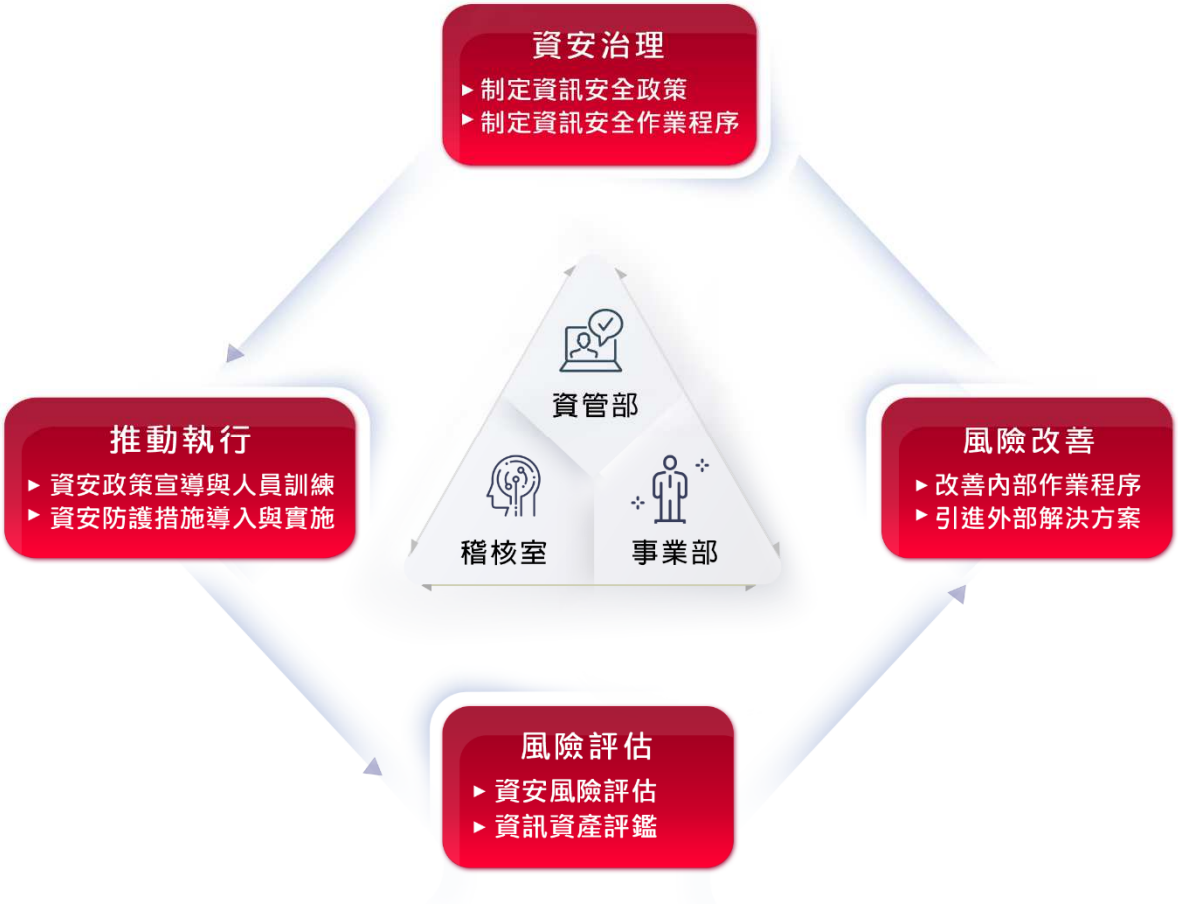
資通安全政策

一、 資訊安全管理架構

(1) 本公司資通安全之權責單位為資管部，該部設置資安主管一名，與專業資安人員一名，負責訂定企業內部資通安全政策、規劃暨執行資通安全防護與資安政策推動與落實，每雙週定期召開資安會議，並公佈公司資安治理概況。

(2) 本公司稽核室為資通安全監理之督導單位，該室設置稽核主管，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。

(3) 組織運作模式採定期稽核與 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

資通安全管理，包含以下面向：

(1) 制度規範：訂定公司資通安全管理制度，規範人員作業行為。

(2) 系統防護：建置資通安全管理系統，落實資安防護管理措施。

(3) 人員訓練：進行資通安全教育訓練，提昇全體同仁資安意識。

(4) 外部查核:對資安與網路風險進行風險評估,適切提出控制點建議,以利控管資安風險。

三、 資通安全具體管理方案

類別	管控措施
強化員工資安意識	■ 新進人員資訊安全教育訓練 ■ 不定期對公司所有同仁進行資安宣導 ■ 每年不定期對公司所有同仁執行社交工程演練
網際網路資安管控	■ 導入次世代防火牆，包含上網行為管理、URL 過濾、入侵防禦系統，避免使用者瀏覽惡意網站及遭受網路攻擊 ■ 每周針對外部站台進行弱點掃描，並評估其弱點修補 ■ 定期對電腦系統資料儲存媒體病毒掃描 ■ 定期覆核各項網路服務項目之 System Log，追蹤異常之情形 ■ 回收個人電腦最高管理權限，依照最小權限原則，劃分給予適當的權限控管 ■ 定期檢討電腦網路安全控制措施
資料存取管控	■ 電腦設備應有專人保管，並設定帳號與密碼 ■ 使用者需定期更新密碼 ■ 電腦機房進出入管制措施 ■ 檔案攜出應經適當之核准 ■ 遠端登入管理資訊系統應經適當之核准 ■ 建立安全檔案交換機制，資料傳輸與資料儲存區加密，降低資料被意外查看風險。完整留存檔案存取稽核軌跡，並定期檢視系統日誌。
應變復原機制	■ 建立系統備份機制，落實異地備份

資安宣導 ×4

每年不定期對公司所有同仁進行資安宣導，傳達資訊保護及資訊安全重要規定及注意事項

資安事件 ×0

2024年未發生重大之資安事件，亦無客戶機密資訊洩漏，以及遭受罰款之情事

災害復原演練 RTO：1.08hour

每年定期執行一次災害復原演練
2024年復原率100%

社交工程演練 ×2

每年不定期執行社交工程演練，模擬駭客釣魚郵件，檢測員工資安風險意識。演練人數超過250人。

新進人員教育訓練 100%

所有新進同仁皆完成資訊安全教育訓練課程

外部網路弱點掃描 ×49

每周定期對外部服務執行弱點掃描

四、 投入資通安全管理之資源

(1) 落實預防演練：每年定期執行本地、異地備援還原演練，針對重要主機系統環境與資料建立自動備份和備援機制，確保人員於災害發生能順利恢復系統運作。

(2) 最小權限原則管理：回收個人電腦最高管理權限，依照最小權限原則，劃分給予適當的權限控管。

(3) 社交工程演練：每年不定期執行社交工程演練，模擬駭客釣魚郵件，檢測員工資安風險意識，輔以資安宣導及教育訓練，避免不當郵件行為造成資安風險。

(4) 網路安全保護：導入次世代防火牆，包含上網行為管理、URL 過濾、入侵防禦系統，定期檢視防護報告並適時調整安全策略，避免使用者瀏覽惡意網站及遭降低企業遭受外部網路攻擊。

(5) 建立安全檔案交換機制：導入企業級雲端檔案交換平台，資料傳輸與資料儲存區加密，降低資料被意外查看風險。完整留存檔案存取稽核軌跡，並定期檢視系統日誌。

五、 資安事件通報程序