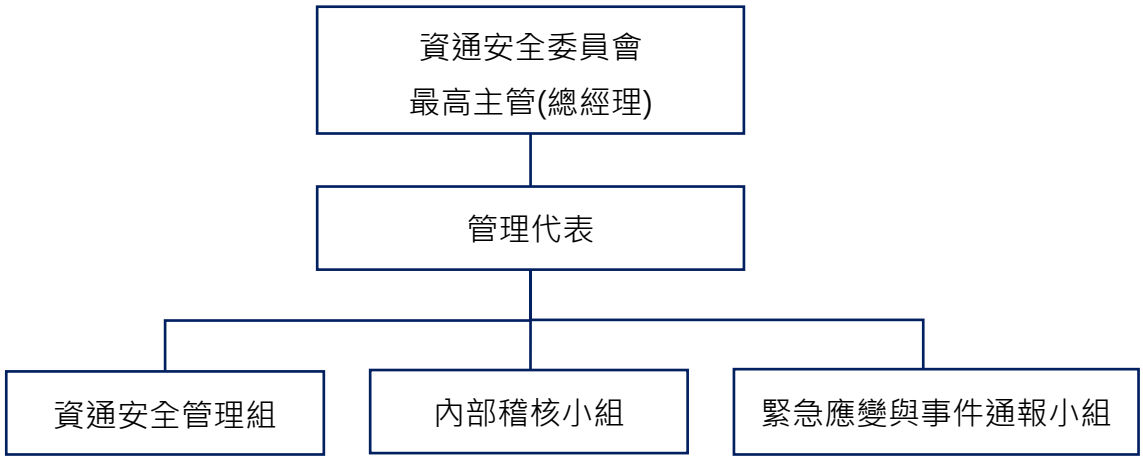
資通安全管理

1.資通安全架構

為提升資訊安全管理，本公司成立資通安全管理委員會，指派公司各部門資訊安全管理人員，每年定期召開資通安全管理會議，並由資訊主管每年定期 呈報資訊安全成果。



2.資通安全政策：

A.資通安全管理策略

1. 恪遵法令訂定相關資通安全管理規章，對本公司資訊資產提供適當的保護措施，以確保其機密性、完整性、可用性及法律遵循性。
2. 定期評估各種人為及天然災害對本公司資訊資產之影響，並訂定重要資訊資產及關鍵性業務之防災對策及災變復原計劃，以確保本公司業務持續運作。
3. 督導本公司同仁落實資訊安全防護工作，建立資訊安全，人人有責觀念，提升各業務部門及人員對資訊安全之認知。
4. 要求本公司全體同仁以及使用或連結本公司電腦系統之往來廠商，應確實遵守本公司資訊安全之相關規定，如有違反者，視其情形分別依本公司規定懲處或依契約罰則辦理外，情節嚴重者另將受相關法律追訴。

B.持續改善架構與資通安全風險管理

本公司資通安全管理之組織運作模式，採 PDCA（Plan-Do-Check-Act）循環式管理架構，以確保資通安全目標之有效達成並持續精進，並定期透過資通安全委員會彙整及回報各項資通安全執行成效。

（一） Plan｜規劃階段

- 建置並持續維運完整之資訊安全管理系統（ISMS），已於 **113 年 7 月取得 ISO/IEC 27001 國際認證**（證書有效期間：113/7/18～116/7/17），從制度面、技術面及程序面系統性降低企業資安風險。

（二） Do｜執行階段

- 每年上、下半年各召開一次資通安全會議，由各部門指派代表參與，推動並執行資通安全管理措施、教育訓練及宣導活動，以確保公司重要資訊資產之安全。
- 持續投入資通安全相關資源，包含人力配置、資訊基礎架構建置，以及主機端與個人端之防毒、防駭、防護軟體與設備，全面提升防護能力。
- 為提升遠端連線安全性，本公司於 2025 年導入 VPN 多因子認證（MFA），透過多重身分驗證機制（如動態密碼、行動裝置驗證等），降低帳號冒用及憑證外洩風險。

（三） Check｜查核階段

- 由資通安全主管指派資通安全專責人員，定期檢核公司資通安全執行情形，並配合外部資通安全專業廠商進行定期稽核與檢測，以確認控制措施之有效性。

（四） Act｜改善階段

- 依內外部查核結果、資通安全事件及風險評估結果，滾動式檢討並修訂資通安全管理制度、作業流程與防護措施，持續精進整體資通安全防護能力。
- 督導全體同仁及往來廠商確實遵循資通安全相關規定，針對違規或缺失事項，依公司規定或契約約定採取必要之矯正與預防措施，以避免類似風險再次發生。

3.具體實施措施：

管理方案：本公司針對公司營運類資產如維護資訊系統及網路設備等資訊設備，皆有簽訂維護及保固合約且因應資訊安全所面臨的挑戰，如 APT 進階持續性攻擊、DDoS 攻擊、勒索軟體、社交工程攻擊及竊取資訊等資安議題，每年依公司資訊安全政策持續關注資訊環境變化趨勢，並參考技術文刊資料，擬定資訊安全防護機制與方案，強化公司同仁資安危機意識及資安處理人員應變能力，以期能事先防範及第一時間有效偵測並止決擴散，並確實執行以下相關資訊安全管理措施辦法，如下表:

