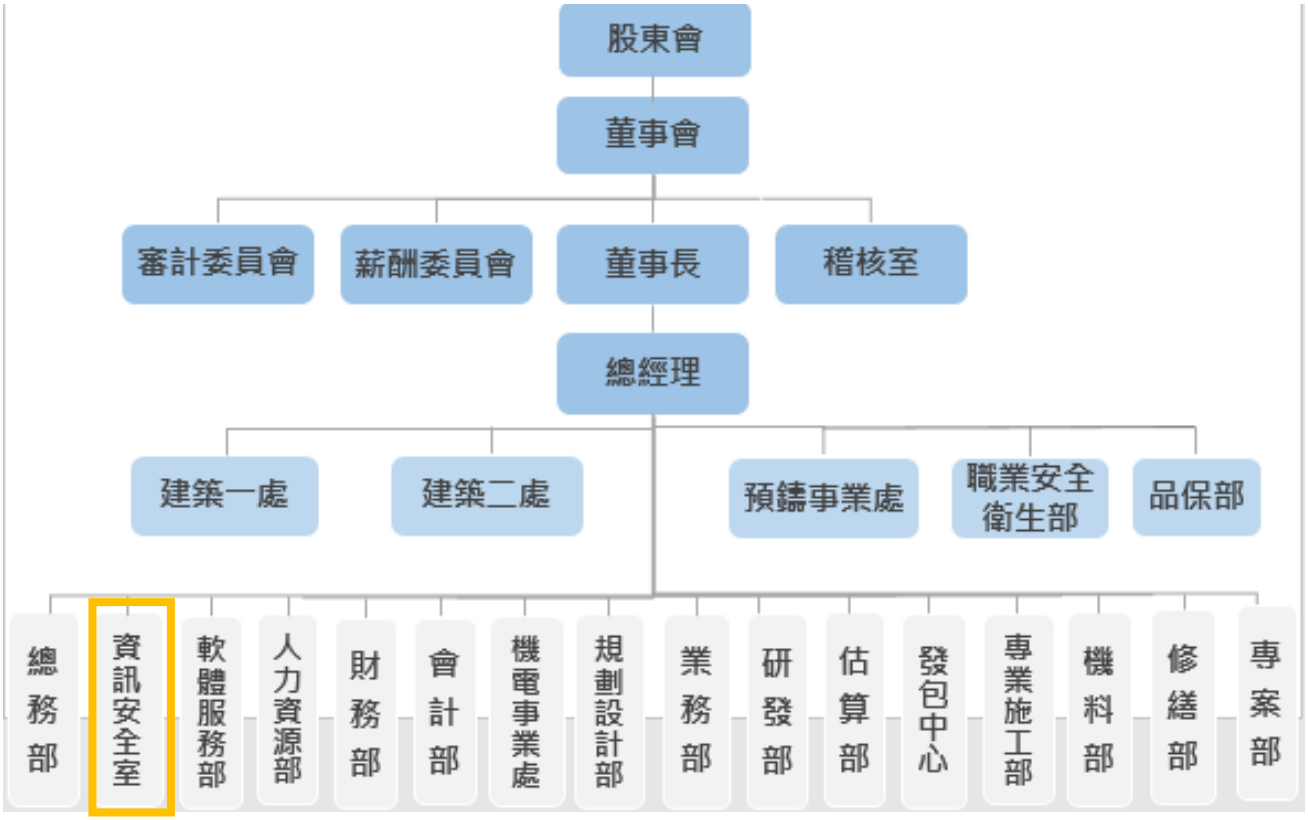
資通安全管理：

(一)資通安全風險管理架構



資訊安全室定期召開管理審查會議，審核資安風險分析結果及採取對應的防護措施與方策，確保資訊安全管理體系持續運作的適用性、適切性及有效性。每年向總經理彙報資安管理成效及資安策略方向，督導資訊安全及網路安全策略，定期檢討修正，稽核單位定期查核資通安全執行情形，稽核報告定期提報董事會。

(二)資通安全管理，三大構面推動

1.政策面及管理面：

- 成立資通安全推動組織及制訂資安目標並設定資安的專責人員，已於 2023/10/31 完成。
- 訂定人員裝置及使用管理規範。
- 訂定資訊作業委外安全管理程序。
- 訂定內部資訊安全稽核機制。
- 業務持續運作演練、建立備份機制及異地備源計畫。
- 鑑別法遵及契約之要求。
- 資通系統安全盤點及風險評估。

- 資安事件緊急應變計畫及通報作業程序 2023/12/31 完成(詳載於公司網站)。

2.技術面：

因應近年勒索病毒及駭客攻擊事件頻傳，本公司於 2021/09 花費 126 萬在各專案工地完成防火牆建置以強化資訊安全，2022/09 規劃更新台北營運總部防火牆，用以強化網路 Intranet 及 internet 資訊安全機制，並於 2023/7/10 完成總部、工廠、工地及個人 SSLVPN 之防火牆建置整合。

