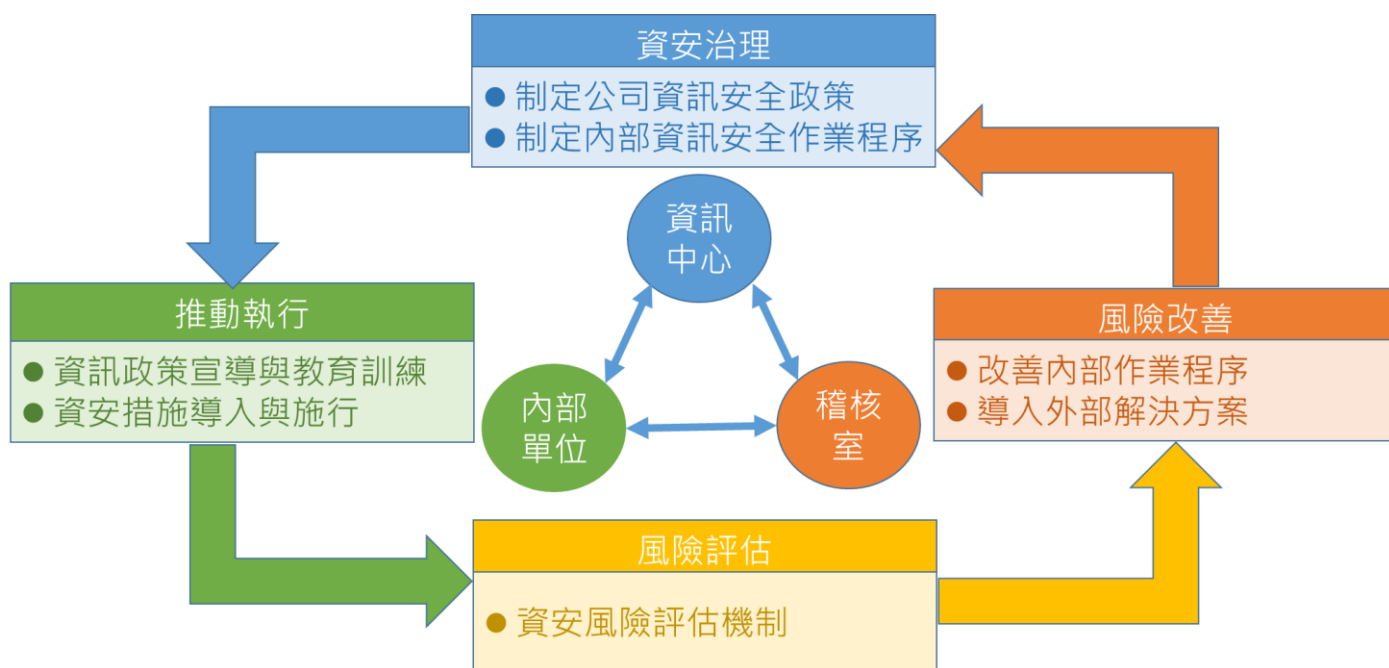


# 資通安全政策及管理方案

## 資通安全風險管理架構

- 本公司資訊安全之權責單位為資訊中心，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識。
- 本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，旋即要求受查單位提出相關改善計畫並呈報董事會，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，確保可靠度目標之達成且持續改善。



## 資通安全政策

本公司已於 110 年 1 月份訂定資訊安全政策，作為資通安全管理最高指導方針，以達到各項資訊系統能正常運作及維護重要資訊系統的機密性，並確保資訊及網路系統之安全維運，達到永續經營目的。

資安承諾：

遵守資安政策，建置資安系統，落實資安管理。

加強教育訓練，提昇資安意識，確保永續經營。

### 資訊安全管理措施：

資訊安全管理措施		
類型	說明	相關作業
存取管制	人員帳號權限、系統存取管控及資料傳輸管道之控制措施	<ul style="list-style-type: none"><li>●人員帳號權限管理與稽核</li><li>●內/外部系統存取管控措施</li></ul>
威脅防護	內、外部潛在弱點、威脅、中毒防護措施	<ul style="list-style-type: none"><li>●主機/電腦弱點、威脅、病毒檢測及更新措施</li><li>●內/外部資安設備建置與管理</li></ul>
系統可用性	系統可用狀態與備份備援之處置措施	<ul style="list-style-type: none"><li>●系統/網路可用狀態監控及通報機制</li><li>●異常處理，定期災害復原演練</li><li>●資訊備份措施，異地備份機制</li></ul>

## 投入資通安全管理之資源：

本公司資訊中心定期辦理員工資安教育訓練及信件宣導資訊安全觀念。

本公司已於 111 年導入 ISO 27001 資通管理系統，並取得 ISO 27001 認證，目前證書之有效期為 112 年 1 月 27 日至 114 年 10 月 31 日。透過 ISO27001 資通安全管理系統之導入，強化資通安全事件之應變處理能力，保護公司與客戶之資產安全。

### 111 年度執行情形：

本公司於 111 年度檢討各單位資安政策之執行情形，當年度並無危害本公司資訊安全之事件。

本年度辦理 2 次異地備援演練及加強對員工宣導對於資訊安全風險之應變與警覺性(於公司內網首頁宣導資訊安全政策及不定時 e-mail 宣導)。

為加強同仁資安意識，公司於 111 年起增加資訊安全課程，並列入全體同仁必修課程，以強化資訊安全觀念。