# 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。

**具體運作及執行情形：**

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. 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。
8. 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。
9. 網站連線由 http 轉換成 https。提升資料傳遞的安全性。
10. 導入內網設備檢查機制，提升設備控管的能力，禁止不合規的設備連線內網。
11. 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。
12. 導入帳號 MFA 驗証。提升帳號登入的安全性。
13. 導入 EDR 系統，提升終端設備端點資安防護。有效阻擋來自各方攻擊。
14. 導入 UEM 系統，完善管理資安相關 PATCH 的派送及安裝，提升系統的安全性。
15. 進行網站源碼掃描，改善程式的漏動以提升系統的安全。
16. 執行相關弱點掃描並改進相關的弱點。
17. 執行滲透測試，偵測系統及網路架構缺失並進行相關改善工作。
18. 對外網站導入 WAF 相關功能，提升網站的安全性及可用性。

**114 年度 投入資通安全管理之資源：**

1. 教育訓練 ： 所有新進員工皆完成線上資訊安全教育訓練課程。
2. 社交工程演練 ： 每年定期執行 2 次社交工程釣魚郵件測試及線上教育訓練。
3. 資安通告宣導 ： 製作超過 6 份資安通告，提升員工資安防護意識。
4. 資安查核 ： 每年定期接受集團資安查核，參與集團資安會議 6 次，內部資安檢討會議 6 次，強化各項資安要求。
5. 資安演練 ：定期弱點掃描 1 次，滲透測試 1 次。
6. 資安人員參加資安相關外訓課程 2 人次。
7. 114 年度執行 EOS 伺服器更新或淘汰計 87 台。
8. 本年度完成應用系統復原計畫更新，並執行年度復原演練；所有系統均符合既定 RTO/RPO 要求，演練後之 改善項目亦已完成。