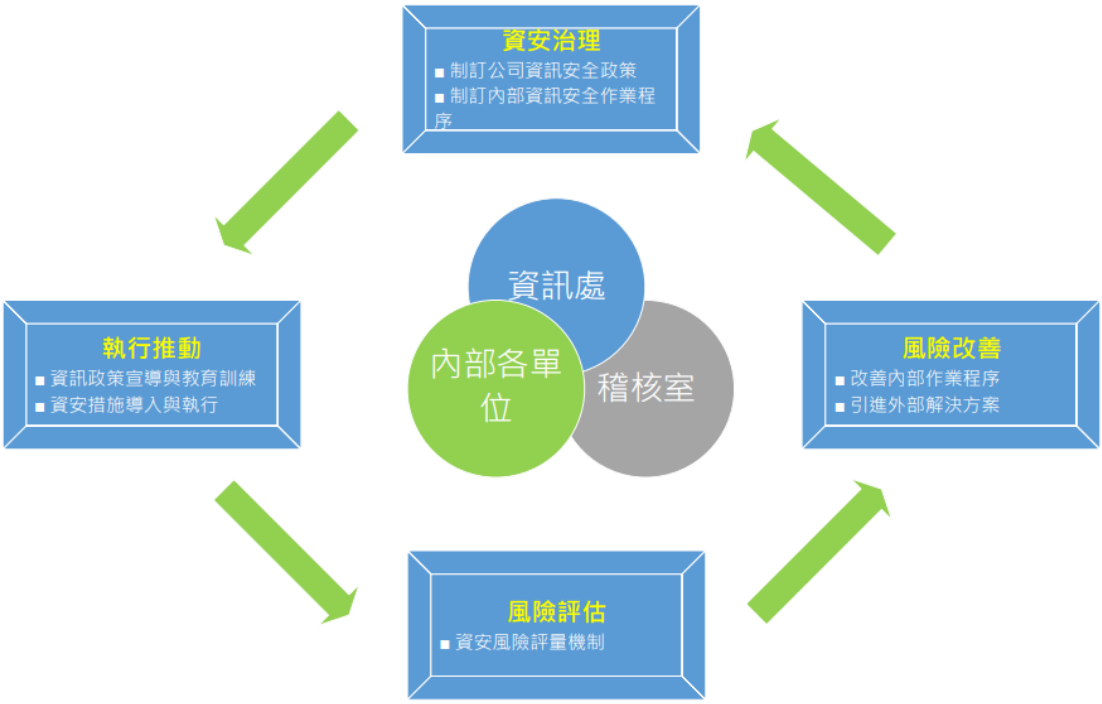
一、目的及組織

1. 目的：

i. 為配合國家資通安全政策並強化公司內部資訊安全管理，以確保相關資訊資產的機密性、完整性及可用性及資訊業務持續運作之資訊環境，並符合國內外相關法規之要求，使其免於遭受內、外部的蓄意或意外之資安事件威脅。

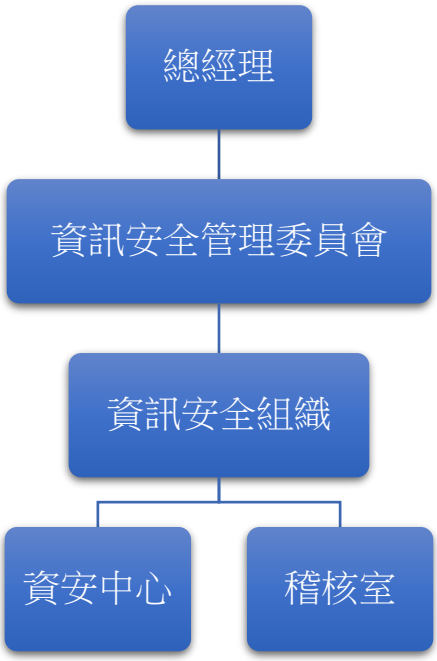
ii. 本公司稽核室會定期查核，若查核發現缺失，即要求受查單位提出改善措施，且定期追蹤改善結果，以降低內部資安風險。資訊安全管理策略採用 PDCA（Plan-Do-Check-Action）循環流程管理模式，確保目標之達成且持續改善。



2. 組織：

為強化本公司之資通安全風險管理、確保資料、系統及網路安全，設立資訊安全管理委員會及資訊安全組織。委員會為本公司資訊安全之權責單位，負責制定內部資訊安全政策、規劃資訊安全作業、資安政策推動與落實。由總經理為召集人，各處級單位最高層級主管擔任委員，並由資訊處最高層級主管擔任資安代表、內部稽核最高主管為觀察員，每季召開會議，檢視即決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施的有效性。

資訊安全組織成員包含資安中心與稽核室。資安中心依資訊安全管理委員會決議之事項，執行資訊安全系統建置，包含網路、系統與資料管理；稽核室依循資訊安全準則，進行資訊安全稽核作業。



二、資通安全政策

1. 為使本機關業務順利運作,防止資訊或資通系統受未經授權之存取、使用、控制、 洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality)、完整性 （Integrity）及可用性（Availability)，特制訂本政策如下，以供全體同仁共同遵循：

i. 建立資通安全風險管理機制,定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

ii. 保護機敏資訊及資通系統之機密性與完整性,避免未經授權的存取與竄改。

iii. 因應資通安全威脅情勢變化,辦理資通安全教育訓練，以提高公司同仁之資通安全意識，公司同仁亦應確實參與訓練。

iv. 針對辦理資通安全業務有功人員應進行獎勵。

v. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

vi. 禁止多人共用單一資通系統帳號。

vii. 機密資料檔案的讀取及複製,須符合本機關各業務單位的規定，並經該單位主管或其授權人員核可。

viii. 本政策每年應至少評估檢討一次，以反映公司資訊安全需求、政府法令法規、外在網路環境變化及資訊安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。

ix. 本政策如遇重大改變時應立即審查,以確保其適當性與有效性。必要時應告知相關單位及委外廠商，以利共同遵守。

三、具體管理方案及投入資通安全管理之資源

項目	具體管理措施
防火牆防護	防火牆設定連線規則 如有特殊連線需求需額外申請開放
使用者上網控管機制	使用自動網站防護系統控管使用者上網行為 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站
防毒軟體	使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。 伺服器與電腦用戶端均安裝有主從式架構的防毒軟體，病毒碼採自動更新方式
作業系統更新	作業系統自動更新，因故未更新者，由資訊部協助更新。
應用系統權限管理	依使用者帳號，設定存取系統的權限
郵件安全管控	郵件伺服器設置有郵件防毒、垃圾郵件過濾、偵測不當郵件行為，以防止惡意郵件造成不可預期的危害。 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
網站防護機制	網站備有防火牆裝置阻擋外部網路攻擊。
資料備份機制	重要資訊系統資料庫皆設定每日備份。
電腦機房設備管理	伺服器置於專用機房，門禁限制人員進出且保留出入紀錄。 機房採獨立空調並放置乾式滅火器。 所有伺服器連接 UPS，避免停電或異常斷電對伺服器之傷害。
重要檔案上傳伺服器	公司內各部門重要檔案存放於伺服器，由資訊部統一備份保存。

四、執行狀況及重大資通安全事件

1. 本公司目前無重大資安事件導致營業損害之情事。
2. 依公司「資通安全事件通報及應變辦法」，持續落實資訊安全管理政策目標，定期實施復原計劃演練，確保公司重要系統與資料安全。