資訊安全風險管理架構

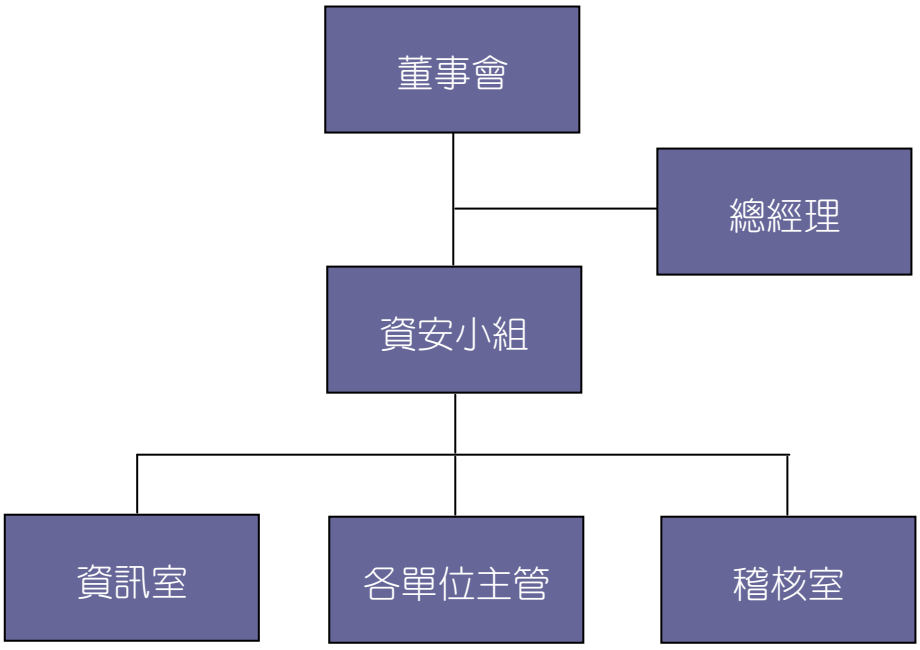
●本公司於 2018 年 10 成立資訊安全小組，由資訊室、稽核室、各作業單位主管組成。

●本公司資訊安全之權責單位為資訊室，負責訂定資安政策、執行及推動資訊安全管理事項，建置安全的資訊環境，並宣導資訊安全意識。

●資訊室主管擔任召集人並配置資訊專業人員 2 名，持續檢視評估資訊環境變化趨勢，不定期回報總經理外，每年至少一次向董事會報告評估資訊安全風險與防護，以確保內部資安管理機制持續有效運作。

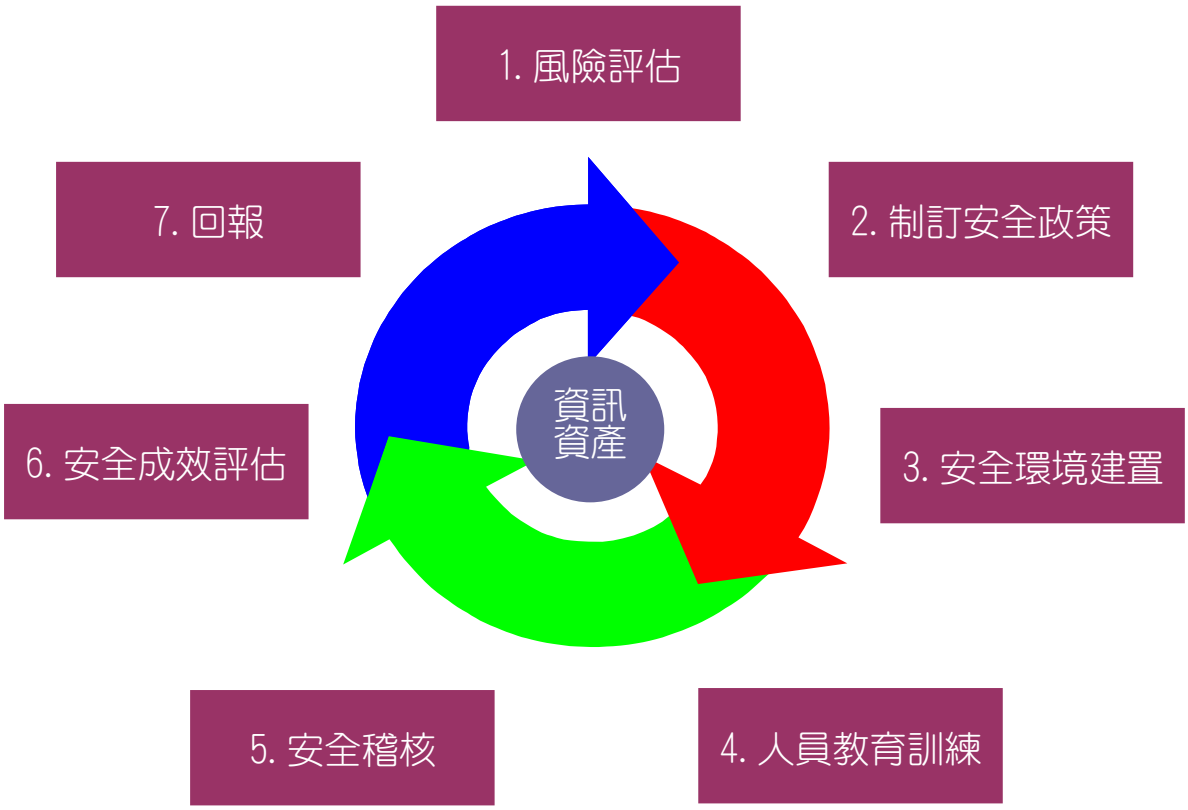
●稽核室為資訊安全監理之督導單位，負責督導內部資訊安全執行狀況，若有查核發現缺失，即要求受查單位提出相關改善計畫與具體措施，且定期持續追蹤改善成效，以降低內部資訊安全風險。

