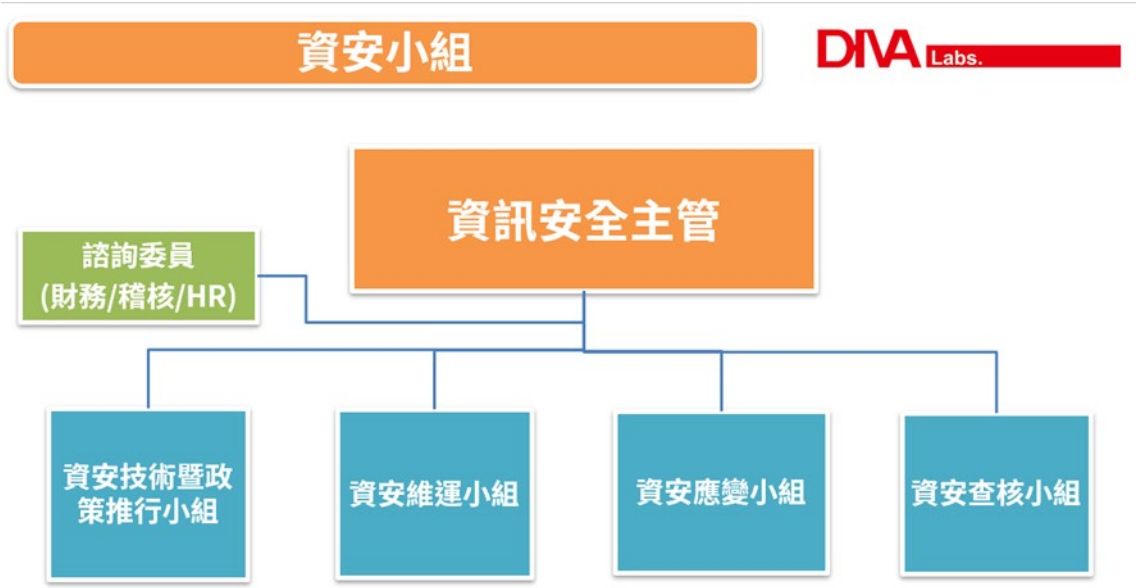
資通安全風險管理

資通安全管理策略與架構

為確保資訊安全管理制度之執行，落實資訊安全政策，本公司已於 2023 年成立資訊安全組織，資訊安全組織架構如下圖所示：



資訊安全組織為非隸屬使用者單位之獨立單位，負責統籌並執行資訊安全政策，宣導資訊安全訊息，提升員工資安意識，蒐集及改進組織資訊安全管理系統績效及有效性之技術、產品或程序等。資安單位每年就內部控制制度—資訊系統循環，進行資訊安全查核，評估公司資訊作業內部控制之有效性。

資安政策

為落實資安管理，公司訂有內部控制制度—資訊系統循環及 IT 資訊安全規則，藉由全體同仁共同努力期望達成下列政策目標

(1)確保資訊資產之機密性、完整性。

(2)確保依據部門職能規範資料存取。

(3)確保資訊系統之持續運作。

(4)防止未經授權修改或使用資料與系統。

(5)定期執行資安稽核作業，確保資訊安全落實執行。

具體管理方法

網際網路資安管控	資料存取管控	應變復原機制	宣導及檢核
→ 架設防火牆（Firewall）	→ 電腦設備應有專人保管，並設定帳號與密碼	→ 定期檢視緊急應變計劃	→ 隨時宣導資訊安全資訊，提升員工資安意識
→ 定期對電腦系統及資料儲存媒體進行病毒掃瞄	→ 依據職能分別賦予不同存取權限	→ 每年定期演練系統復原	→ 每年定期執行資通安全檢查，呈報董事長
→ 各項網路服務之使用應依據資訊安全政策執行	→ 調離人員取消原有權限	→ 建立系統備份機制，落實異地備份	
→ 定期覆核各項網路服務項目之System Log，追蹤異常之情形	→ 設備報廢前應先將機密性、敏感性資料及版權軟體移除或覆寫	→ 定期檢討電腦網路安全控制措施	
	→ 遠端登入管理資訊系統應經適當之核准		

投入資通安全管理之資源

(1)本公司資安小組成員共有七位，其中設有資訊安全主管及資訊安全專責人員各一名。每半年開會一次並每年和董事會報告資訊安全管理執行情況。

(2)為妥善保護本公司資訊安全管理體系內之資訊資產，對於資訊資產訂定及落實相關規範並執行風險評鑑程序，以確認資訊資產的風險水準，透過風險評鑑結果以及內部會議決定風險事項之處理措施，以達到風險能有效降低、移轉、消除甚至接受該風險。

每年並檢視各項法規及評估公司內部的資訊安全規章以確保符合法規及有效性，定期宣導相關資安規章，避免同仁違反內部規範造成公司損害。

在供應鏈環境，要求與第三方服務廠商簽訂合約，有要求其遵守保密及網路安

全規定。

另本公司亦定期舉辦電子郵件社交工程演練，對員工進行電子郵件收發等相關資訊安全知識之教育訓練，以降低員工誤點擊惡意郵件之風險。透過各類課程的進行，除提升同仁資訊安全意識，亦確保資訊安全觀念能融入日常作業中。

2024 年度執行情形

1. 資安小組(每半年一次)召開，於 2024 年度分別已於 4 月、10 月召開 2 次會議，並向總經理彙報管理成效。
2. 本公司一年至少一次向董事會/審計委員會彙報資安管理成效、資安相關議題及方向，已於 2024 年 10 月執行報告。
3. 本公司內部參考 ISO 27001 資訊國際安全標準，定期執行社交工程演練、實施源碼檢測、導入多因子認證機制、持續進行數位還原演練等與框架對應之執行作業。