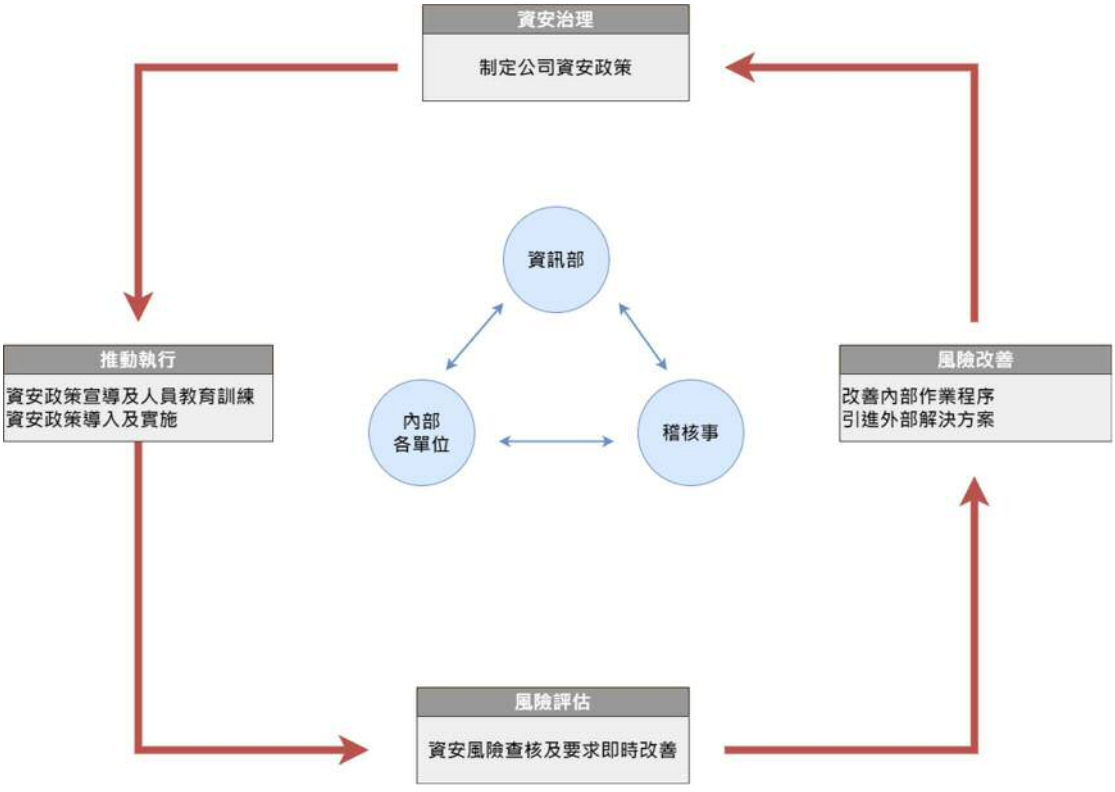
資通安全政策及具體管理方案

資通安全管理

資通安全風險管理架構

- 本公司資通安全（簡稱資安）之權責單位為資訊室，該單位設置資安主管與資安人員，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業及資訊安全政策推動與落實，以確保本公司營運所需之資訊與資訊資產的機密性、完整性及可用性。
- 本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管與專職稽核人員，負責督導內部資訊安全執行狀況，若查核發現缺失，即要求受查單位提出相關具體改善作法， 並定期追蹤改善成效，以降低內部資訊安全風險。
- 組織運作模式：資訊室制定公司資訊安全政策及資訊安全作業，內部各單位推動執行並 加強宣導資訊安全政策、資訊安全作業及人員教育訓練，落實資訊安全政策的導入及實施，稽核室進行資訊安全風險查核，如發現缺失，要求受查單位提出相關具體改善作法，且定期追蹤改善成效。



資通安全政策及具體管理方案

本公司資通安全管理政策，包含三個面向：

一、 制度：訂定公司資通安全相關管理制度，規範人員作業行為，並定期執行內部稽核，以降低內部資通安全風險。
資安治理制定公司資安政策風險改善改善內部作業程序引進外部解決方案推動執行 資安政策宣導及人員教育訓練資安政策導入及實施風險評估資安風險查核及要求即時改善資訊室、內部各單位、稽核室。

二、科技：建置有關資通安全防護設備，以提昇資訊環境之安全性，落實資通安全管理措施。

三、 人員：進行資通安全教育訓練或宣導，提昇員工資通安全意識或相關知識。

資通安全風險評估情形

本公司資訊室定期評估資通安全風險情形，並每季向董事會報告。

資安治理	資安治理	評估情形
2024/05/16	系統連線申請	正常
	檔案安全控制	正常
	設備安全控制	正常
	資通安全檢查控制	正常
2024/06/13	系統連線申請	正常
	檔案安全控制	正常
	設備安全控制	正常
	資通安全檢查控制	正常
2024/07/18	系統連線申請	正常
	檔案安全控制	正常
	設備安全控制	正常
	資通安全檢查控制	正常
2024/08/22	系統連線申請	正常
	檔案安全控制	正常
	設備安全控制	正常
	資通安全檢查控制	正常

資通安全管理措施

一、各部門之個人電腦，安裝防毒軟體，避免電腦病毒入侵。
二、資訊室每日上網更新病毒碼及掃毒引擎。
三、裝設防火牆以隔絕外來侵害。
四、資訊人員定期檢視伺服器上郵件收發情形，若有異常狀況應呈報權責主管處理。

投入資通安全管理之資源

為實踐資通安全管理措施，投入之資源如下：

一、網路硬體設備如防火牆、郵件防毒、垃圾郵件過濾、上網行為分析、網管型集線路等。
二、軟體系統如端點防護系統、備份管理軟體及加密軟體等。
三、購置硬碟備份、入侵防護服務等。
四、投入人力 ： 每日各系統狀態檢查、每週定期備份及備份媒體異地存放之執行、每年至少 一次資安宣導教育課程、每年系統災難復原執行演練、每年對資訊循環之內部稽核、會計師稽核等。
五、資安人力 ： 資安主管一名及資安人員二名，負責資安架構設計、資安維運與監控、資安事件回應與調查、資安政策檢討與修訂，資安主管每年向董事會至少報告一次。