資訊安全風險管控執行情形

一、資安風險管理架構：

本公司資訊安全風險管理之權責單位為資訊部，依規定設置資安主管及資安人員各一名。負責訂定公司內部資訊安全政策、執行規劃，並協調資安政策在集團內有效推動與落實。

資安政策執行狀況由本公司稽核室排列入年度稽核計畫，定期檢視落實情形；資安風險管理的權責單位每年定期將資安風險管控執行狀況提報本公司董事會。

二、資訊安全政策：

本公司資訊安全政策，包含以下三個面向：

制度建立：訂定資訊安全管理辦法，規範資安管理措施。

軟硬體建置：建置資安相關軟硬體設備。

人員培訓：建立全體同仁資安意識。

三、資訊安全具體管理措施：

公司集團員工及約聘僱人員皆須遵循下列各方面的資安規範：

資訊設備使用、密碼使用、公司電子郵件使用、網際網路使用、資訊處理、軟體使用與授權、防毒與資安防護軟體部署、遠端存取、資安事件管理、對外網路應用服務資安要求、公司資源使用等各方面。

四、投入資通安全管理之資源：

1.資通安全管理

資通安全專責人員定期組織並主持資訊安全會議，審視當前資訊安全問題，分析潛在威脅，確保公司資訊安全政策有效執行。定期對公司資訊系統進行風險評估，識別並優先處理高風險區域。

2.資安運營監控

資訊安全監控團隊，採用監控技術和工具，實現資訊安全事件監控。加強應急回應機制建設，確保在資訊安全事件發生時能夠迅速、有效地進行處置，降低損失。對於委外管理的資訊系統或服務，通過審核和監管

確保外部合作夥伴遵守公司的資訊安全規定。

3.弱點掃描與滲透測試

定期對公司的網路設備、應用系統及產品進行深度弱點或漏洞掃描，及時發現並修復安全性漏洞。加強對網站及系統的滲透進行測試，類比駭客攻擊行為，檢驗系統的安全防護能力，並根據測試結果進行針對性的加固。

4.年度資通安全教育訓練、災害復原計劃演練

定期對公司員工進行資訊安全意識教育和技能培訓，提高員工的安全防範意識和技能水準。每年舉行災難恢復演練，模擬多種可能的災難場景，檢驗災難恢復計畫的可行性和有效性，並根據演練結果不斷優化計畫。

2024 年進行資安相關培訓紀錄如下：

項目	總人次	備註
新人入職-資訊安全培訓	60 人次	川源(中國)資訊安全納入新人培訓。
資安訓練	22 人次	基士德環科、川源(中國)
災難恢復演練	2 場	基士德環科、川源(中國)

5.川源(中國)導入加密軟體

子公司川源(中國)已上線並導入加密軟體，確保公司敏感性資料在傳輸和存儲過程中得到充分的保護。並對加密軟體進行定期更新和維護，確保其安全性和穩定性。

6.資訊設備由行政處統一做固定資產管理，每年定期盤點。

7.公司電腦全數安裝防毒軟體，病毒碼定期更新。

8. 建立「資訊系統數據備份與還原計畫」，系統逐日自動進行備份，並有異地備份機制，以確保資訊系統之正常運作及資料保全完整，降低無預警之天災或人為災害所產生資料損失風險。資訊部門每年進行一次系統還原測試。

四、取得資安認證狀況：

2023/10 月➔川源(中國)機械有限公司取得 ISO27001 認證。

2022/11 月➔浙江川研環境科技有限公司取得 ISO27001 認證。