# 怡利電子工業股份有限公司

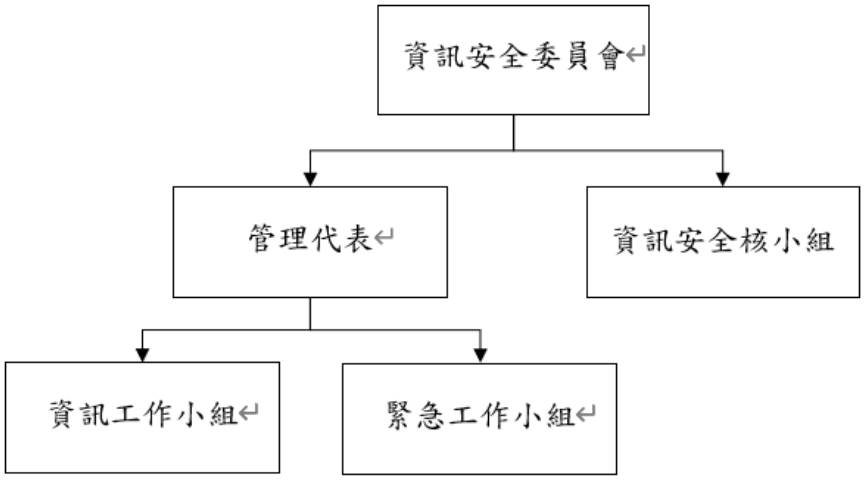
# 資訊安全政策及管理方案

## 一、資訊安全風險管理架構

為促進本公司資訊安全管理制度執行之有效性，已於 109 年 1 月 31 日成立「資訊安全委員會」，由總管理處主管擔任召集人，每年定期或視需要召開會議，審查資訊安全管理相關事宜，使制度能有效達成既定之目標，增進業務運作之安全。

本公司資訊安全權責單位為資訊室，由部門主管擔任資訊安全委員會執行祕書與資訊工作小組、緊急處理小組組長，部門人員擔任資訊工作小組、緊急處理小組之成員，主要任務為負責資訊安全管理制度之規劃、執行、監控與改善資及處理資訊安全事件。資訊安全核小組由稽核室擔任，負責評估與查核資訊安全管理制度之執行狀況，每年至少執行一次資訊安全內部稽核活動。

資訊安全委員會每年至少召開一次管理審查會議，主要內容為檢討資訊安全政策、內外部關注者議題、 稽核結果報告、風險評鑑與持續改善機會有關之決策。最近一次內部稽核已於 112 年 4 月 14 日完成。管理審查會議報告已於 112 年 5 月 10 日完成。




資訊安全委員會架構圖

## 二、資訊安全政策

**目的:**

本公司為強化資訊安全管理，確保本公司所屬之資訊資產的機密性、完整性及可用性，以提供資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特訂定資訊安全政策規範。

**願景與目標:**

1. 資訊安全政策願景：

   強化人員認知、避免資料外洩

   落實日常維運、確保服務可用

2. 依據資訊安全政策願景，擬定資訊安全目標如下：
   - 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
   - 保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整。
   - 定期進行內部稽核，確保相關作業皆能確實落實。
   - 確保本公司關鍵核心系統維持一定水準的系統可用性。.
3. 應針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間以及結果評估方式與評估結果，相關監督與量測程序，應遵循本公司”監督與量測管理辦法”IS-I15 辦理。
4. 資訊工作小組應於管理審查會議中，針對資訊安全目標有效性量測結果，向資訊安全委員會召集人進行報告。
5. 網路安全政策：
   - 本公司遵循 ISO 21434 等國際網路安全標準或與客戶約定的網路安全管理流程來維護管理系統。
   - 應識別與管理具有價值且與網路安全活動相關的資產，並由客戶與本公司協議適當的處理方式。
   - 本公司將以開發安全的產品作為核心價值，並確保採取必要的活動。

- 本公司將定期對流程進行網路安全稽核，以確保流程和開發活動符合 4.2.1 條的要求。
- 本公司將確保員工具備良好的網路安全技能或安排適當的培訓。

**責任:**

1. 建立及審查此政策。
2. 資訊工作小組透過標準和程序以實施此政策。
3. 所有人員和委外服務供應商均須依照相關安全管理程序以維護資訊安全政策。
4. 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
5. 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行懲處。

**審查:**

1. 本政策應至少每年於管理審查會議審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本公司永續運作及資訊安全實務作業能力。

**實施:**

1. (含子公司)因業務需求取得本公司機敏性資訊或個人資料時，應負起資料保密責任及妥善運用，並遵守國家相關之法令及本公司之相關資訊安全規定。
2. 若因疏失造成資料外洩或資安事件，應負相關法律責任。
3. 本政策經「資訊安全委員會」進行會審後，由召集人核定後實施，修訂時亦同。

## 三、 資訊安全具體管理方案

1. 經由ISO27001資訊安全管理制度的實施，可以有效減少資安事件的發生，對風險管理具有一定的成效，綜合評估成本與效益後，目前暫無承保資安險的急迫性與必要性。
2. 已實施的ISO27001:2013標準14個領域及相關控措施。
   - 資訊安全政策
   - 資訊安全組織
   - 人力資源安全
   - 資產管理
   - 存取控制
   - 密碼學
   - 實體及環境安全
   - 運作安全
   - 通訊安全
   - 系統獲取開發及維護
   - 供應者關係
   - 資訊安全事故管理
   - 營運持續管理之資訊安全層面
   - 遵循性
3. 目前常見的網路惡意攻擊、勒索軟體等資安風險議題，已有投入網路資安設備的建置進行防護，如防火牆的入侵預防系統(IPS)設置，網路行為分析。
4. 每年都會針對核心系統，如網域控制站、電子郵件、ERP系統、資料庫、文件主機等...進行弱點掃掃描，弱點修補、備份還原演練、資安事件演練、營運持續演練，有效的預防資安風險的發生，如果風險發生時可以有效的控制災害並減少損失。