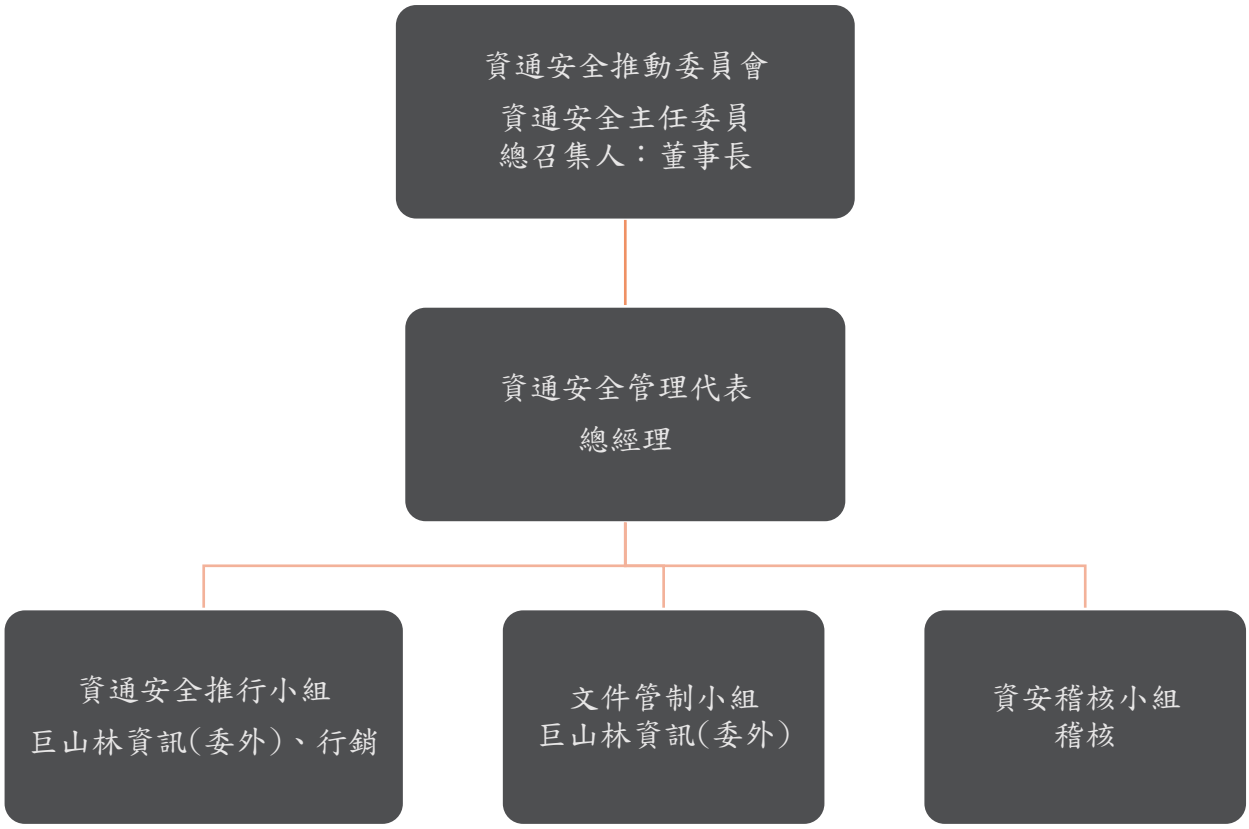
力麒建設股份有限公司

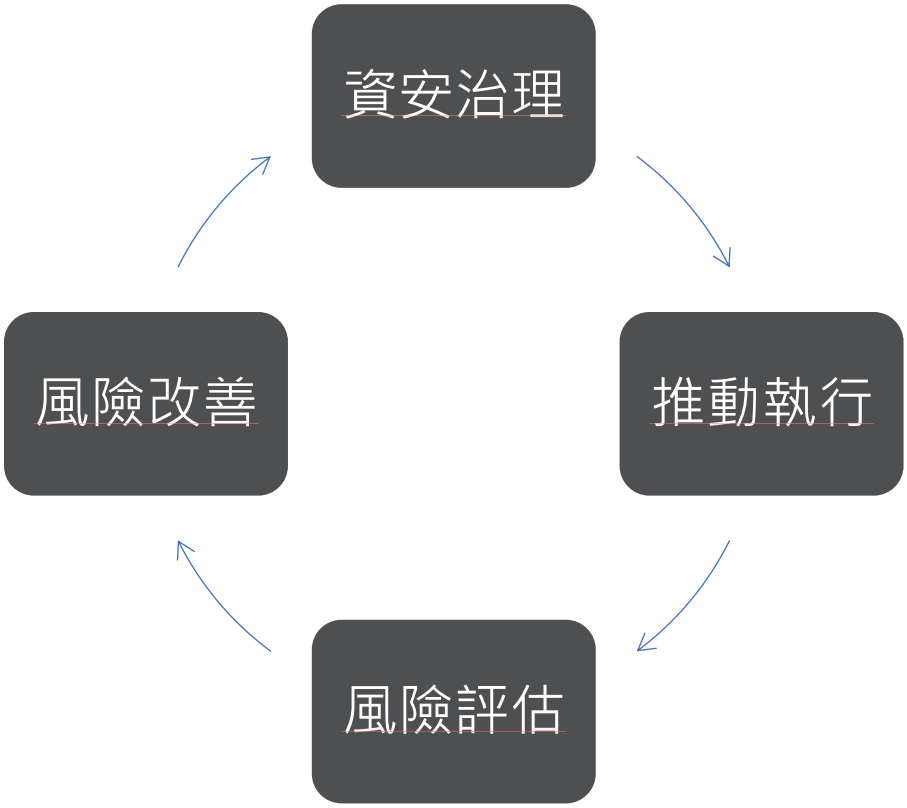
資訊安全政策及管理方案

一、 資訊安全風險管理架構



- 本公司資訊安全之主要執行單位為資通安全推行小組，由資通安全管理代表及營運相關部門主管組成，並得依業務需要由巨山林資訊科技提供技術支援。
- 資通安全推行小組依本公司制定之資訊安全政策與年度管理方案，負責推動及執行各項資安管理措施、事件處理、弱點修補、文件管理等作業，並定期向資通安全推動委員會報告執行成果。
- 本公司稽核室為資訊安全稽核之獨立單位，設置專職稽核人員，負責督導內部資訊安全管理措施之執行情形，並查核各單位之資安作業是否符合公司政策及相關法規要求。

- 若查核發現缺失，稽核室將要求受查單位提出改善計畫並持續追蹤改善成效；查核結果亦將定期呈報資通安全管理代表，以確保資訊安全治理具備透明性與有效性。
- 組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



二、 資訊安全政策

本公司資訊安全管理機制，包含以下四個面向：

（一）制度規範：訂定資安政策、管理制度、作業流程、人員安全規範，以規範人員作業行為，每年檢視制度與實際作業一致性並持續改善。

（二）科技運用：建置防護系統、入侵偵測、弱點掃描、備援機制，落實資安管理措施。

（三）人員宣導：辦理年度教育訓練、社交工程演練、宣導郵件，提昇全體同仁資安意識。

（四）供應商管理：明定廠商之資訊安全責任與保密規定，定期檢視廠商資安控制措施並要求廠商依安全管理程序提供佐證文件。

管理措施說明如下：

- 制度規範：訂定資訊安全管理制度、規範與程序，以規範人員作業行為及管理責任分工。制度每年至少檢視一次，必要時依營運環境、威脅趨勢及集團資安策略予以滾動式修訂。
- 科技運用：本公司為防範各類外部資安威脅，建置必要之資安防護系統並定期進行弱點掃描與網站安全檢測，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，關鍵系統之導入亦陸續導入多因子認證，落實人員資訊安全管理措施。