●各單位主管，依循公司資訊安全政策規範，協助各資訊作業人員辨識重要業務存在之風險，一旦發現來自內部或外部的資安威脅時，立即通報聯繫，確保資安工作落實執行。



資安小組運作模式

●小組採循環運作模式，確保執行落實持續改善。



資訊安全管理政策

為確保公司資訊資產(軟體、硬體、電腦資料、資訊環境、人員)之機密性、完整性及可用性，避免遭受來自內、外部的各種威脅損害，使公司資訊系統永續運作，故訂定此資訊安全政策內容如下：

1. 制度規範：遵循法令訂定公司資訊安全管理規章，規範人員作業行為，對資訊資產作適當的保護措施。

2. 風險評估：定期評估各種人為及天然災害對本公司資訊資產之影響，並訂定重要資訊資產及關鍵性業務之防災對策及災害復原計劃，確保本公司業務持續運作。

3. 員工教育：督導本公司員工落實資安全防護工作，建立「資訊安全、人人有責」觀念，提昇全體同仁資訊安全意識。

4. 落實執行：要求內部員工及外部往來之客戶、廠商需使用本公司資訊資產時，應確實遵守本公司資訊安全相關規定，如有違反者，視其情形分別依公司規定或依契約罰則處理，情節嚴重者，則訴諸法律。

資訊安全管理方案

項目	說明	相關措施
資訊架構檢視	檢視對於持續營運所採取相關措施之妥適性及單點故障之最大衝擊與風險承擔能力	●檢視相關措施之架構與維運機制是否存在單點失效之風險，及針對業務持續運作之妥適性進行風險分析，並提出資訊架構安全評估之結果與建議。
權限管理檢視	人員帳號、權限管理與系統操作之管理措施	●人員帳號權限管理與審核。 ●人員帳號定期盤點。
安全設定檢視	伺服器安全原則設定	●檢視伺服器「密碼設定原則」與「帳號鎖定原則」之設定是否符合內控規範。
系統可用性檢測	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。 ●資料備份措施、本/異地備份機制。 ●定期災害復原與演練。
存取管控檢視	人員存取內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。 ●操作行為軌跡記錄。
網路設備、伺服器等設備檢測	弱點掃描與修補作業	●定期或適時辦理網路、伺服器及終端機的弱點掃描，並針對所發現之弱點進行改善、修補作業。
網路活動檢視	檢視設備之存取紀錄及帳號權限	●撿視網路設備、資安設備及伺服器之存取紀錄、帳號權限之授予與監控機制是否符合內控作業規範；以最小權限原則清查該等設備之帳號權限及存取紀錄，識別異常紀錄與確認警示機制。
網站安全檢測	針對網站進行滲透測試	●利用安全檢測工具，針對開放外部連結之網站進行滲透測試，俾利儘早發現網站暴露於外之弱點，並進行修復。
郵件社交工程演練	針對資訊作業人員，於內部安全監控範圍內，寄發演練郵件，測試、宣導及強化資通安全教育	●演練目標主要在於讓同仁瞭解使用電子郵件之風險，提高同仁防範社交工程攻擊之危機意識，持續演練以降低社交攻擊所造成之風險，進而達到保護客戶資料及重要營運資訊與服務之目的。

具體措施

本公司於 2018 年成立資安小組後，由資訊室主管擔任召集人，自 2018 年起每年至少一次向董事會報告公司資訊安全執行情形。

每年一次委由外部會計師事務所風險資詢服務單位，針對本公司重要 ERP 營運資訊系統，作整體使用環境的檢視與查核。

每月執行一次 ERP 重要資訊系統備份還原演練，並由使用單位確認還原資料是否正確無誤。

資訊人員持續監控檢視防火牆過濾設定狀態與網路活動紀錄。

公司對外寬頻網路電信端增加租用 IPS(Intrusion Prevention System) 入侵防護服務，從前端的網路電信機房端阻絕來自駭客的大部份網路攻擊，包括網路型病毒/蠕蟲、特洛伊木馬程式、阻斷式的 DDos、緩衝區溢位等攻擊行為，服務商隨時更新調整攻擊特徵與防護規則，以應付新型態的網路攻擊，減少攻擊封包佔據頻寬，提升網路應用效能，加強防禦效果，該系統可產生統計報表供資訊人員持續檢視外部活動狀態。

負責資訊安全人員，每年接受資訊安全專業課程訓練；2024 年已完成下列資安治理系列課程
02/16：內稽人員對於「資訊安全」之稽核管控實務、07/26：「網站安全與稽核簡介(II) 、07/31 :「ISMS 資訊安全管理系統內部控制與稽核」、12/8 與 12/16 二位資訊室同仁個別通過財團法人台灣金融研訓院舉辦之「資訊安全意識、必備知識與責任 E-Course」、「資安事件說明及預防措施 E-Course」、「上市上櫃公司資通安全管控指弔說明 E-Course」等課程。

本公司於 2022/09/26 訂定「資訊資產清查暨風險評鑑管理辦法」，優先由核心資訊系統開始陸續實施評鑑，2024/08/27 召開年度資安會議後，呈總經理簽核資訊資產評鑑表並於 2024/11/11 向董事會說明年度「資安風險與防護報告」。