資訊安全風險管控執行情形

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管理部資訊處，該處設置資訊主管，與專業資訊人員，負責訂定公司內部資訊安全政策、執行規劃、資安政策推動與落實等。

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。最近一次資安風險管控執行情形於 2022 年 12 月 22 日提報董事會，相關內容如下：

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。

資訊安全具體管理措施&投入資通安全管理之資源：

1. 資訊設備由行政處統一做固定資產管理，每年定期盤點。
2. 公司電腦全數安裝防毒軟體，病毒碼定期更新。
3. 建立「信息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。
4. 公司各個信息系統均採帳號管理，資料之存取及申請皆須依據簽核流程，經權責主管核准後始能使用及變更;各信息系統定期要求使用者更換密碼，維持帳號安全性。員工職務或部門異動時，帳號權限同步更新。
5. 建立「信息系統管理辦法」，規範資安事件的處理程序，以避免傷害擴大。若有偵測到病毒入侵或病毒郵件，亦即時於員工信息平台發布公告，預防員工誤開啟病毒郵件或連結。

6. 各部門主管督導資安措施落實狀況，強化員工資安認知。資訊處亦定期向員工宣導常見釣魚網站、勒索病毒手法。2022 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	42	除了培訓課程之外，亦不時以公告方式提醒員工注意。

7. 網路管理者隨時注意資訊安全以及網路設備的變動，檢討及調整防火牆設定、調整系統存取權限以反應最新的狀況。建立網路示警系統，針對網路重要端點發生異狀時能即刻發出警示，以利網管人員於特定異常事件發生時，採取有效的防範措施。

取得資安認證狀況：

2022/11 月➔子公司-浙江川研環境科技有限公司取得 ISO27001 認證。