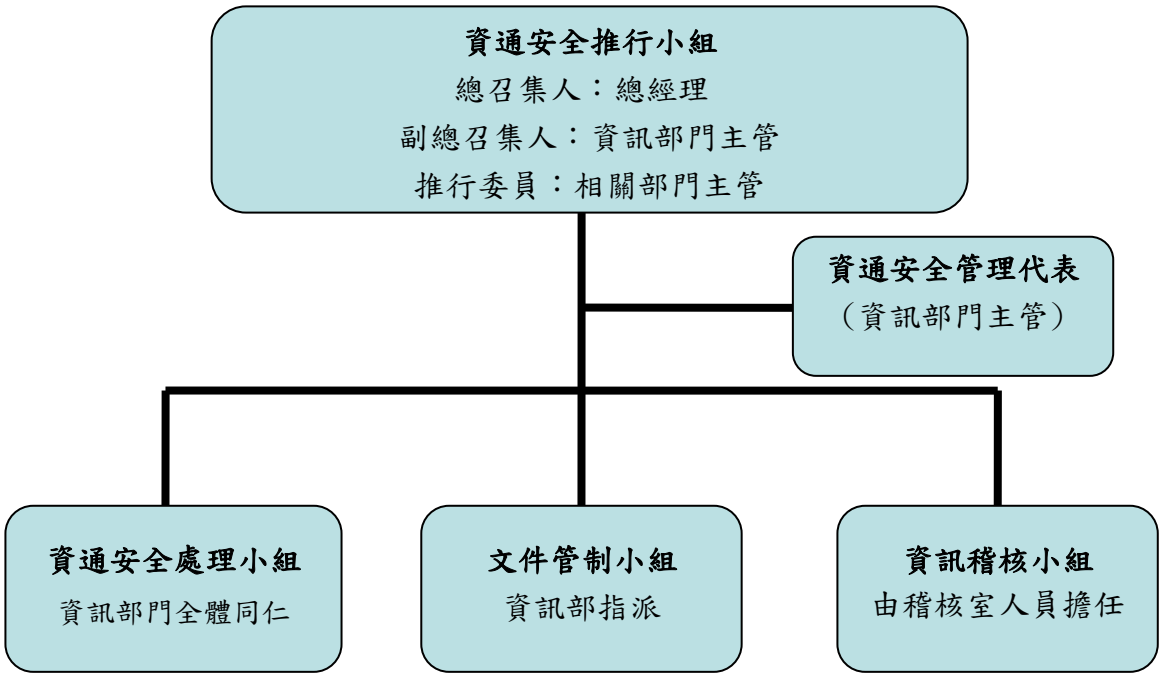
資訊安全政策

本公司為確保資訊資料、系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或毀損等風險，訂定「資訊安全政策」、「資訊安全組織程序書」、「資訊安全實施程序書」、「營運持續管理程序書」等，建立資訊安全管理系統，於 107 年 4 月成立資訊安全專責單位，落實資訊安全管理與政策。

