# 資通安全管理

一、 企業資訊安全管理策略與架構：

1. 企業資訊安全治理組織

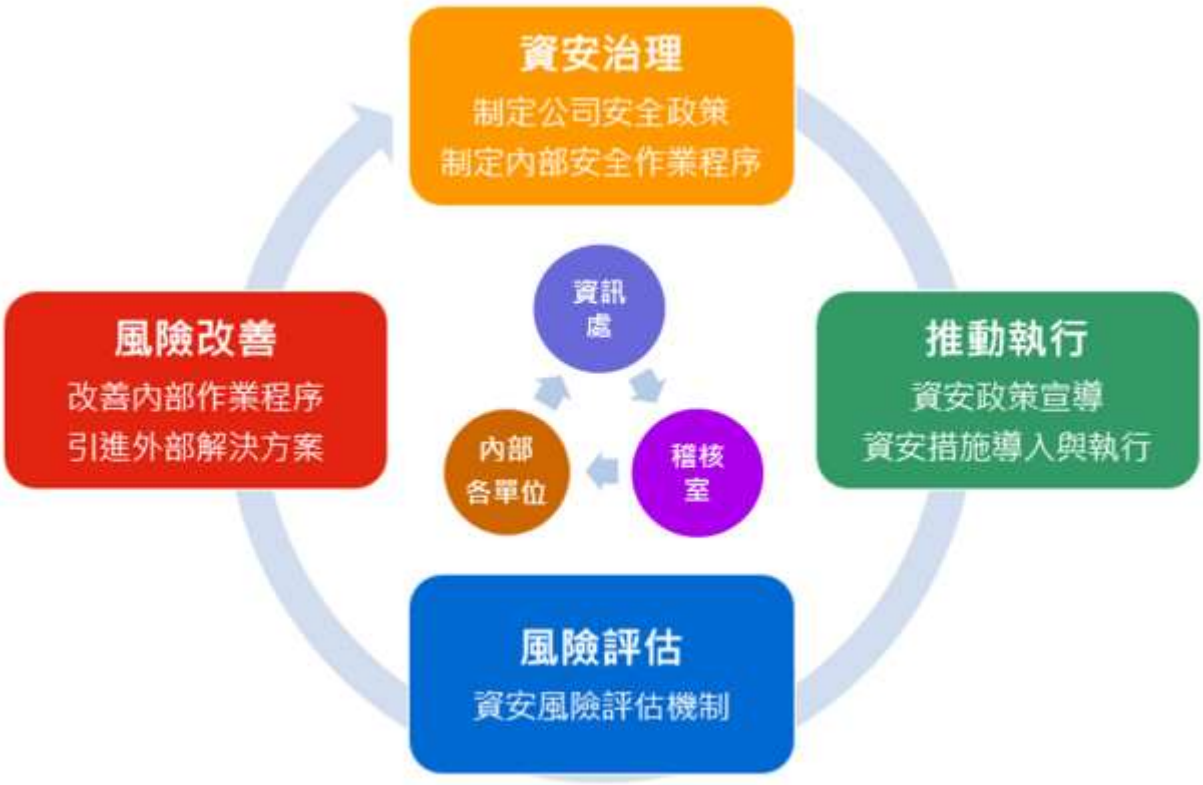
本公司現有網路管理人員 2 名兼任資通安全管理，並將管理規則與執行作為與資訊主管報告訂定資訊安全管理政策，以強化本公司資訊安全管理，確保資料、系統、設備及網路安全，保障公司與全體員工之權益，並全面提升資安意識。資訊處已於 2022 年 12 月 28 日向董事會報告目前資訊安全管理情形。

2. 資訊安全風險管理架構

(1) 本公司資訊安全之權責單位為資訊處，負責規劃、執行資訊機房、電腦資訊檔案安全、網路安全、郵件安全管理、資訊控制存取等管理及推動資訊安全意識。

(2) 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，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，以降低資訊安全風險。

(3) 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。



二、 資通安全政策

1. 資通安全之目標：

為貫徹本公司各項資訊管理制度能有效運作執行，建立安全及可信賴之電腦化作業環境，確保資訊系統、設備網路之安全維運，以保障公司利益及各單位資訊系統之永續運作，達到永續經營目的。

2. 資通安全之範圍：

(1) 人員管理及資訊安全教育訓練。

(2) 電腦系統安全管理。

(3) 網路安全管理。

(4) 系統存取管制。

(5) 系統及維護安全管理。

(6) 資訊資產安全管理。

(7) 實體及環境安全管理。

(8) 資訊安全稽核。

3. 資訊安全的原則及標準：

(1) 不定期資訊安全宣導，包括資訊安全政策、資訊安全法令規定、資訊安全作業程序、資訊安全案例以及如何正確使用資訊科技相關設施等，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工對資訊安全意識，並遵守資訊安全規定。

(2) 為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及防範措施，對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。

(3) 為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。

(4) APP 開發遵守

4. 資訊安全具體管理措施：

| 項目 | 具體管理措施 |
| --- | --- |
| 權限管理 | 人員帳號、權限管理與系統操作行為之管理措施：<br>● 人員帳號權限管理與審核。<br>● 人員帳號權限定期盤點。 |
| 存取管控 | 人員存取內外部系統及資料傳輸管道之控制措施：<br>● 內部網路、DMZ 網段、測試網段與外部網路之連線存取均需透過防火牆之安全管控。<br>● 使用自動網站防護系統控管使用者上網行為。<br>● 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。 |
| 外部威脅 | 潛在弱點、中毒管道與防護措施：<br>● 使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。<br>● 使用軟體及作業系統定期更新。<br>● 有自動郵件掃描威脅防護，如不安全的附件檔案、釣魚郵件、垃圾郵件，及惡意連結。 |
| 系統可用性 | 系統可用狀態與服務中斷時之處置措施：<br>● 重要資訊系統定期由專業顧問檢查、調整及優化。<br>● 各部門重要檔案存放於伺服器，由資訊單位統一備份保存。<br>● 重要資訊系統資料庫皆設定每日備份<br>● 定期進行災害復原演練。 |