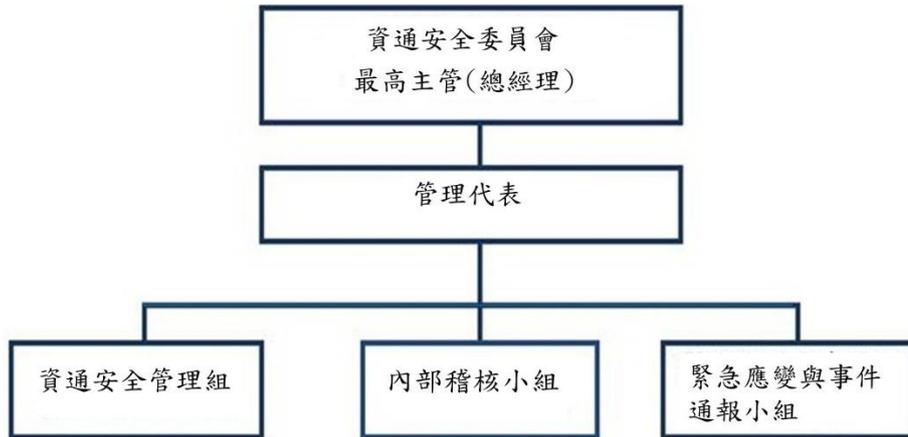


資通安全管理

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

(1)組織運作模式-採 PDCA (Plan-Do-Check-Act) 循環式管理，確保資通安全目標之達成且持續改善，並定期透過資通安全委員會回報執行成效。

(2)規畫階段：持續規劃建立完整的資訊安全管理系統 (ISMS)，並已於 113 年 7 月取得國際資安管理系統認證 (ISO 27001)，目前證書有效期為 113 年 7 月 18 日到 116 年 7 月 17 日，從系統面、技術面、程序面降低企業資安威脅。

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	<ul style="list-style-type: none"> ● 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
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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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
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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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
業務永續運作計畫之規劃及管理	備援及回復作業	<ul style="list-style-type: none"> ● 每年應進行備份備援，回復作業之測試演練
資訊安全稽核	確認資訊安全管理作業之執行情形	<ul style="list-style-type: none"> ● 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

- A. 每年定期召開資訊安全會議，各部門派代表參加，檢討及執行資訊安全措施、教育訓練及宣導等改善作為，確保公司重要機密資訊不外洩。
- B. 資訊部門二人負責資安管理，檢核資安狀況，且配合外部資安廠商定期檢核資安情形。
- C. 持續投入資源於資訊安全相關領域，民國 113 年度較民國 112 年投入費用成長 21%，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. 提高資訊安全，於 113 年已將公司及工廠防火牆、SWITCH、無線 AP 皆更換為 Fortinet，導入安全織網(Security Fabric)，從物聯網到雲端，實現對整個組織安全的控制、整合並輕鬆管理。

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 113 年度本公司並無因重大資通安全事件而遭受損失。