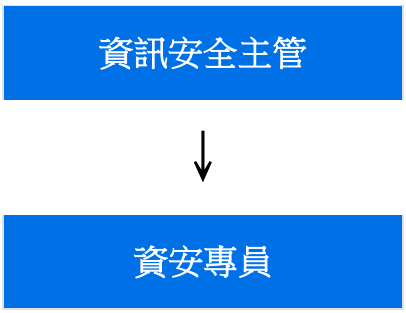
資通安全管理組織架構

本公司由資訊安全主管及資安專員，負責規劃執行及分析資安相關問題。



資通安全管理策略與架構

依據金融監督管理委員會公開發行公司年報應行記載事項準則第 18 條第 6 款第 1 目：敘明資通安全風險管理架構、資通安全政策、具體管理方案等，請參閱本公司最新年報第 76~79 頁。

投入資通安全管理資源

1. 人力配置：資安主管一位及資安專員一位。

2. 集團(總部與海外七廠區)每年投入台幣 300+萬購買第三方管理式整合性資安防護服務 UTM/MDR/IPVPN。

3. 資安專員外訓取得國際證照。

4. 積極聘請雲端逢甲大學雲端資安專家來公司內訓提升資安意識。

5. 除公司的季會外，每月另舉行資安長與資安專員 IT 內部資安月會研討市場資安事件技術吸取經驗後舉辦員工相應的資安教育訓練。

2024 年	資安議題	開會人數
1 月	2024 年台灣政府部門每日平均遭受約 240 萬次網路攻擊，較 2023 年的 120 萬次翻倍。探討規劃年度強化公司資安預算是否足夠因應。	2

2024 年	資安議題	開會人數
2 月	針對鴻海集團旗下半導體設備大廠京鼎 1/16 公司網站遭勒索軟體集團 LockBit 入侵探討公司異地備份政策是否完善	2
3 月	Deepfake 橫行，探討如何提升公司員工社交工程辨識能力	2
4 月	針對花蓮大地震發生後，假借地震捐款名義的釣魚網站增加，詐騙善款。規劃員工資安教育訓練	2
5 月	台灣醫療機構遭駭客攻擊，興起零信任(zero trust)議題的探討	2
6 月	台灣半導體業利潤豐厚引來國際駭客攻擊竊取資料，重新檢視內部網路的分段	2
7 月	勒索軟體攻擊增加，全球活躍的勒索軟體集團超過 75 個，較 2023 年成長 70%。重新檢討公司目前的線上與離線備份程序。	2
8 月	國內大型企業雲端帳號外洩，探討公司系統密碼輪替強制政策是否足以因應	2
9 月	有聽聞 SQL injection 式攻擊，探討目前 ERP 系統對此類攻擊的防護力，是否部屬 WAF(web 應用防火牆)	2
10 月	生成式 AI 輕易快速繁殖各類詐騙釣魚網站，探討擷取一些案例與員工分享的規劃	2
11 月	駭客針對 5G 核心網路進行滲透測試，企圖植入惡意軟體。針對此案例重新評估公司與電信公司簽約的防火牆 UTM 授權是否完備	2
12 月	大型跨年晚會期間，票務與直播系統易遭駭客侵入詐騙。探討如何特別提醒同仁這類事件。	2

6. 規劃採購社交工程服務強化員工資安意識。畢竟根據統計 95%的資安事件都與人有關，另外 43%的資安事件來自於內部。