資通安全風險管理

1. 資訊安全政策：

本公司制定資訊安全政策作為資通安全管理之指導準則，聚焦個人資料檔案之安全維護與管理、營業秘密檔案管理及資訊系統安全三大面向，並持續落實資通安全管理，強化人員、設備、系統、資料及網路等資訊資產之安全管理，免於因外在威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險。

2. 資訊安全組織架構：

(1) 本公司於 109 年設置「資訊安全委員會」，負責資通安全推動等相關事宜。
(2) 「資訊安全委員會」下設個人資料保護管理、營業秘密管理及資訊系統安全管理等小組，負責執行相關管理作業，114 年召開 5 場次以上相關會議。
(3) 由稽核室稽核資訊安全作業。
(4) 全體員工及協力廠商等資訊使用者遵行本公司資訊安全要求。

3. 管理階層支持：

114/3/12 已向董事會報告資訊安全管理執行狀況。

4. 資訊安全具體管理方案：

(1) 建置防火牆系統防止非法入侵、破壞或竊取資料，以保障資料安全，114 年未發生重大的網路攻擊或事件。
(2) 遠端連線機制採多重身分驗證，並宣導使用者應對網路風險保持警覺。
(3) 建置垃圾郵件過濾系統，降低垃圾郵件造成之資安風險。
(4) 每台電腦安裝防毒軟體，定期掃毒，重點機台安裝 EDR 軟體，以提供同仁安全的作業環境。
(5) 定期下載漏洞修補程式更新作業系統，以防止駭客或病毒攻擊。
(6) 每日、每月定期進行備份作業，並將備份資料異地存放。
(7) 114 年 6 月進行 ERP 系統還原演練，確保備份資料正確及有效。
(8) 資料存取權限須經權責主管核可後，方由資訊單位設定。
(9) 114 年度人員到職、異動、離職時，均依作業要求進行權限變更。
(10)應用系統軟體之變更，由使用部門填具「電腦作業變更申請單」經權責主管核准，並依程式開發及設計程序辦理。
(11) 110 年起加入臺灣電腦網路危機處理暨協調中心(TWCERT/CC)、112 年起加入台灣資安主管聯盟，取得資安預警情資、資安威脅與弱點資訊。

5. 資通安全資源投入：

(1) 本公司建置防火牆系統、垃圾郵件過濾系統，每台電腦皆安裝防毒軟體、重點機台安裝 EDR 軟體、定期進行漏洞更新，防止非法入侵、破壞或竊取資料，以保障資料安全。
(2) 上述資通相關系統皆指定專人負責，提升資通防護能量。
(3) 114 年委託資安廠商進行資通安全檢測，無重大問題。
(4) 114 年資訊設備皆納入電子設備險投保。
(5) 114 年實施 2 次電子郵件社交工程演練、3 次資安通報、3 場次資訊安全教育訓練。
(6) 114 年資訊人員參加資訊安全相關課程，計 2 人次。
(7) 維持資安專責主管 1 人，資安專責人員 2 人，114 年累計 iPAS 中級資訊安全工程師證照 1 張、iPAS 初級資訊安全工程師證照 5 張、。

6. 資安與網路風險之評估：

(1) 114 年勤業眾信聯合會計師事務所進行資訊作業內部控制之有效性查核，並無重大之

風險問題。

(2) 114 年委由外部廠商進行網路安全檢測 2 次，並未發現重大之網路資安問題。

(3) 114 年執行「主機系統弱點掃描」、「防火牆連線設定檢視」等檢測項目，掌握內部資安防護現況，並採取適當強化措施。

7. 資安事件：

(1) 近三年度未發生任何重大資安事件，致公司遭受損失或對營運產生不利影響。

(2) 每年皆進行 ERP 系統及重要主機異機還原演練，以因應異常狀況之快速回應。