圓剛科技-公司治理 資訊安全政策

● 資訊安全治理責任

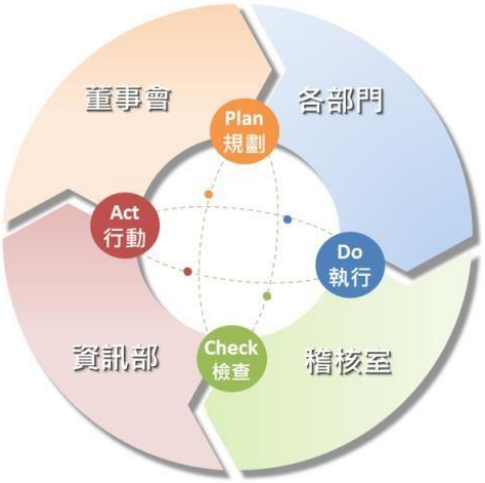
為落實經營者的責任，促進經營績效、保障投資者權益，圓剛科技善盡資訊安全治理之責任，掌控資訊安全與企業風險管理，保護公司之研發成果資料、策略、合約文件、智慧財產、資訊系統等企業重要資產，落實資訊安全策略與內部控制，持續對資訊安全精進治理與強化防護能力，以確保公司永續營運之基礎。

● 資訊安全治理架構

圓剛科技以資訊安全治理架構作為指導及控制組織資訊安全活動之系統，目標在於確保資訊安全目標及策略承接組織營運的目標及策略，使資訊安全策略與業務目標一致，由上而下的持續回饋資訊安全治理架構以降低資安風險。

● 資訊安全治理組織

圓剛科技資訊安全管理執行組織透過規劃、建立、執行與監督(PDCA)機制，保護資訊資產的機密性(Confidentiality)、完整性(Integrity)以及可用性(Availability)，並透過日常維運執行與監督的過程確保其持續改善，並提供組織得以再次評估回饋，落實資訊安全管理執行機制，透過治理架構向上溝通，回應組織策略之要求。



● 資訊安全管理機制

資訊安全管理機制，包含以下四個面向：

（一）內控制度規範：
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。

（二）資安推展執行：
落實執行公司訂定 ISO 程序及各資安規範制度，管理與監控所有營運系統及網路服務安全事件和狀態，評估及導入資訊技術、資安設備運用。

（三）弱點風險評估：
定期審視內部資訊安全，根據資產價值、弱點、威脅與影響性，分析內部風險水平，並以此風險評估結果制定安全措施強化項目，精進且提升整體資訊安全環境。

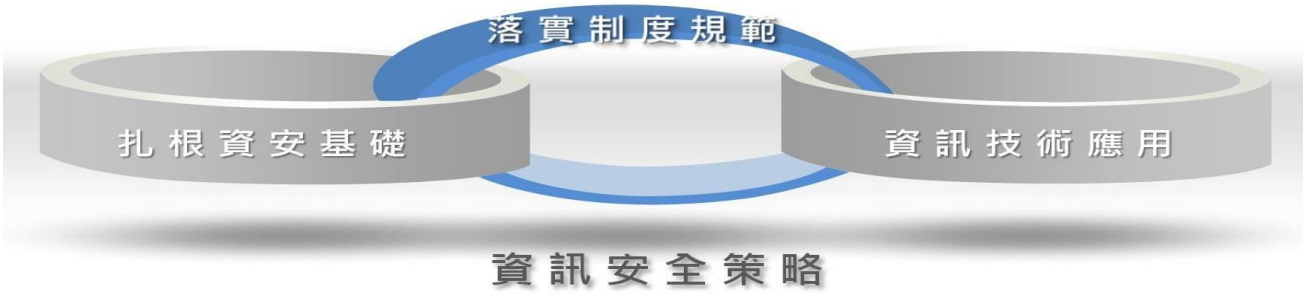
（四）資安應用改善
本公司為防範各種外部資安威脅，採多層式網路架構設計，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦設計作業程序和導入資安系統工具，落實人員資訊安全管理措施。