- 定期安全性檢測並完成系統弱點之修補。
- 資通安全防護及控制
- 實體安全管控
- 資安要求納入資通系統開發及維護需求規格（含委外開發之資通系統）

3.資安認知訓練及社交工程：

為讓全體同仁瞭解資通安全的重要性及全員皆為資訊安全的一份子，不僅新到職員工強制資安課程及測試外，未來規劃定期對所有同仁進行資安教育訓練，以提高資訊安全之認知及工作上保持資訊安全的警覺性。

- 定期資通安全教育訓練。
- 資安專職人員將外訓資通安全專業課程訓練（如：CISSP、CISM、CEH）
- 規劃定期辦理電子郵件社交工程測試演練。

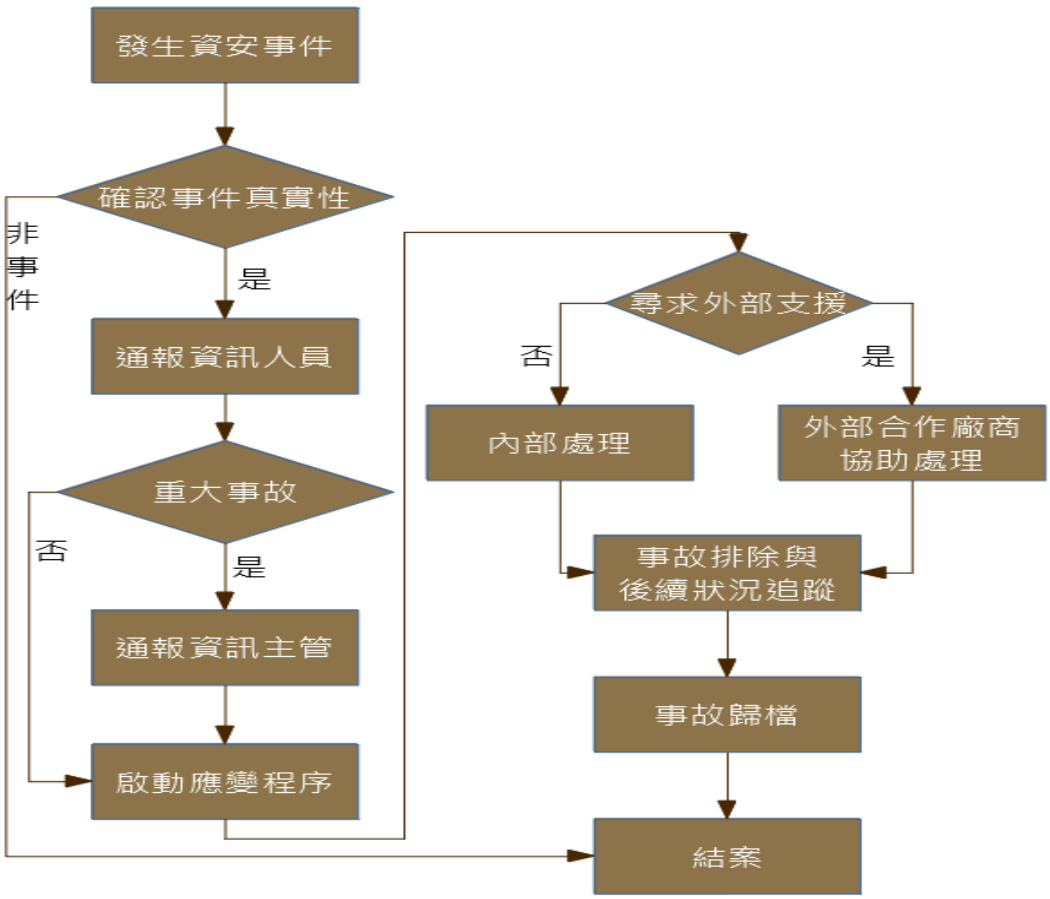
（三）本公司目前資訊安全執行相關具體措施如下：

項目	具體管理方式
防火牆防護	• 防火牆設定連線規則。 • 如有特殊連線需求需額外申請開放。 • 監控分析防火牆數據報告。
使用者上網控管機制	• 使用自動網站防護系統控管使用者上網行為。 • 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網
防毒軟體	• 使用多種防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	• 作業系統自動更新，因故未更新者，由資訊部協助更新。
郵件安全管控	• 有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。

項目	具體管理方式
	• 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
網站防護機制	• 網站有防火牆裝置阻擋外部網路攻擊。
資料備份機制	• 重要資訊系統資料庫皆設定每日完整備份、每小時差異備份。
異地備份機制	• 伺服器與各項資訊系統備份檔，透過 intranet 存放 IDC。
重要檔案上傳伺服器	• 公司內各部門重要檔案上傳伺服器存放，由資訊部統一備份保存。
資訊中心檢查紀錄表	• 資訊中心檢查紀錄表紀錄機房溫溼度、資料備份、防毒軟體更新、網路流量等紀錄。

(四)資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行。



(1)112 年度，因重大資通安全事件所遭受之損失：無。

(2)可能影響及因應措施：

本公司已建置資通安全環境、強化資安防護設備並定期檢討資通安全防護計畫，迄今未曾因重大資通安全事件遭受損失，預計未來亦無因重大資通安全事件而受損害。