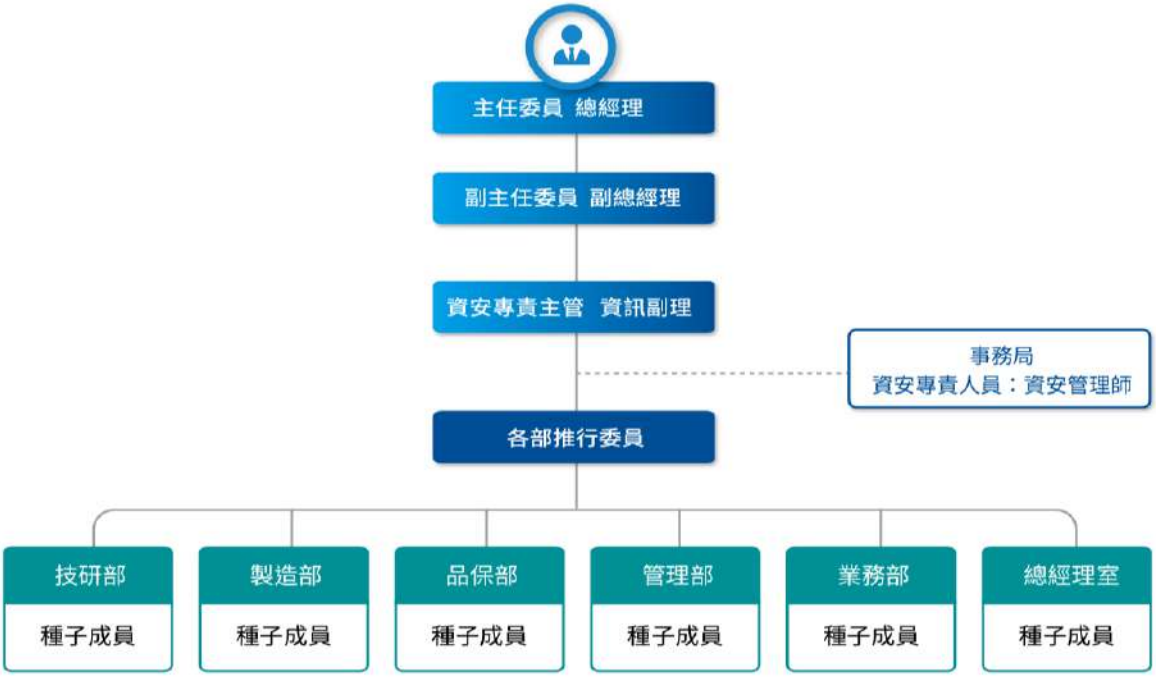
資訊安全管理

1. 資訊安全風險管理架構

本公司成立有風險管理委員會，每年定期進行風險評估，107 年 8 月起因應資訊系統設備可能故障或遭受入侵影響，增加營運中斷之風險，故加強各項資訊安全防護措施，訂定管理目標：以提升資訊管理效率，管理目標定期進行績效檢討管控。

本公司訂定「資訊作業管理辦法」、「可攜式儲存媒體管理辦法」、「電子郵件作業」等相關作業標準，包括：應用系統開發與維護資料存取、備份機制、病毒與網路入侵防護、機房設置不斷電系統、門禁系統、攜帶式硬碟及隨身碟管理、電子郵件使用權限管理等。同仁依據公司規定執行並落實權限控管，以確保資訊安全的活動及服務。

自 111 年 1 月成立資訊安全管理委員會，由總經理、副總經理擔任主任委員、副主任委員，並指定總經理室副理及管理師擔任資安專責主管及資安專責人員，以主導並維護資訊安全政策執行，資訊安全管理委員會組織圖如下：

