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，該處設置資訊主管乙名，下轄二個軟硬體專業資訊部門人員數名，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

本公司資訊安全政策，包含以下三個面向：

（一） 制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

（二） 科技運用：建置資訊安全管理設備，落實資安管理措施。

（三） 人員訓練：進行資訊安全教育訓練，提昇全體同仁資安意識。

說明如下：

制度規範：本公司以 ISO 27001 為參考標準，並依據公司內部實際管理需求制定資訊安全政策。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。

科技運用：本公司為防範各種外部資安威脅，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。

人員訓練：本公司不定期實施人員資訊安全教育訓練實務課程、發佈資訊安全風險及人員應對措施案例，並建置數堂線上學習（E-Learining）資訊安全課程，藉以提昇內部人員資安知識與專業技能。

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

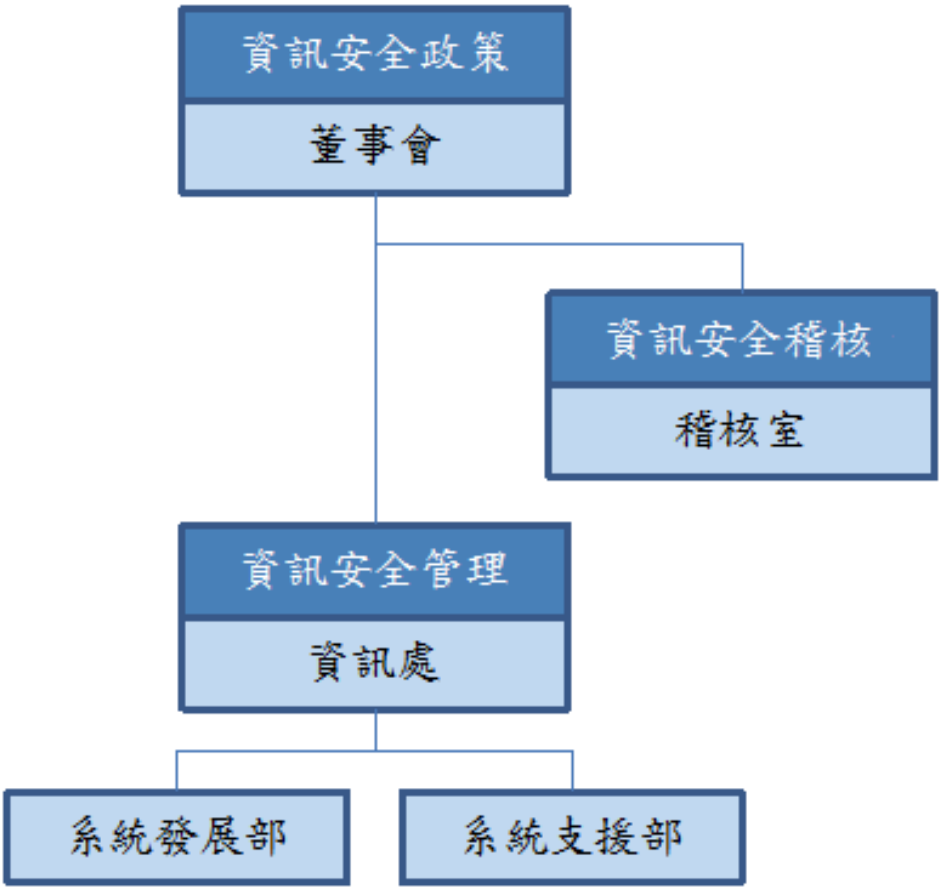
本公司資通安全通報程序如附件五，資安事故之通報與處理，皆遵守該程序之規範進行。

