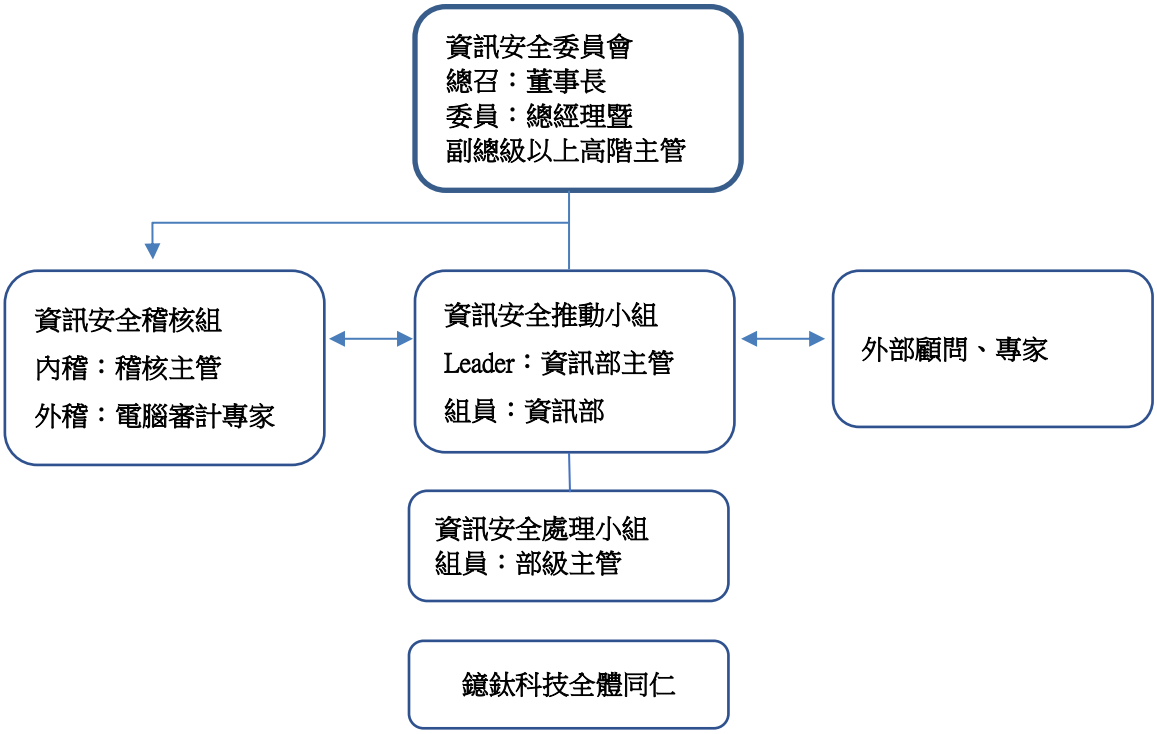
資通安全風險管理架構及運作情形

一、資通安全風險管理架構：

本公司於 108 年制定資訊安全政策管理辦法，設立資訊安全委員會推動資訊安全改革，透過每年檢視、評估及監督資訊安全規章及程序之設定及執行，降低資安事故發生之機率及管理事故造成之風險至可接受的程度，確保公司業務正常運作、資訊資產免於各種威脅與破壞。本公司已執行資訊安全技術檢測，針對網路架構可用性、安全性、機密性等進行安全防護強度評估，並發掘潛在安全漏洞及提出強化建議報告，於 109 年開始成立資安改善專案，公司依據專業建議進行資安架構修補事宜，並按季向董事會報告執行進度，於 111 年資安改善之軟硬體架設已大致完善，並已訂定及調整相關資安政策，期能提昇本公司資安防護能力。



組織名稱	職責
資訊安全委員會	1.資訊安全政策之擬定、核轉及督導 2.資訊安全責任之分配及協調 3.資訊資產保護事項之監督 4.資訊安全事件之檢討及監督 5.檢討、審核並頒行資訊安全政策 6.了解、審查資訊安全執行成效及相關資安議題 7.審核內部稽核成果
資訊安全推動小組	1.跨部門資訊安全事項權責分工之協調 2.應採用之資訊安全技術、方法及程序之協調研議 3.整體資訊安全措施之協調研議 4.資訊安全計畫之協調研議 5.其他重要資訊安全事項之協調研議 6.規劃、執行、稽核並改善資訊安全管理系統之運行 7.監督日常資訊安全事務運作並協助各小組執行資訊安全委員會之決議事項 8.審核執行風險管理機制，包含風險評鑑與風險處理計畫 9.協助稽核作業並報告稽核成果及相關建議事項予資訊安全委員會 10.協助及督導資訊安全政策與規範之修訂作業 11.監督年度資訊安全教育訓練，並追蹤其成效與紀錄 12.監督彙整業務持續運作計畫及其演練紀錄
資訊安全稽核小組	1.稽核資訊安全規範是否符合內稽內控要求 2.稽核資訊安全規範是否符合相關法律要求 3.稽核資安作業執行是否符合資安政策規範要求
資訊安全處理小組	資安事件發生時，BU 所屬資訊安全處理小組與資訊安全推動小組配合處理資安事件
外部顧問、專家	資訊安全推動小組可適時請求外部資訊安全顧問、專家幫助與咨詢
本公司全體同仁	所有員工皆有責任遵循本政策並記錄及通報資訊安全事件及任何明顯之安全弱點

二、資通安全政策：

1.保護資訊避免未經授權的使用。

2.確保資訊的隱密性(機密性)、完整性及可用性。

3.符合法律的要求。

4.制定、執行及維護公司業務持續運作。

5.進行資訊安全訓練，提升資安意識。

6.通報及處置所有違反資訊安全的事件。

三、具體管理方案：

1.本公司已加入 SP-ISAC 科學園區資安資訊分享與分析中心，ISAC 如有重大資訊資訊，會使用 E-mail 通知及分享。

2.本公司已制訂施行之資通安全管理規章辦法：

管理面向	管理規章及程序	
資產安全	硬體/軟體控管	軟體使用管理辦法 資訊設備維護與管理辦法 軟體清冊 硬體設備清冊
	基礎設施	電腦機房控管辦法 網路架構圖
	人員	資訊部門資安作業辦法 資訊部門組織圖 資訊部門人員職掌
電腦系統安全	存取控制管理辦法	
實體及環境安全	實體與環境安全管理辦法	
網路安全	網路安全管理辦法 通信與作業管理辦法	
業務持續營運計畫	營運持續管理辦法 資訊安全事件管理辦法 還原演練	

四、投入資通安全管理之資源：

本公司已成立資訊安全推動小組，由資訊部主管帶領 3 位資訊部同仁執行資訊安全委員會所推動之管理措施。

111 年已召開 2 次資安會議，由資訊安全推動小組提出上網行為資訊安全問卷調查結果、可攜式儲存控管行為模式，向高層提出管理建議並取得同意後予以執行。

113 年採用端點軟體記錄外網存取記錄，每月不定期隨機抽查。

具體成效：

1. 總廠網路採用新技術之身份驗證，內/外上網存取依據使用者帳號控管，可防止未授權電腦存取網路實作 VLan 且限制各部門網路互不存取，如發生資訊事件時可讓影響限制於單一部門。
2. 限制外網存取行為，針對雲端空間、雲端 mail 於 111 年 4 月開始禁止使用。
3. 已制定及推行資安相關管理辦法。
4. 強化防火牆防禦能力
5. 限制及管控 USB 存取
6. 不定期宣導及網頁資訊分享，強化同仁資安意識