

資通安全管理運作情形

(一) 資通安全風險管理架構、資通安全政策、投入資通安全管理之資源等：

1. 資通安全風險管理架構

(1) 資訊安全治理組織

本公司資訊安全委員會，設置主任委員、資安政策制定暨推廣小組(負責資訊安全政策之制定及教育訓練與推廣計劃)、資安風險事件管理小組(監控、記錄與調查資訊安全事件及確認資訊資產的所有權與控制皆有適當的管理)、內部稽核小組(規劃執行資安稽核計劃，提出稽核報告，追蹤改善情形)及推行委員(各部門主管或其成員)，負責資訊安全政策之制定，並向董事會報告資通安全執行情形，確保運作之適切性及有效性。

(2) 資訊安全組織架構

由總經理指派一高階主管為委員會主席監督資訊安全委員會運作，114 年 2 月 2 日舉行第一次會議、114 年 10 月 17 日舉行第二次會議，於 114 年 11 月 10 日董事會報告執行情形。

2. 資通安全政策

本公司資訊安全管理涵蓋下列資訊安全管理事項，以避免如因人為疏失、蓄意或天然災害等因素，遭致不當使用、破壞、遺失或洩漏等情事，而對本公司可能帶來相關風險及危害。本公司資訊安全管理事項如下：

- 2.1. 資訊資產之安全管理
- 2.2. 人員安全管理及教育訓練
- 2.3. 實體及環境安全管理
- 2.4. 電腦系統及網路安全管理
- 2.5. 系統存取控制
- 2.6. 系統發展及維護之安全管理
- 3. 投入資通安全管理之資源

(1) 專責人力：設有資安專員人力 1 名，負責公司資訊安全規劃、技術導入與資安相關的稽核事項，以維護及持續強化資訊安全。

(2) 教育訓練：114 年度共計執行乙次以上社交工程釣魚郵件測試。

(3) 本公司對 VPN 連線裝置購置 MFA 解決方案降低連線風險，114 年度相關費用合計總支出 約為新台幣 300,000 元，以減少資安攻擊之風險。

(二) 最近年度及截至年報刊印日止，因 114 年 2 月重大資通安全事件所遭受之損失、可能影響及因應措施：無客戶和內部機敏資料外洩且營運在可控天數內恢復正常，將持續投入資安軟硬體加強防範。