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。

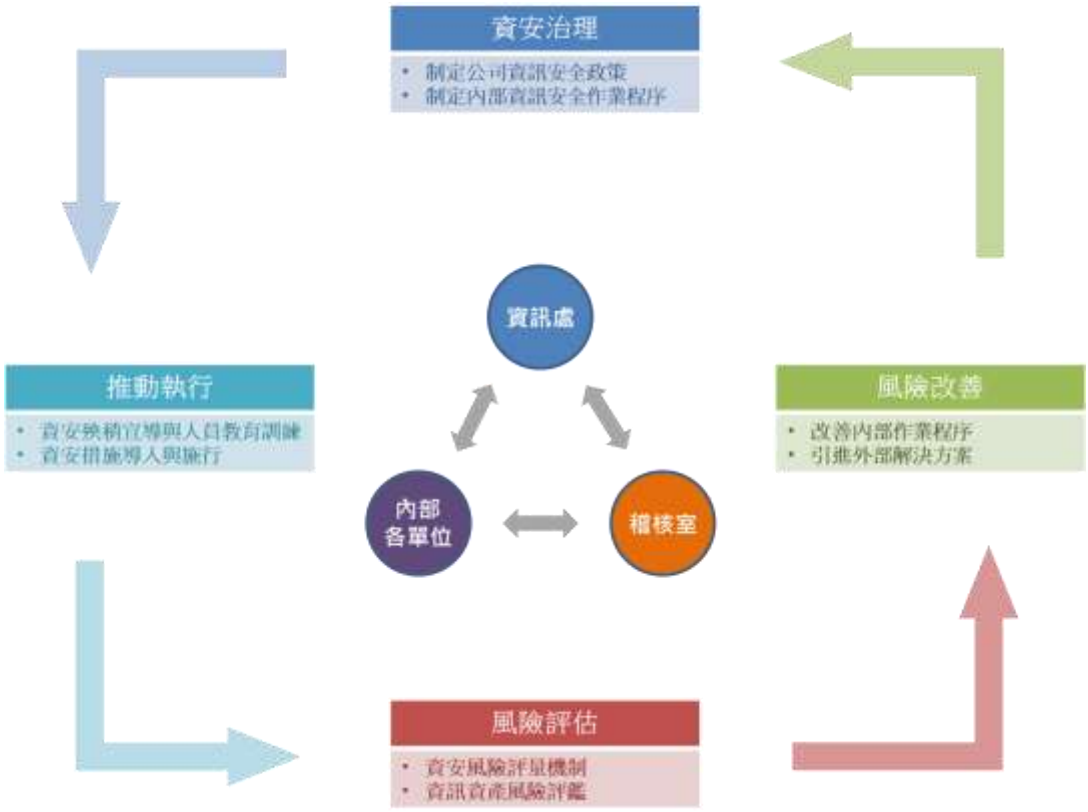
第七條：本政策及方案經董事會討論通過後施行，修正時亦同。

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。

附件一



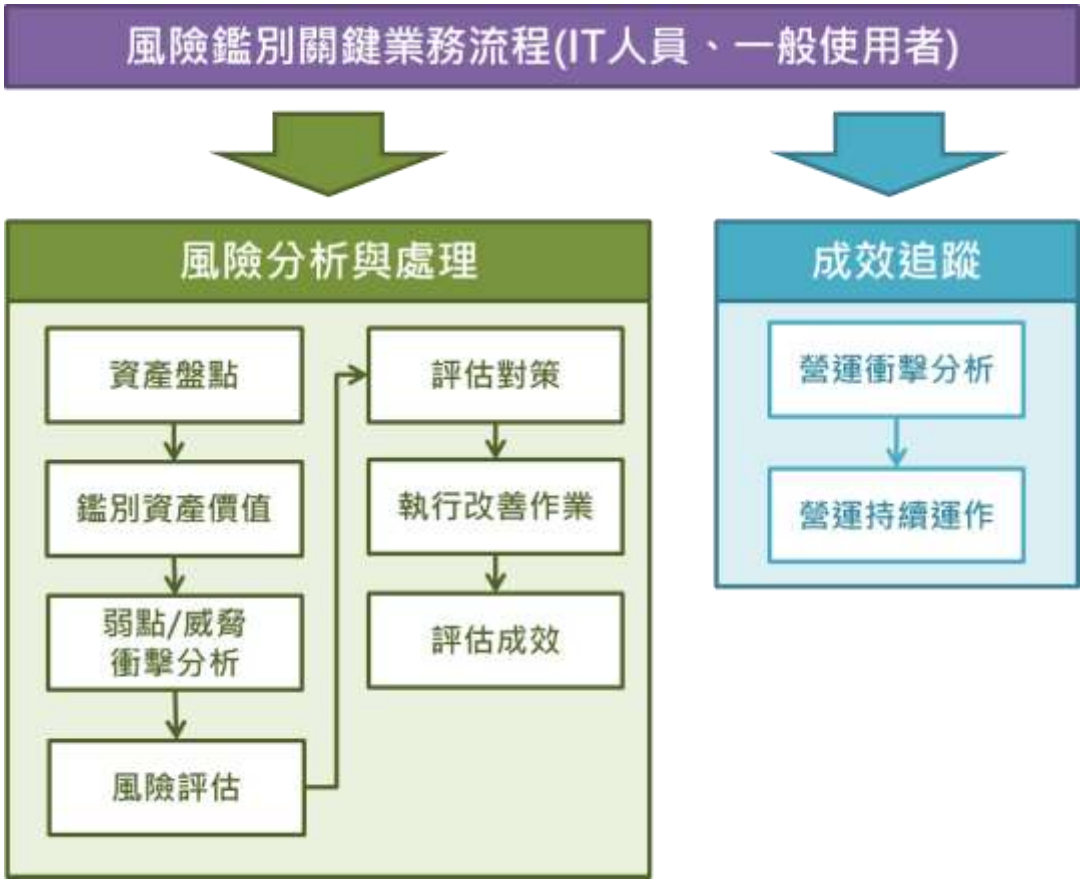
附件二


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

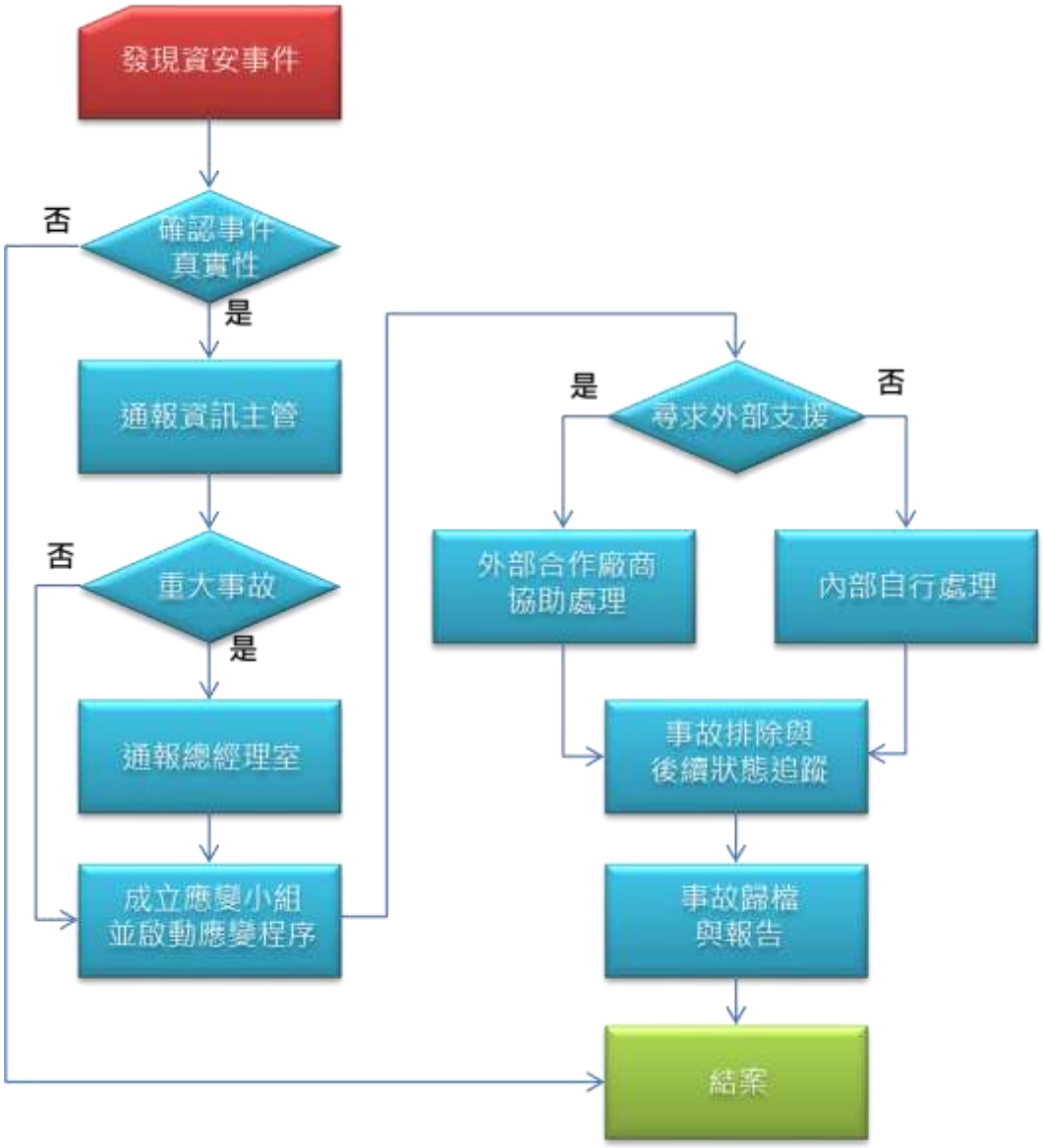
附件三

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