榮剛材料科技股份有限公司
資訊安全政策及管理方案

第一條：資訊安全風險管理組織架構(如附件一)

公司資訊安全之權責單位為資訊處，該處設置資訊並兼任資安專責主管乙名，下轄二個軟硬體專業資訊部門人員數名及資安專責人員乙名，以及遵循ISO 27001：2022管理系統設立資訊安全工作小組負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實，並定期向董事會報告公司資安治理概況。

本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管乙名，與專職稽核人員，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。

組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理(如附件二)，確保可靠度目標之達成且持續改善。

第二條：資訊安全政策

「提升資安共識」、「確保營運持續」

為了促使榮剛公司各項資訊安全管理制度能貫徹執行、有效運作、監督管理、持續進行，維護公司重要資訊系統的機密性、完整性與可用性，特頒佈此一資訊安全政策，讓員工於日常工作時有一明確指導原則，保障本公司職員之權益，並期許全體同仁均能了解、實施與維持，達到本公司營運的目標。

提升資安共識

督導並教育全體員工以自律、自主、共榮精神，落實資訊安全工作，建立「資訊安全，人人有責」的觀念，每年持續進行適當的資訊安全教育宣導，以提高資訊安全意識。如有違反資訊安全相關規定，究其權責依人員獎懲相關規定辦理。

確保營運持續

由本公司全體員工貫徹執行資訊安全管理制度，以保護各項資訊資產免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的資安防護措施，將風險降至可接受程度，持續進行監控、審查及稽核資訊安全管理制度的工作，確保各項資訊系統營運持續，達到永續經營的目標。

第三條：資訊安全管理方案

本公司定期審視內部資訊安全規範，並於董事會中報告資安治理概況。本公司亦遵從 ISO 27005 風險評鑑原則，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。關於具體管理措施，詳如附件三。

第四條：資訊風險評估程序

關於資訊風險評估程序，詳如附件四。

第五條：資安事件通報程序

本公司訂立資安通報標準流程如附件五，若發生資安事件將由「資訊安全工作小組」擔任通報窗口，且需於目標處理時間內排除及解決資訊安全事件，並在事件處理完畢後進行檢討與分析並提出改正措施，以預防事件重複發生。

