資通安全政策及管理：

1. 資通安全管理策略與架構

企業資訊安全治理組織：本公司為落實資訊安全管理於 2020 年 8 月 5 日成立隸屬董事會之資訊安全委員會，協助董事會持續推動資訊安全管理之落實，負責制定資訊安全政策及管理、執行資訊安全工作之推展與政策規劃。資安委員會由獨立董事擔任召集人。基於資訊安全的重要性，權責單位每年定期檢討資安政策，且每年至少一次向董事會報告公司資訊安全治理與執行狀況。資安委員會於 2024 年 12 月 12 日召開一次會議，並於 2024 年 12 月 12 日將委員會 113 年度運作及執行情形向董事會報告。

本公司於 112 年 11 月 15 日設置資安主管一名及資安人員一名，負責資訊安全及實體安全規劃與相關的稽核事項，以及系統之協調、推動及監督等事項。

2. 資通安全政策

精益求精、提升資訊效度-

透過資訊可用、完整、保密(機密性 C、完整性 I、可用性 A)，提升營運績效。

共榮共存、安全分享資訊-

營運資訊運用不受地理限制(可用性 A)，於組織授範圍內，在內部及外部安全分享資訊。

實事求是、精確資訊內容-

營運資訊正確無誤(完整性 I)，提升決策品質。

創新求變、創造資訊價值-

不斷創新資訊運用方式，並確保公司機密資訊安全(機密性 C)。

3. 資訊安全管理

本公司定期依資訊安全風險評鑑與管理作業程序執行資安風險管理，辨識及分析資安風險與評估其等級，若超過可接受等級將採取風險處理及改善措施，以降低可能面臨之風險，並依循 PDCA 的管理循環以確保資安目標之達成，進而促使資安持續改善。

- 規劃（Plan）— 資安風險管理

（1）企業資訊安全風險評估

（2）資訊安全風險管理與對策制訂

（3）遵循資安國際標準（ISO27001）

- 執行（Do）— 多層資安防護

（1）資訊資產管理

(2) 存取控制
(3) 實體與環境安全管理
(4) 網路安全管理
(5) 資訊安全事故管理

➢ 檢查（Check）— 監控資安管理成效

(1) 資訊安全持續監控
(2) 資訊安全指標量化
(3) 資訊安全弱點掃描
(4) 資訊安全內部稽核
(5) 通過資安國際稽核認證

➢ 行動（Act）— 檢討與持續改善

(1) 資訊安全措施檢討改善
(2) 資訊安全教育訓練與宣導

4. 資通安全具體管理方案

(1) USB 管控：導入資產盤點工具，透過管理工具，管制 USB 隨身碟之使用，避免資料外洩及電腦病毒傳播。
(2) 異地備援系統規劃演練：資料定期備份；核心系統定期災難復原演練。
(3) 端點資安：依電腦類型，建置端點防毒措施，強化惡意軟體行為偵測。
(4) 主機弱掃：每年定期執行主機弱點掃描，修補資安漏洞。
(5) 滲透測試：每年定期執行主機滲透測試，修補資安漏洞。
(6) 網路資安：導入 FORTINET 防火牆：提昇網路資安防護力。
(7) 社交工程演練：模擬釣魚網站的手法進行演練，以加強員工的資安意識。
(8) 雙因子認證:提升外部連線安全性

5. 投入資通安全管理之資源

(1) 軟硬體盤點：導入資產盤點工具，透過管理工具管控，並每年一次進行盤點，以保證合法使用授權軟體及防範惡意軟體。
(2) 端點防護：每週檢查病毒碼更新及定期掃描。
(3) 威脅偵測服務：雲智維科技 — 建構一網管與資安整合中心服務。
(4) 災難復原演練：每年一次，核心系統災難復原演練。
(5) 主機弱掃：每年二次(初掃、複掃) 主機弱掃，修補資安漏洞。

6. 企業資訊安全措施推動執行成果

資安認證: 經外部單位實地審查結果，維持資訊安全管理標準
111 年 2 月 17 日 通過台灣檢驗科技公司(SGS)認證，取得 ISO 27001

資訊安全管理系統(ISMS)證書。有效期限為 2022/2/17~2025/2/17。
112 年 1 月 5 日　ISO 27001 證書資格延續。
113 年 1 月 12 日 ISO 27001 證書資格延續。

7. 企業資訊安全措施推動執行成果

(1)定期宣導：自動定期要求同仁更換系統密碼，以維帳號安全，並提醒釣魚信件封鎖。

(2)教育訓練：每年對內部同仁實施資訊安全相關的教育訓練課程。

課程名稱：ISO 27001 資安宣導
日期：2024.10.15
時數：1
人數：503 人

課程名稱：電子郵件安全與社交工程防範
日期：2024.10.30
時數：2
人數：4 人