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，定期召開資安代表會議檢視公司資通安全議題。

2.資安運營監控

專責團隊負責即時監控與識別資通安全事件，強化資通安全事件之應變處理、資通系統或資通服務委外辦理之管理措施。

3.弱點掃描與滲透測試

對基士德集團之網路設備、應用系統及產品定期進行弱點掃描，對網站及系統進行滲透測試。

4.年度資通安全教育訓練、災害復原計劃演練

對基士德集團員工進行資通安全教育訓練；於公司每年執行災害復原演練會議，模擬災害情境演練以持續提升計畫有效性。

2023 年進行資安相關培訓紀錄如下：

項目	總人時	備註
資訊安全培訓	92	除了培訓課程之外，亦不時以公告方式提醒員工注意。

5.資訊設備由行政處統一做固定資產管理，每年定期盤點。

6.公司電腦全數安裝防毒軟體，病毒碼定期更新。

7.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。資訊處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。