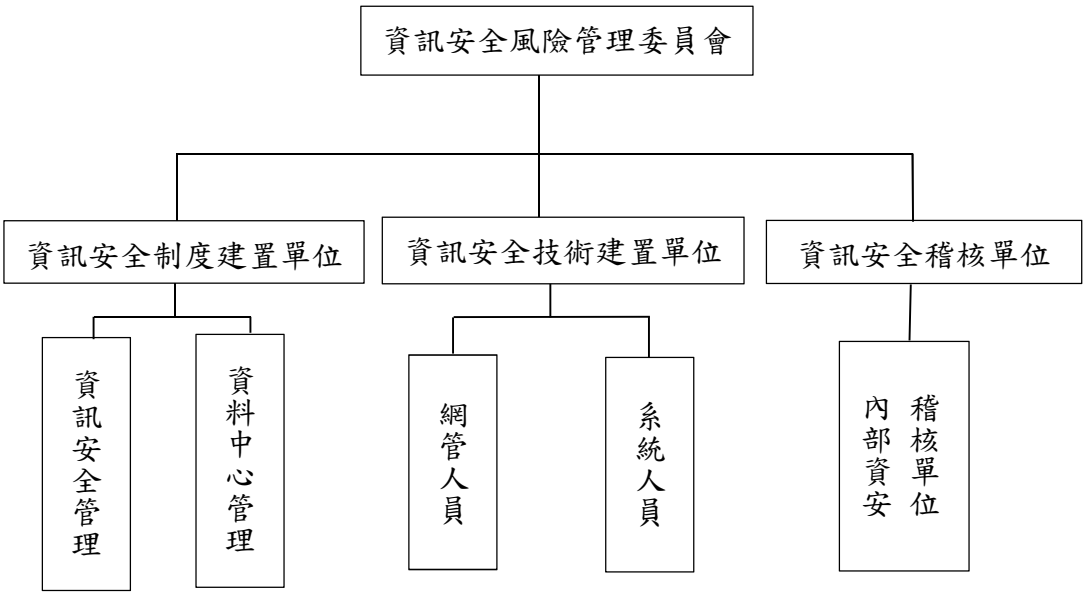
資訊安全風險管理架構



為提升資訊安全管理，本公司針對資安風險建立一套資訊安全系統以進行管理，並成立風險管理的組織架構，負責審視公司資安治理政策，監督資安管理運作情形，由資訊中心擔任召集人，定期向董事會報告資安治理概況。組織團隊包含資訊安全制度建置單位-負責制定與維護各項資訊安全管理制度、資訊安全技術建置單位-執行資訊安全系統管理與系統管理的建置、資訊安全稽核單位-配合公司稽核進行資訊安全稽核工作。

資訊安全風險管理方案

參照資安管理系統認證之要求標準進行制定，並針對各項資訊系統服務建立風險管理系統，資安與網路風險以風險評估流程進行評估，針對風險影響等級與發生機率，進行風險管控，並對評估後之高風險系統進行對應的管理機制，建立高可用性之高可靠度架構、資料備份、異地主機備援機房設置等，以確保服務不中斷，並建立專線，將備份資料送往異地保管存放，每半年進行系統切換演練，以確保備援機制之正常運作，並能符合系統復原目標。公司亦投保資安保險，針對各種資安風險提供保障，對於各種重大資安事件之影響與對應處置措施均已訂定相關規定，每年執行資通安全性檢測及資安事件演練，強化公司同仁資安危機意識及資安處理人員應變能力，以期能事先防及第一時間有效偵測並阻絕擴散。稽核單位每年定期對資通安全各項目進行查核，將其年度稽核計畫之稽核項目，並覆核其執行績效簽署意見呈報公司例行會議並建立追蹤改善機制，以持續追蹤改善情形。

資訊安全政策

廣明光電資訊安全政策訂有下列目標：

1. 恪遵法令訂定相關資訊安全管理規章，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畫，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，提昇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供應商，應確實遵守本公司資訊安全相關規定，如有違反者，視其情形分別依本公司規定懲處或依契約罰責辦理外，情節嚴重另將受相關法律之訴追。
5. 不定期辦理資訊安全趨勢分析與宣傳講座，建立同仁對資訊安全的觀念。

本公司針對公司機密資訊(或重要資訊)之定義與品質要求、資訊化程度、使用的資訊系統可靠性、資訊作業委外程度議題進行討論，評估本公司現行環境所需之資訊安全檢查之範圍、頻率與項目作為資訊安全檢查控制選擇的指引。資訊安全檢查工作執行結果，由稽核單位覆核其執行績效並簽署意見呈報公司例行會議並建立追蹤改善機制，以持續追蹤改善情形。本公司於 111.08.08 及 111.11.02 安排兩場資訊安全趨勢分析與宣導講座，要求全體同仁參與，以建立同仁的資訊安全觀念，期能降低資訊安全事件之發生與其造成之公司損害。

董事會報告資安治理概況

評估項目	說明	執行情形
電腦系統安全管理	◉電腦作業系統環境設定及使用權限設定需經有關主管核示，並由系統管理人員執行。 ◉電腦系統檔案異動前後皆有前一營業日之備份處理措施。 ◉程式的存取使用，有詳細的書面管制說明。 ◉使用者依照程序申請使用權限，並由主管核可。 ◉密碼以亂碼或隱藏方式儲存。	均有效執行

評估項目	說明	執行情形
電腦系統安全管理	◉人員異動時及時更新其使用權限。 ◉人員異動時及時更新其使用權限。 ◉對於程式及檔案之存取使用，按權限區分。 ◉使用者忘記密碼之處理，有嚴格的身分確認程序。	
網路安全管理	◉定期評估自身網路系統安全。 ◉定期或適時修補網路運作環境之安全漏洞。 ◉電腦網路安全之事項隨時公告通知。 ◉各電腦主機、重要軟硬體設備有專人負責。 ◉防火牆安全管理。 ◉網路使用者帳號管理。 ◉電腦病毒及惡意軟體之防範。	均有效執行
系統發展及維護安全管理	◉資訊業務委外開發時，事前審慎評估可能發生之潛在安全風險，並於廠商簽訂適當的資訊安全協定，將相關的安全管理責任納入契約條款，保障資料及系統之安全。 ◉資料進入正式環境之資料庫前進行合理之查驗，以確保資料的正確性。 ◉應用軟體建立控制程序並嚴格執行，為減少可能危害作業系統的風險。 ◉建立應用系統正式之變更控制程序，並嚴格執行，以降低應用系統之安控風險。	均有效執行
資訊資產安全管理	◉資訊公共槽設定使用者群組並依群組分類設定存取權限。 ◉資訊設備實體報廢前由資訊部門將硬碟資料銷毀以防止公司及個人資料外洩。	均有效執行
實體及環境安全管理	◉資訊相關設備安置在適當的機房並予以保護。	均有效執行

評估項目	說明	執行情形
實體及環境安全管理	◉電腦設備有獨立之電源供應系統含不斷電系統，以保護重要之應用系統。 ◉電腦機房隨時上鎖並備置有效之滅火器。 ◉備份資料應異地儲存。 ◉機房設有嚴格之進出管制保護措施，並記錄來訪人員進出時間和目的，以確保僅被授權之人員始得進入。	
資訊安全趨勢分析與宣導講座	◉建立同仁的資訊安全觀念，降低資訊安全事件之發生與其造成之公司損害。	均有效執行