第六條：本公司所訂定之資訊安全政策及管理方案應於公司網站充分揭露，以備查詢。

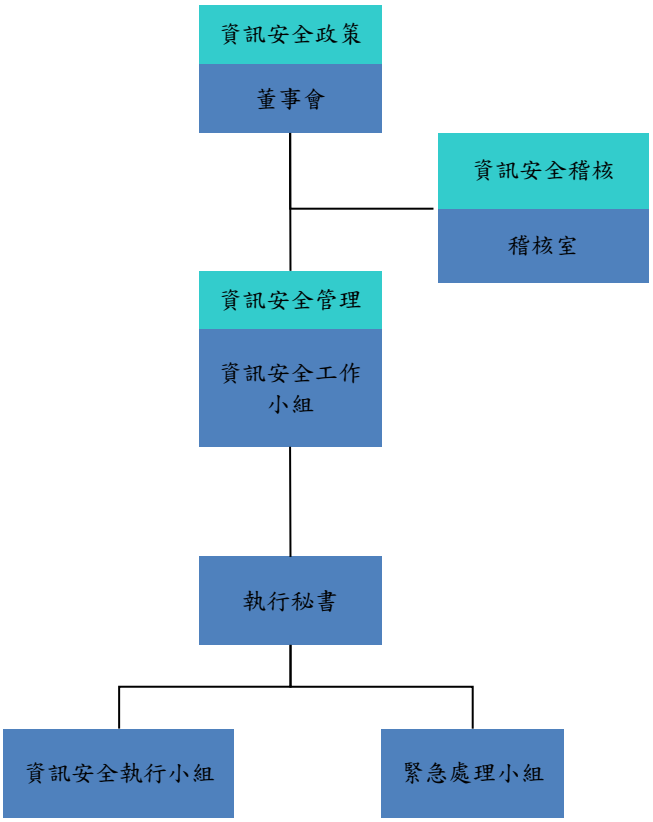
第七條：本政策及方案經董事會討論通過後施行，修正時亦同。

第八條：本政策及方案訂立於中華民國一〇九年十月二十八日。

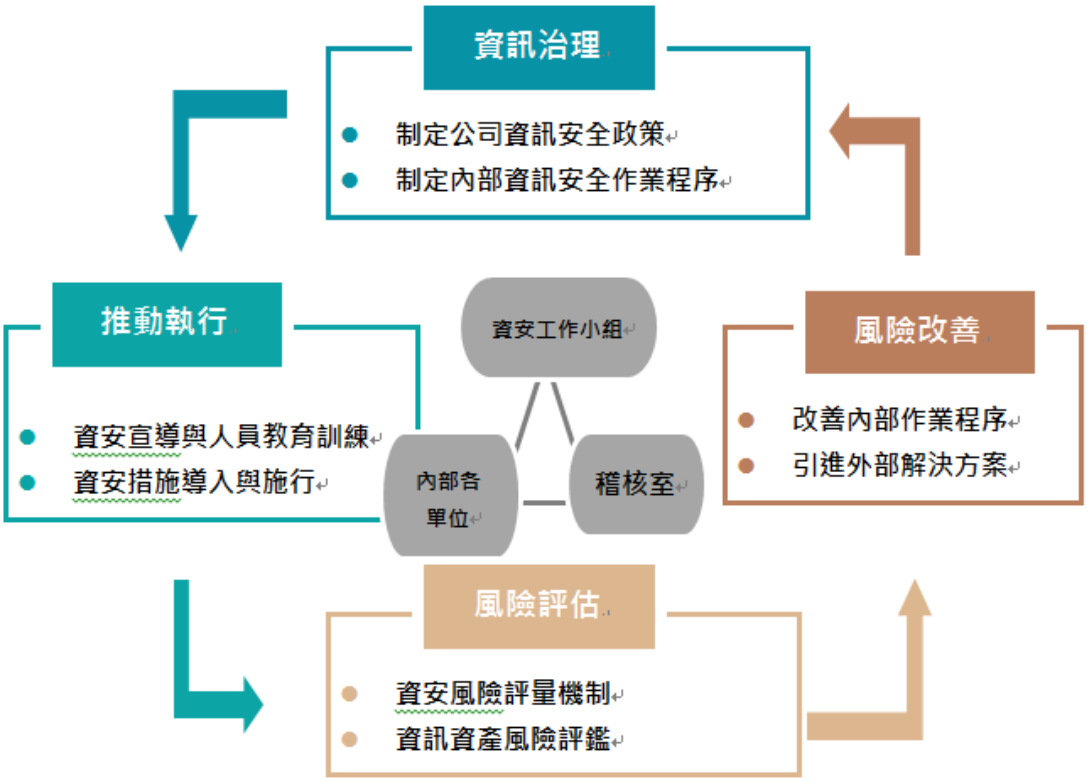
第一次修訂：中華民國一一二年七月二十七日。

第二次修訂：中華民國一一四年一月十三日。

