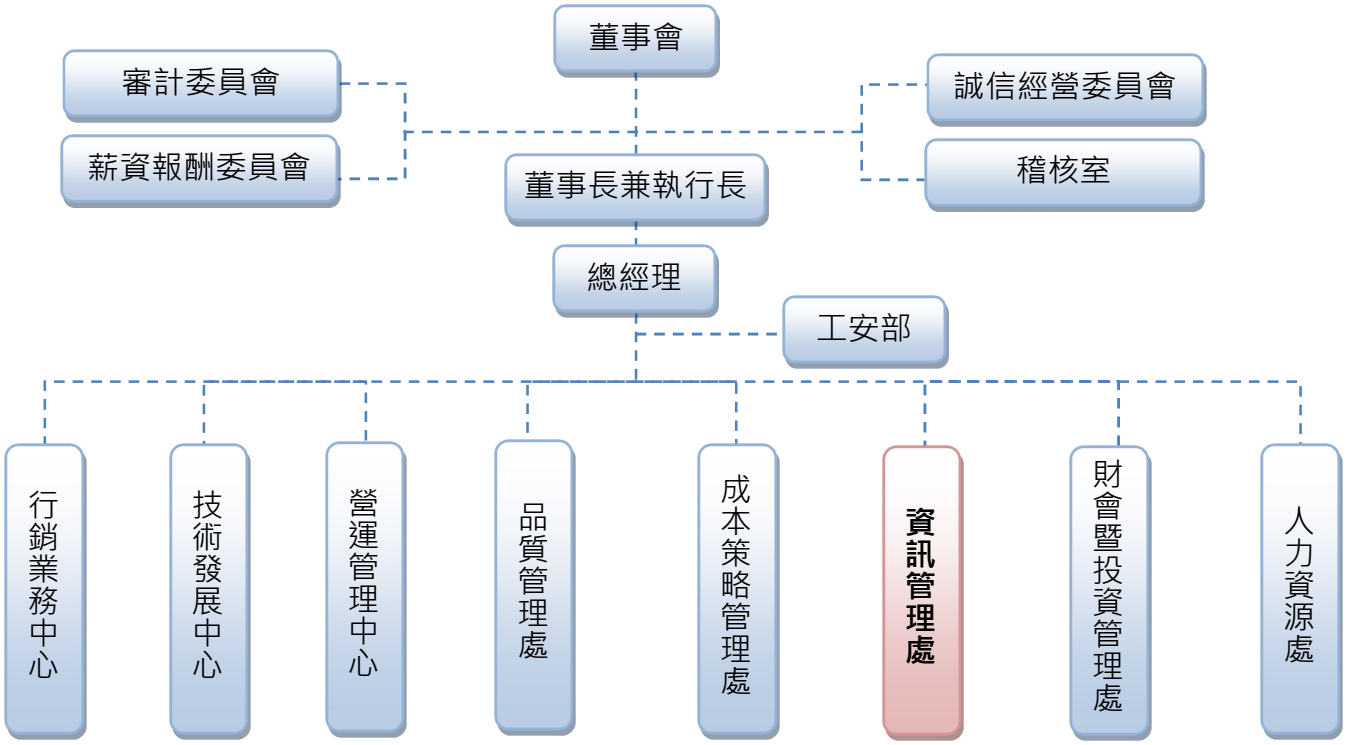
AOT
Solid-State Light. Done Right.

➢ **資訊安全風險管理架構：**

本公司設置隸屬於總經理下之「資訊管理處」，其工作職掌主要為負責資訊安全及風險管理；配合公司之經營策略與模式，設計資訊管理系統，提供即時決策支援系統與管理資訊。



➢ **本公司資訊安全政策：**

本公司致力保護公司機密資訊，重視機敏資訊安全是本公司對客戶、員工及全體股東的承諾，深知資訊安全將攸關公司現在與未來的競爭優勢，為妥善管控公司資訊安全，本公司持續不斷強化機密資訊保護的能力，並提升員工對機密資訊安全保護的正確觀念及警覺性，降低機密資訊外洩的風險以確保公司、股東、員工、客戶及供應商的最佳利益。

➢ **具體管理作法：**

預防駭客/網路攻擊	本公司已制訂資訊安全管理政策及建立基礎的網路及電腦安全防護系統以控管或維持公司的製造營運等重要企業運作的功能，資訊架構依其風險等級，建置適當的次世代防火牆保護，也建置高可用度主機備援系統、實施完整資料備份及異地存放媒體作業並舉行重大系統備援演練，確保資訊系統之正常運作及資料保全，以降低無預警天災及人為疏失造成之系統中斷風險。
教育、宣傳	透過「開機宣導平台」、教育員工了解資訊安全觀念。以「ASRC 郵件指紋採集機制」，阻絕外部惡意攻擊郵件，降低遭受釣魚郵件威脅風險。
正版/合法軟體	使用正版/合法軟體的政策及做法：只有 IT 人員可安裝軟體，並透過資產掃描工具掌控軟體數量，避免任意安裝來路不明軟體，導致機敏資訊洩露資安事件。
文件加密保護	使用文件保全加密技術，保護公司內部重要機敏資料，避免未經授權機敏文件外流事件發生。