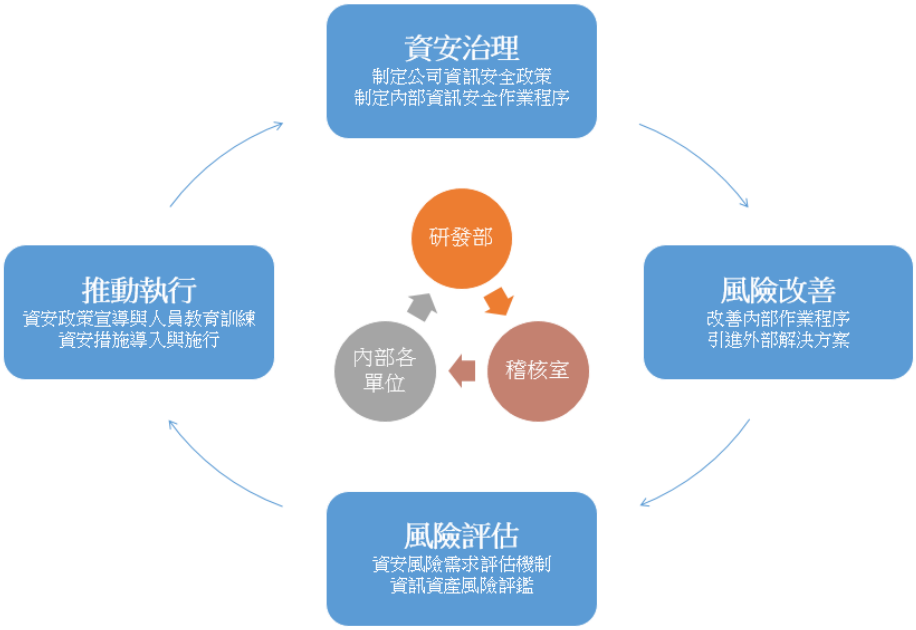
資通安全風險管理

一、資通安全風險管理架構

1. 本公司資訊安全之權責單位為研發部，該部設置資訊主管一名與專業資訊人員一名，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資訊安全政策推動與落實。
2. 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稽核職務代理人，負責督導內部資訊安全執行狀況，若有查核發現缺失，即要求受查單位提出相關改善計畫與具體作為，且定期時續追蹤改善成效，以降低內部資訊安全風險。
3. 組織運作模式為循環式管理，確保可靠度與目標之達成且持續改善。



二、資通安全風險政策

1. 台北總公司與新屋廠皆建立設置妥善防火牆，以阻擋外部駭客之攻擊，並不定時檢閱相關記錄檔。
2. 電腦用戶端部署安裝防毒軟體，並不定時檢閱病毒記錄及相關對應處理。
3. 不定時不定期進行作業系統更新相關作業，減少系統漏洞而降低資訊安全風險。
4. 建立妥善的備份機制與方式。

三、資通安全風險管理方案

1. 電腦機房設備管理：

I. 本公司電腦伺服器主機及應用伺服器皆置於專用機房，機房門禁限制人員進出，且保留進出紀錄存查。
II. 機房內部設立獨立空調冷氣，並適當的溫度環境下運轉；且放置乾粉式滅火器，可適用於一般或電器所引起的火災。
III. 機房伺服器主機連接不斷電系統，確保臨時停電或異常斷電時不會中斷電腦應用系統的運作。

2. 網路安全管理：
   I. 對外連線設置企業級多功能防火牆，以防止駭客非法入侵。
3. 伺服器或電腦用戶端防護管理：
   I. 伺服器與電腦用戶端設備內均安裝有端點防護多功能軟體(防毒、防惡意程式、防間諜程式…等)，病毒特徵碼採取自動更新方式，確保能阻擋並提升各類病毒或資訊安全防護。
   II. 電子郵件設置有郵件防毒、垃圾郵件過濾機制及反勒索詐騙的郵件防禦機制，以防堵上述類別惡意郵件被電腦用戶端收下後，造成不可預期的損失或危害。
4. 應用系統使用者帳號權限管理：
   I. 帳號管理，系統設定要求使用者需定期進行密碼變更。
   II. 權限管理，依不同使用者職務屬性定義其可使用權限。
5. 確保系統可用性：
   I. 妥善的備份管理策略，採取每日備份機制，備份媒體共有兩份，一份保留於機房，另一份備份媒體存放於銀行保險箱進行異地資料存放。
   II. 災害復原計畫演練，每年不定期實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，確保備份媒體的正確性與有效性。

四、投入資通安全管理之資源

1. 網路：採用企業級防火牆，外網 VPN 連線認證，提升安全性。
2. 硬體：採用伺服器等級設備，提升穩定性。
3. 軟體：付費專業備份軟體、自動更新端點防護軟體，提升防護性。
4. 人力：設置資訊主管一名與專業資訊人員一名，負責資安架構設計與維運，資安事件回應與調查，資安政策檢討與修訂，提升可靠性。