附件一


資訊安全政策
董事會
資訊安全稽核
稽核室
資訊安全管理
資訊安全工作小組
執行秘書
資訊安全執行小組
緊急處理小組

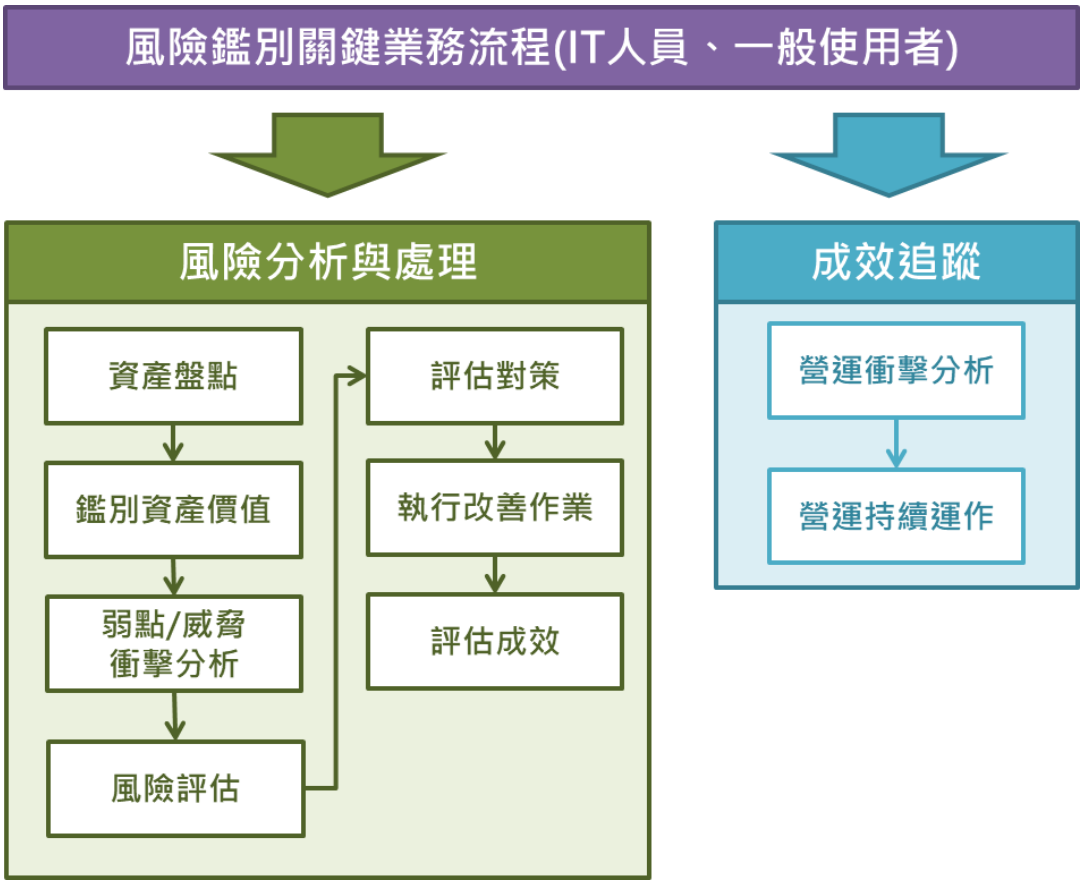
附件二


資訊治理
制定公司資訊安全政策
制定內部資訊安全作業程序
推動執行
資安宣導與人員教育訓練
資安措施導入與施行
資安工作小組
內部各單位
稽核室
風險改善
改善內部作業程序
引進外部解決方案
風險評估
資安風險評量機制
資訊資產風險評鑑

