期執行資訊安全宣導作業 強化同仁資安認知及法令觀念

112 年度執行情形：

- 本公司資訊安全本公司於 112 年度召開 11 次資訊安全管理委員會議，檢討各單位資安政策之執行情形，當年度並無危害本公司資訊安全之事件。
- 公司內部網站有資訊安全宣導影片，及不定期郵件宣導資訊安全新知，加強員工對於資訊安全風險之應變與警覺性。
- 資料備份：透過定期排程及手動的操作，確保原資料損壞時能有複本資料可復原，降低資料損壞所造成的衝擊。
- 個人電腦及公用電腦安裝防毒軟體並定期確認病毒碼之更新。
- 重要資訊系統定期災難復原演練，如遭重大之天災或人為破壞時，以最短時間內重建系統，恢復公司正常之營運業務運作。
- 進修課程：指派資訊人員 ESET 防毒企業版產品課程，共 12 小時。

投入資通安全管理之資源

本公司投入資通安全管理之資源，以落實各項資安措施，提升作業安全。

1. 導入遠端操作系統，提供員工具有網路安全連線並有效率在家工作，IT 能集中管理遠端資源，降低公司設備受到威脅，保護企業機密資料。
2. 定期更新防火牆軟體系統，強化網路防火牆與網路控管，防止不信任的外部網路連線入侵。
3. 測試安裝針對公司內部網路環境進行監測弱點分析軟體，並依分析結果進行資訊安全優化改善。