資通安全管理措施		
類型	**說明**	**相關作業**
人員安全管理	人員帳號，權限管理，教育訓練	●人員帳號權限管理與審核 ●人員離職調任帳號刪除 ●資訊安全教育訓練 ●VPN 多因子認證
電腦系統安全管理	系統安全管理，資料安全管理，電腦病毒和惡意軟體之防範	●電腦作業系統設定與管制 ● ERP 系統每日備份和每日異地備份 ●使用合法軟體，隨時更新病毒碼
網路安全管理	網路安全規劃與管理，網路使用者管理，電子郵件安全管理	●建置防火牆及防毒系統 ●定期資訊安全宣導 ●來路不明電子郵件，不隨意打開 ●定期進行社交工程演練
系統存取控制	人員存取內外部系統及資料傳輸管道之控制措施	●系統存取權限以執行業務及職務所需為限需為限 ●系統使用者開啟帳號後，使用者每隔半年需更改密碼 ●使用者權限異動應提出申請同意後，資訊始得修改
資訊資產之安全管理	資訊資產移轉及報廢之處置	●資訊設備報廢，應在報廢前移除所有硬碟內資料並記錄報廢申請單 ●資訊設備移轉應記錄到移轉申請表
系統發展與維護之安全管理	一般電腦系統及委外作業安全管理	●應用系統程式更新，由各應用系統負責人配合 ●委外資訊廠商除安全管理責任外，也應落實保密作為
實體及環境安全管理	電腦設備安全管理，電源，機房主機管理，消防系統的設置	●電腦機房專人負責，定期維護保養及測試 ●提供不斷電系統，消防設備 ●電腦機房實施門禁管控

		●增加 24 小時錄影監控
業務永續運作計畫之規劃及管理	備援及回復作業	●每年應進行備份備援，回復作業之測試演練，包含核心系統、網路設備與 UPS 電力
資訊安全稽核	確認資訊安全管理作業之執行情形	●發現有資訊安全事件時，應迅速通報權責主管單位及相關人員處理

4.資訊安全所投入之資源

持續維運資訊安全管理系統（ISMS）

自 2024 年取得 ISO 27001 認證後，公司持續維運資訊安全管理系統（ISMS），並每年投入相應資源，以確保系統之有效性、適切性與合規性，相關作業如下：

A.管理審查（Management Review）

由高階管理層每年至少召開一次管理審查會議，檢視 ISMS 運作成效、重大資安議題與資源需求。並定期召開資訊安全會議，由各部門代表參與，檢討年度資安措施、教育訓練與宣導執行情形，確保關鍵資訊資產受到適當保護。

B.內部稽核（Internal Audit）

每年依 ISMS 要求執行內部稽核，以確認資訊安全控制是否符合法規與公司政策。資訊部門專責人員並與外部資安廠商合作，定期檢視資安狀況，確保改善措施落實。

C.風險評鑑與處理（Risk Assessment & Risk Treatment）

依據 ISMS 規定每年進行風險評鑑並依風險評鑑結果制定「資安改善計畫」，設定責任單位、完成期限、控制措施。

定期追蹤改善進度至資訊安全委員會。對高風險項目提出改善成果佐證。

持續投入資源於資訊安全相關領域，民國 114 年度較民國 113 年投入費用增加 1 倍，資源投入事項包含人力、技術面之基礎架構及加強主機端、

個人端防駭及防毒設備及軟體、情資監控分析等，全面提升資訊安全能力。

D.政策與程序文件檢視（Policy & Procedure Review）

每年至少檢討一次資訊安全政策及相關程序文件，依營運與技術需求適時修訂。113 年亦完成公司與工廠防火牆、Switch、無線 AP 全面升級至 Fortinet，並導入 Security Fabric 以強化跨環境整合式安全管理。

E.教育訓練與意識提升（Training & Awareness）

依職務別規劃資安訓練課程與時數，持續提升人員資安素養，降低人為風險：

- 各級主管：每年至少 1 次
- 資訊人員：每年 2 小時
- 資通安全專職人員：每年 12 小時
- 電腦使用者：每年至少 1 次
- 非電腦使用者（如專櫃 / 生產單位）: 不定期於內部會議宣導

F. 持續改善與矯正 / 預防措施（Corrective & Preventive Actions）

針對內部稽核結果、資安事件或風險評鑑發現事項，提出改善計畫並追蹤執行，以確保控制持續有效。

G.事件管理與通報（Incident Management）

建立完整之事件通報、分析、應變與紀錄流程，確保資訊安全事件能即時處理與回復。

H.合規性確認（Compliance Checks）

定期檢查並確認公司持續符合適用的法律法規、契約義務與相關資訊安全要求。

I.供應商管理檢查（Supplier Evaluation & Review）

定期評估關鍵供應商之資安管理與合規性，確保外部供應鏈不成為資安風險來源。

5.最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施： 民國 114 年度本公司並無因重大資通安全事件而遭受損失。