資訊安全管理制度暨 2025 年度運作情形

■ 資訊安全管理政策與治理架構

一、 資通安全政策

本公司訂有《資訊安全政策》與《資通安全管理規範》，確保資訊資產之機密性、完整性與性。該政策包括以下面向：

1. 制度建立：制訂資訊安全政策，規範資安管理措施
2. 軟硬體建置：建置資安相關軟硬體設備
3. 加強資安意識：建立全體同仁資安意識

二、 治理架構

1. 本公司於 2023 年 12 月成立資安中心
2. 編制：資安主管 1 名、資安人員 1 名
3. 資安中心職責：規劃、推動、稽核與教育宣導
4. 稽核室：執行資安措施之監督與追蹤
5. 委託外部資安專業團隊建立 7X24 資安監控機制，即時監控潛在資安事件及通報異常事件，降低資安事件所造成的損失風險

■ 資訊安全風險管理

一、 風險管理目標

1. 確保資訊管理正確與完整
2. 確保系統與作業環境可靠安全
3. 降低資通安全風險
4. 支持公司持續正常營運

二、 風險管理架構

1. 資安中心：資訊安全權責單位，負責預防、通報、處理、制度維護、版本控管
2. 稽核室：稽核及矯正追蹤
3. 重大資通風險通報與監控機制已全面到位。
4. 定義重大資通安全事件為造成營運中斷、機敏資料外洩、系統遭入侵或需向主管機關通報之衝擊資安事件。

■ 主要資安管理措施

一、 權限管理：帳號與權限審核、定期盤點

二、 存取管控：內外部存取控管、操作軌跡分析

三、 外部威脅防護：病毒與惡意程式偵測、電子郵件安全宣導、防火牆及郵件過濾系統更新與強化

四、 系統可用性：資料備份、異地備份及離線備份、災害還原演練

■ 2025 年度執行情形

一、 資安中心每半年定期於永續發展委員會報告資安執行計畫及狀況，2025 年度分別於 5/8 及 12/3 進行報告，並向董事會報告。

二、 為強化企業資安防護能力、因應日益嚴峻的資安威脅，保障本公司系統資料的機密性、完整性、可用性及個人資料的安全，2025 年度本公司共投入約 888 萬元執行多項資安專案，包含社交工程演練、MDR 威脅偵測、異地備份等計畫。

三、 在 2025 年度具體成果內，資安中心在人員方面除了定期對全體同仁進行資

安宣導，每年也執行兩次資安盤點與稽查。此外，針對經手機密資料部門人員及資安防護意識較弱的同仁，特別規劃專項課程培訓。2025 年度累計培訓時數為 135 人時，進而展現本公司對資訊安全的重視與承諾。

四、 2025 年度具體成果：

項目	2025 年度具體成果
資安教育訓練	前次社交工程演練未通過人員，合計 4 場、90 人、135 人時
資安宣導	每月 e-mail 推播資安宣導 1 次，推播對象全體同仁，累計推播 4,000 人次
資安盤點與稽核	配合資訊設備盤點抽查同仁電腦使用狀況，今年隨機抽查 65 位同仁，合格率 100%。 NAS 備份每季稽核 1 次，目前累計 3 次，合格率皆 100%。

五、 MDR 威脅偵測與防護機制啟用後，2025 年度即時處理 51 項警示並成功阻斷多起惡意與未授權行為；所有事件均在初期即被隔離排除，全年未發生重大資通安全事件。