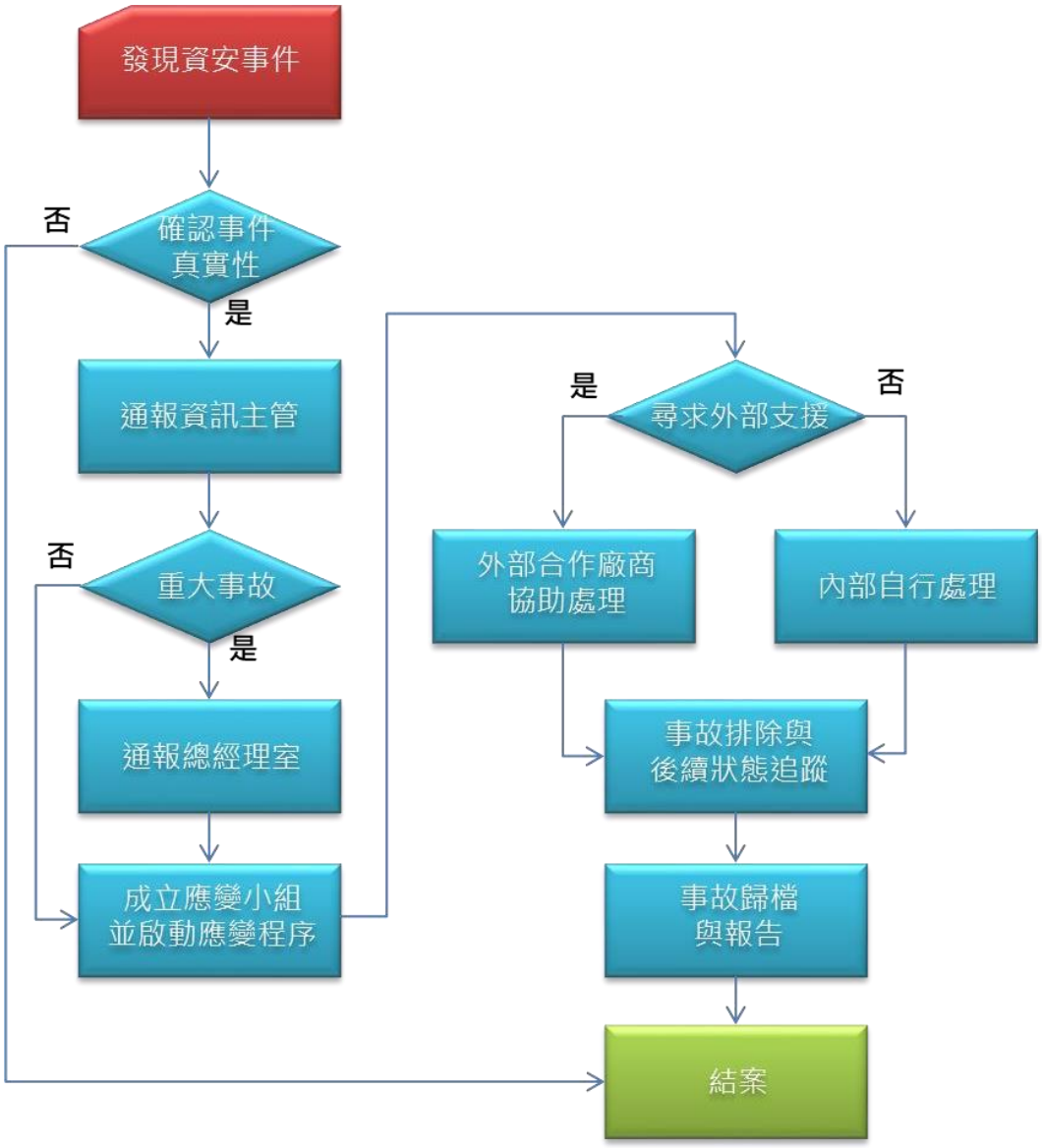
附件三

資訊安全管理措施		
類型	說明	相關作業
權限管理	人員帳號、權限管理與系統操作行為之管理措施	• 人員帳號權限管理與審核 • 人員帳號權限定期盤點
存取管控	人員存取外部系統及資料傳輸管道之控制措施	• 內/外部存取管控措施 • 資料外洩管道之控制措施
外部威脅	內部系統潛在弱點、中毒管道與防護措施	• 主機/電腦弱點檢測及更新措施 • 病毒防護與惡意程式偵測
系統可用性	系統可用狀態與服務中斷時之處置措施	• 系統/網路可用狀態監控及通報機制 • 服務中斷之應變措施 • 資料備份備援、本/異地備援機制 • 定期災害還原演練

附件四


風險鑑別關鍵業務流程(IT人員、一般使用者)
風險分析與處理
資產盤點
鑑別資產價值
弱點/威脅
衝擊分析
風險評估
評估對策
執行改善作業
評估成效
成效追蹤
營運衝擊分析
營運持續運作

附件五


發現資安事件
確認事件真實性
否
是
通報資訊主管
重大事故
否
是
通報總經理室
成立應變小組並啟動應變程序
是
尋求外部支援
否
外部合作廠商協助處理
內部自行處理
事故排除與後續狀態追蹤
事故歸檔與報告
結案