資訊安全

■資訊安全風險管理架構：

本公司資訊安全風險管理目前由資訊中心負責，包含網路與系統安全管理、相關資訊應用系統軟體與硬體設施控制、資訊安全維護作業；並依資訊安全政策及改善計畫配置妥適人力與資源，含括資訊安全作業程序之訂定、風險控制執行、監督與審理安全相關事項。本年度針對資訊安全防護執行情形，內部資安稽核及客戶稽核皆未有重大缺失問題或發現。

執行資訊安全作業與資安政策推動與落實，並定期向董事會報告公司資安治理概況，近期報告日期為2023年11月13日。

■資訊安全政策與具體管理方案：

本公司資訊安全具體管理可分為「內部管制」與「外部防護」面向，簡要列舉說明如下：

一、 內部管制：

1、 針對營業機敏性資料處理及儲存建立適當之防護措施，依工作職務權責施行權限管控，確保存取安全。

2、 針對電腦機房、人員進出管控、環境維護 (溫溼度控制) 等配置適當管理措施，達成基礎資訊安全要求。

3、 為確保營運與重要業務的永續運作，避免重要資訊系統因重大災難事件而導致服務無法持續的風險，公司建立重要資訊系統之備援計畫、備份及每年定期進行災難復原演練，確保公司在關鍵時刻發揮災難應變能力以災害復原機制快速回復至企業正常或可接受的營運水準，以達到關鍵應用系統能持續運作並確保企業的營運不中斷。

4、 確保法遵與合規要求，禁止非授權軟體或硬體的使用，並訂定資訊裝置使用管理規範，如：軟體安裝、電子郵件通訊及可攜式媒體等使用規則。

5、 綜理資訊安全事件反應處理、問題鑑識與調查、緊急處置及應變程序執行，降低事件帶來的傷害或損失。

二、 外部防護：

1、 設置嚴密網路區隔、防火牆政策與導入入侵偵測，即時更新防毒 / 防駭軟體特徵碼，定期修補系統弱點以降低外部攻擊或駭客透過弱點入侵系統之風險威脅。

2、 為了避免因人員因使用VPN服務而造成帳號密碼外洩，導致駭客入侵的威脅，公司在2022年3月全面啟用多因素認證因子來強化人員的識別及認證，以提高連線存取安全性。且於2023年9月導入VPN（虛擬私人網路）的SSL憑證, 提升網路安全。

■資通安全管理之資源：

一、 具體成果與持續資源投入：

1、 自2021年起逐步建構完成網路行為偵測暨通報系統，可有效針對外部與內部網路攻擊、電腦病毒破壞或通訊異常行為即時監控及告警，已有具體成效。

2、 加入資安聯盟及臺灣電腦網路危機處理暨協調中心(TWCERT/CC) , 達成資安聯防作業。

3、 另外為配合公開發行公司配置適當人力資源及設備，於2023年3月完成資訊安

全專責單位設置(含人員編制-資安主管一員，資安人員一員)，專職於資訊安全制度之規劃、監控及執行資訊安全管理等作業。

4、 資安相關主管及人員於2023年皆有外派參加相關資安教育訓練。
5、 資安單位2023年共四次，定期每季都在企業永續發展委員會之風險管理組中報告每季資安執行狀況。
6、 於2023年上、下半年各安排一次外部弱點掃瞄 / 滲透測試。
7、 為了落實資訊安全觀念至每一位員工，公司提供實體課程及eLearning線上教學(94%上網學習率)
8、 透過一年兩次(Q2/Q4)的社交工程演練，模擬駭客的釣魚郵件，檢測員工資安風險意識，輔以資安宣導及教育訓練，來提升同仁對於資安的意識及警覺性。
9、 每季定期檢討閒置與特權帳號和郵件帳號使用、資訊系統的密碼皆有定期更新的機制，以加強資訊安全強度。
10、 不定期發佈有關病毒及駭客相關郵件訊息，提升同仁對於資安的意識及警覺性。
11、 於2023年3月導入新的備份管理系統，依3-2-1備份原則，為企業進行資訊系統的全面性保護。

二、中長期計畫：

持續評估導入 ISO 27001 資訊安全管理系統的可行性，承諾達到每年零資訊安全事件目標。

透過每年資訊安全防護計畫 / 方案逐步完善外，聚焦於流程制度、法令遵循、人員訓練及科技運用，強化資料、資訊系統、設備及網路通訊之安全及防護能力，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，以確保對股東、客戶的承諾，達到保證公司業務持續營運之目的。使能降低資訊安全風險對本公司所帶來的損失。

持續關注新的資安資訊、技術，將防禦或管理手法與時俱進，增強現有的資訊安全措施，以有效阻擋新型態的資安威脅，降低營運的風險，達成企業永續經營之目標。