- 人員宣導：本公司定期實施人員資訊安全教育訓練、社交工程演練、資安宣導郵件與新進人員資安宣導，藉以提昇內部人員資安意識。
- 供應商管理：事前研提資訊安全需求，明定廠商之資訊安全責任及保密規定且列入契約，要求廠商提供年度資安證明（如 ISO 27001 或 CNS 27001）並定期查核廠商資訊安全作業與履約狀況。

三、資訊安全具體管理方案

本公司實施之資訊安全具體管理方案如下：

資訊安全管理措施		
類型	說明	相關作業
權限管理	人員帳號、權限管理、系統操作管理措施	●人員權限管理與審核 ●人員帳號權限定期盤點 ●系統登入採多因子認證
存取控制	人員存取內外部系統、操作行為軌跡管控	●內/外部存取管控措施 ●操作行為軌跡管控措施 ●防火牆及網路流量檢視
外部威脅	內部系統潛在弱點、病毒防護措施	●主機/電腦弱點掃描（每年兩次） ●病毒防護與惡意程式偵測
系統可用性	系統可用狀態、服務中斷處置措施	●系統/網路可用狀態監控及通報機制 ●服務中斷之應變措施 ●資料備份措施、本/異地備份機制 ●定期災害還原演練
資安通報應變	資安通報處理程序	●加入 TWCERT 資安情資分享組織 ●訂定資安事件應變處置及通報程序

四、投入資通安全管理之資源

依據五大類管理安全措施，投入之資源如下：

（一） 網路硬體設備：防火牆、郵件防毒、垃圾郵件過濾、負載平衡器等。

（二） 軟體系統：端點防護系統、備份管理軟體、VPN 及 MFA 認證等。

（三） 投入人力：

每日	系統狀態檢查
每周	備份與異地備份檢查
不定期	執行資安宣導、釣魚演練、資安事件處置
每年	資訊循環之內部稽核、會計師稽核、災難復原演練

（四） 資安通報應變：加入 TWCERT 資安情資分享組織並訂定資安事件應變處置與通報程序。

（五） 資安宣導：2025 年製作二份資安宣導郵件，傳遞資安風險案例與注意事項。

（六） 教育訓練：2025 年實施一次全體員工線上社交工程與個資保護教育訓練，並於正式公告後施行一次社交工程演練。

（七） 社交工程演練：2025 年於教育訓練完成後施行一次社交工程演練。

（八） 弱點掃描：2025 年針對核心系統進行兩次主機及網站弱點掃描並予以修正。

（九） 客戶滿意：無重大資安事件與客戶資料遺失之投訴事件。