資訊安全組織



資通安全職責

一、審核資訊安全管理系統目標及實施範圍。

二、審核資訊安全管理相關作業執行情形及改善的有效性。

三、檢討資訊安全相關政策及規定，協調資源之分配及使用。

四、監督營運持續演練之辦理。

五、審核實施矯正預防措施所需之資源，包括人力、時間及經費。

六、審核矯正預防措施之有效性。

七、每年至少召開管理審查會議 1 次，必要時得召開臨時會議。

作業機制

一、為落實資訊安全管理系統之推動，資通安全處理小組人員應進行資訊安全管理相關程序之宣導與

配合事項。

二、為解決資訊安全各種問題，必要時應詢問資訊安全顧問，使資訊安全管理得到最高效率和最好效果。

三、於資通安全事件發生時，為能迅速採取行動，資通安全處理小組應與執法機關、主管機關、資訊服務供應商、通訊廠商和資訊安全顧問取得適當聯絡，以保障本公司權益。

四、為確保本公司之矯正措施有效運作，應確實落實管理審查機制，至少每年舉行一次管理審查會議，並確實討論下列議題：

（一）過往管理審查之議案的處理狀態。

（二）與資訊安全管理系統有關之內部及外部議題的變更。

（三）資訊安全績效之回饋，包括下列之趨勢。

1. 不符合項目及矯正措施。

2. 監督及量測結果。

3. 稽核結果。

4. 資訊安全目標之達成。

（四）關注方之回饋。

（五）風險評鑑結果及風險處理計畫之狀態。

（六）持續改善之機會。

五、管理審查結果應作為紀錄，依內部文件與紀錄管制行政程序陳報與列管。紀錄內容應至少下列項目：

（一）持續改善機會有關之決策。

（二）資訊安全管理系統變更之需要。

資訊安全管理系統架構

本公司實施 ISO 27001 資訊安全管理系統主要分四大階段，並配合持續進行之管制考核，其執行單位說明如下：

階段	作業步驟	執行單位
P	資訊安全政策	資通安全推行小組
	資訊安全組織	資通安全推行小組
	文件管制	資通安全處理小組
	全景風險評鑑	本公司資訊部全體同仁
	訂定資訊安全管理系統目標及有效性量測	驗證實施範圍單位
	風險評鑑	驗證實施範圍單位
	業務持續管理	驗證實施範圍單位
	訂定與審視資訊安全管理系統範圍與適用性聲明	資通安全推行小組
D	執行資訊安全	資通安全推行小組、資通安全處理小組
	人力資源安全	資通安全處理小組、人資部

階段	作業步驟	執行單位
	資產管理	資通安全處理小組
	存取控制	資通安全處理小組
	密碼	資通安全處理小組
	實體與環境安全	資通安全處理小組
	運作管理	資通安全處理小組
	通訊管理	資通安全處理小組
	系統獲取、開發及維護	資通安全處理小組
	供應者關係	資通安全處理小組
	資訊安全事故管理	資通安全處理小組
	營運持續管理之資訊安全層面	資通安全處理小組
	遵循性	資通安全處理小組
C	內部稽核	資通安全推行小組、資訊稽核小組
A	矯正與改善	資通安全推行小組、資通安全處理小組

資訊安全機制

本公司資訊安全管理除遵守台灣證券交易所規範之「建立證券商資通安全檢查機制」外，已自中華民國100年7月起導入ISO 27001資訊安全管理系統驗證，據以執行資訊安全工作計畫。

自導入以來，已完成以下資安改善作業：

系統方面，逐年增加各項資訊安全防護機制、每年針對核心關鍵系統辦理定期演練、建立測試環境專用防火牆、異地交易系統備份、電子文件平台權限管理。

軟、硬體方面，辦理定期檢視並淘汰老舊硬體設備，以及過時之作業系統軟體，以降低各項服務與系統性之風險。

稽核人員每年定期或不定期辦理資訊安全作業查核與資訊安全政策檢討。

各項查核作業如下：

項次	內容
1	公司運用科技，建置控制作業以支持目標之達成
2	公司蒐集、產生及使用來自內部與外部之攸關與具品質之資訊，以支持內部控制制度之持續運作。
3	定期對全公司之資訊資產及各項作業辦理資訊安全風險評鑑，並留存紀錄
4	資訊安全政策應定期評估並留存相關紀錄
5	指定專人或專責單位負責規劃與執行資訊安全工作
6	定期對全公司員工辦理資訊安全宣導講習，並留存紀錄
7	實體及環境安全

8	通訊與作業管理-網路安全管理
9	通訊與作業管理-電腦系統及作業安全管理
10	權限存取控制
11	系統開發及程式修改之控制
12	營運持續管理
13	法令法規遵循性
14	新興科技應用
15	個人資料保護作業
16	主管機關、周邊單位及會計師查核改善要求
17	內部稽核查核改善

資訊安全檢測

為提升資訊安全管理，本公司於 107 年 4 月成立資訊安全專責單位，監督與協助各分、子公司推動資訊安全管理。

每季定期宣導電腦使用安全與系統更新，降低感染勒索病毒。不定期舉行社交工程演練，提高同仁對於釣魚網站的識別與警覺。

每年度執行各項資安檢測，藉以改善並強化現行資訊系統各項安全防護能力。

每年定期舉行集團人員資通安全講習，提昇員工資訊安全意識，降低駭客滲透之風險。

每年定期進行「分散式阻斷攻擊演練」與「證券期貨市場資通安全通報系統」演練作業，提昇與強化資安事件整體應變能力。

經內部評估 107 年 01 月 01 日至 107 年 12 月 31 日確實符合並遵循主管機關之法令法規要求，且 107 年度本公司未發生對公司重大不利影響之資訊安全事件。