推動資通安全執行情形

本公司管理階層積極落實公司資通安全風險管理，制訂「資訊安全政策」明確規範網路系統暨實體事務機器的使用權限，並由本公司管理資訊處負責執行管理。

運作及執行情形：

1. 定時備份各資訊系統及異地備援，並於每年定期進行資訊系統復原演練測試，以確保資訊系統之正常運作及資料保全，降低無預警天災及人為疏失造成之系統中斷風險。
2. 建置各種資安技術控管方案，包括網路防火牆、防毒系統、防垃圾郵件等系統。
3. 增加資訊資料保護保險(CYBER EDGE)，以分散可能的風險損失。
4. 定期執行社交工程演練，宣導同仁最新詐騙釣魚郵件/型態，避免同事誤觸。
5. 提高及改善各系統的密碼複雜度及安全性設定，降低被駭客攻擊的風險。
6. 定期檢視整理各系統使用帳號，停用無用的帳號，確保無未經授權的存取。
7. 本公司於 111 年度全面更新同仁設備為公發設備，以提高資安防護效能。
8. 不定期進行資通安全宣導，提高同仁資安相關意識。以減少資通安全事件的發生。
9. 導入 FIREWALL IPS（入侵防禦系統）、IDP(入侵偵測系統)功能。提升網路使用的安全性。
10. 網站連線由 http 轉換成 https。提升資料傳遞的安全性。
11. NAC 系統導入，提升設備控管的能力，確保設備的合規性。
12. 進行軟體相關盤點工作，確保軟體的合法性及版本相關控管工作。