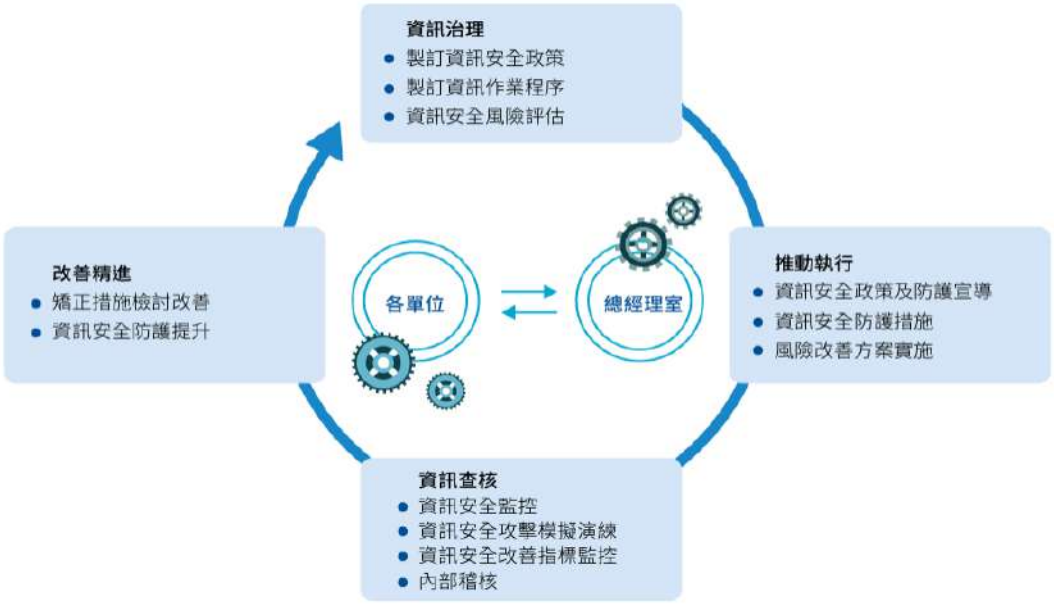


2. 本公司「資訊作業管理辦法」訂定資訊安全政策如下：

本公司為從事汽、機車零件及自行車零件製造之企業，為防止資訊系統受未經授權之存取、控制或其他侵害，並確保資訊機密性、完整性及可用性，制訂本政策如下，供全體同仁共同遵循：

1. 符合政府資訊安全相關法規之要求。
2. 建立系統及網路的權限，防止未經授權之使用。
3. 提供合適的資訊軟硬體，維持公司之正常運作。
4. 建立系統資料備份機制，驗證資料回復的可行性及正確性。
5. 建立資訊安全防護措施，預防病毒及駭客入侵。
6. 建立資訊安全通報機制，降低公司營運的影響。
7. 員工資訊安全教育訓練，強化資訊安全的認知。

3. 資訊安全風險管理與持續改善流程圖



4. 具體管理方案

網路安全

- 強化網路防火牆與網路控管，防止電腦病毒跨機台及跨廠區擴散

112 年執行狀況

- 建置防火牆進行即時監控，異常即時回報、排除

裝置安全

- 每兩年至少 1 次弱點偵測與滲透測試
- 依電腦類型建置端點防毒措施，強化惡意軟體行為偵測

112 年執行狀況

- 111 年已實施弱點偵測與滲透測試，預計安排於 113 年中實施。
- 每周病毒碼更新與掃描

資訊安全保護技術強化

- 文件及資料加密控管及有效追蹤

112 年執行狀況

- 依部門職務設定存取權限
- 電子郵件使用權限管理
- 攜帶式硬體及隨身碟管理

教育訓練與宣導

- 各單位每年至少 1 次實施資訊安全宣導
- 每年至少 1 次實施資訊安全緊急應變演練

112 年執行狀況

- 112 年資訊安全宣導共 150 人次
- 112 年 5 月已實施資訊系統遭受入侵應變演練，下次實施日期為 113 年 5 月

5. 投入資通安全管理之資源

(1) 人力資源：本公司資訊安全作業執行人力包括主任委員、副主任委員、資安專責主管、資安專責人員、各部門推行委員及種子共 23 人。

(2) 資安設備：防火牆、防毒軟體、網路自動防禦系統、郵件過濾系統、應用系統開發與維護資料存取、行動媒體管理、存取管控及密碼管理、備份系統及雲端備存管理等。

(3) 實體環境建置機房門禁與不斷電系統等。

6. 即使本公司已建立上述管理作業流程與許多資安防護措施，但無法保證其控管或維持公司製造、營運及會計等重要企業功能之電腦系統，能完全避免來自任何第三方癱瘓系統的網路攻擊。

本公司將透過持續檢視和評估資訊相關的作業標準，以確保其適當性和有效性；透過內部每年各單位至少進行 1 次之資訊安全訓練宣導，如不開啟來路不明檔案、不隨意安裝不明程式、不任意連結網站…等，以提高各單位使用者養成辨識資訊安全能力及良好的操作習慣；定期進行模擬資訊系統遭受入侵災害復原演練，並進行演練結果檢討，必要時檢討修訂原管理作業流程及增加必要設施，以降低可能發生不法入侵資訊系統的風險。

7、本公司 112 年度並無重大資安風險發生之情形。