● 資訊安全策略

資安策略主軸聚焦於扎根資安基礎、落實制度規範及資訊技術應用三個面來進行，從內部資通安全管理辦法、並透過資訊科技主動通報資安風險事件，人員到組織全面提升資安意識。

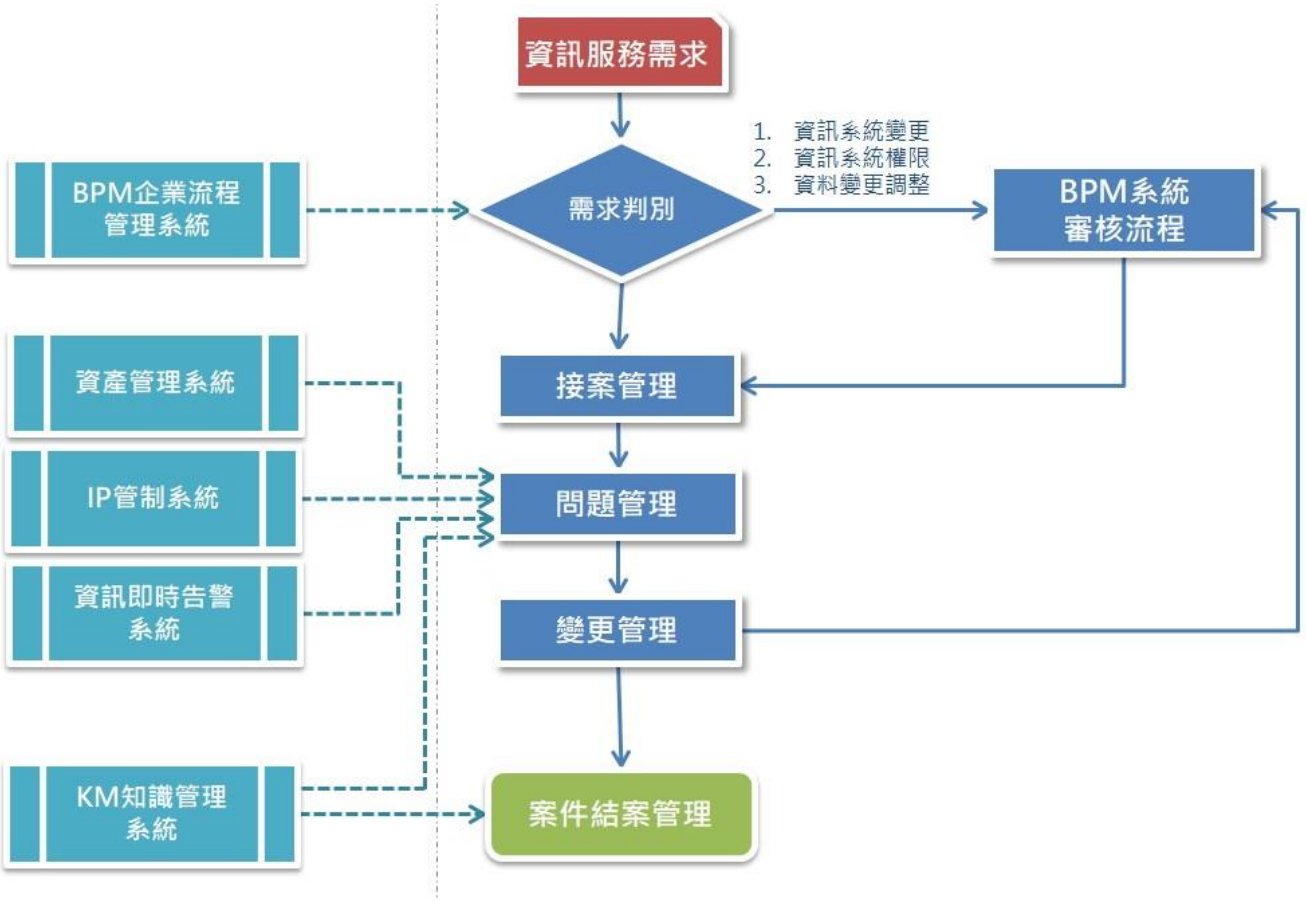
資訊安全策略

扎根資安基礎	定期檢視及升級網路基礎架構環境、持續修補內部系統潛在弱點、定期演練災難還原機制，實施人員資訊安全教育訓練實務課程，全面性的深化資安基礎防禦力。
落實制度規範	訂定公司資訊安全管理制度，定期審視及檢核資安內控執行成效，並貼合國際資訊安全規範，落實資訊安全控管機制之運行。
資訊技術應用	持續導入資訊安全設備及資安技術應用，透過如即時告警系統、端點防護系統、弱點掃瞄、入侵偵測聯防等技術應用，預先掌握資訊風險狀態，提升資安防禦力及應變能力。



- 資安服務處理流程

依據公司訂定之資訊管理辦法及案件管理流程，由資訊服務需求開始至案件結案，針對整體流程中各逐一環節,進行審核、分析、管理、記錄，並應用資訊系統之輔助，以有效控制資訊案件之管理、預先掌控及降低資訊風險發生。



- 資訊安全事件

無。