

資通安全政策

資通安全管理之目的：

確保本公司營運所需之資訊與資訊資產的機密性、完整性及可用性，在符合安全、合理、有制度之原則下，以資訊安全為基礎，提供本公司之資訊業務持續運作之資訊環境，建立營運創新、強化服務安全、提高團隊能力，達成永續經營，並符合相關法規之要求。

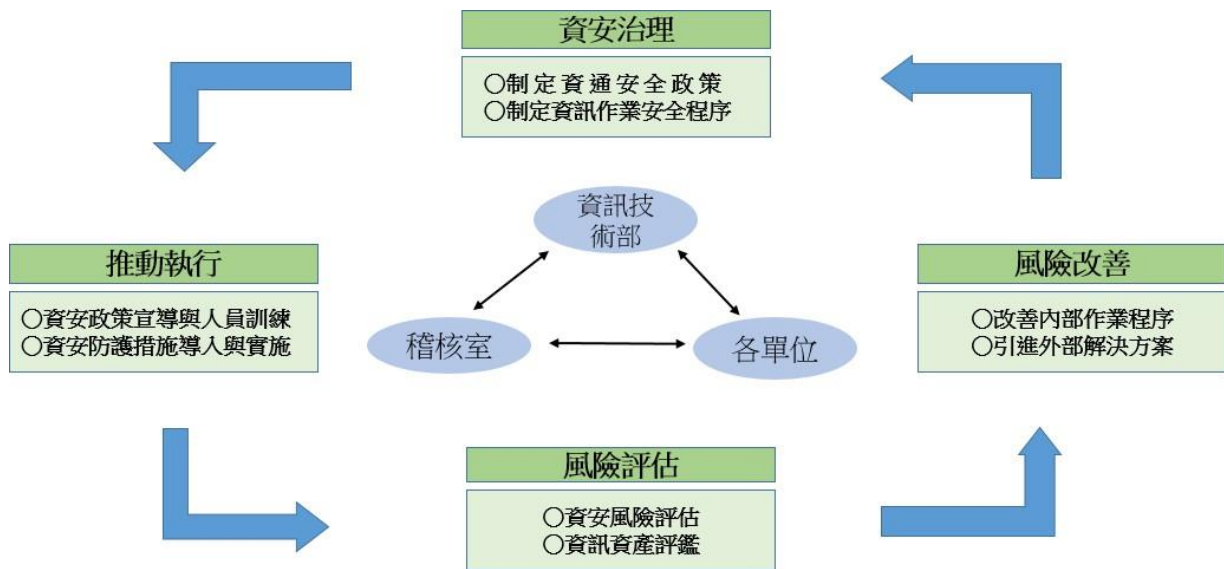
資通安全政策內容：

本公司資訊安全管理涵蓋事項如下：

- (1) 資訊安全組織
- (2) 資產分類與控管
- (3) 人員安全與管理
- (4) 實體與環境安全管理
- (5) 通訊與操作管理
- (6) 存取控制
- (7) 系統開發與維護
- (8) 永續經營管理
- (9) 內部稽查
- (10) 新增及修訂

資通安全風險管理架構：

1. 本公司資訊技術部隸屬營運副總經理指揮，該部設置資訊主管1人，與專業資訊人員1人，負責訂定企業內部資訊安全政策、規劃暨執行資訊安全防護與資安政策推動與落實，並定期公佈公司資安治理概況。
2. 本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。
3. 組織運作模式採定期稽核與循環式管理，確保可靠度目標之達成且持續改善。



資通安全政策具體管理方案：

制度規範：本公司內部訂定多項資安規範與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。

系統防護：本公司為防範各種內/外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部同仁之作業行為符合公司制度規範，亦設計作業程序稽核機制和導入資安管理工具，落實人員資訊安全管理措施。

人員訓練：本公司定期實施新進人員資訊安全教育訓練實務課程，並不定期實施資訊安全機會宣導，藉以提昇公司同仁資安知識與專業技能。

資通安全具體政策及執行情形：

- 1.政策及目標：由營運副總經理核定，並定期檢視政策及目標且有效傳達員工其重要性。
- 2.作業程序：資訊安全應包含核心業務及其重要性、資通系統盤點及風險評估、資通系統發展及維護安全、資通安全防護及控制措施、資通系統或資通服務委外辦理之管理措施、資通安全事件通報應變及情資評估因應、資通安全之持續精進及績效管理機制等。本公司已建置相關作業程序。
- 3.投入資金：本公司113年度投入資訊安全相關費用約為116.8萬元，導入資訊設備資產管理系統以有效控管內部資訊相關設備相關資訊及資安控管行為。
- 4.資安會議：本公司資訊安全部門由營運副總經理每月召集資訊安全會議，討論資訊安全相關議題及改善方向並定期追蹤，113年度共計召開11次會議。於113年12月23日董事會報告資安防護計劃。

具體管控措施：

類別	說明	相關措施
權限管理	人員帳號，權限管理，系統操作	人員帳號權限管理與審核
		人員帳號權限定期盤點
存取管制	人員存取內外部系統，資料傳輸管道安全措施	內/外部存取管控
		資料外洩管控
		操作行為軌跡紀錄
外部威脅	內部系統潛在弱點，防毒防駭的保護措施	主機電腦弱點檢測與更新措施
		防毒防駭，垃圾與惡意程式偵測
系統可用	系統可用狀態與服務中斷時的處置措施	系統/網路可用狀態監控及通報機制
		服務中斷之應變措施
		資料備份與系統備援機制
		定期災害還原演練

本公司資通安全通報程序如下：

資安事件之通報與處理，皆遵守該程序之規範進行。

