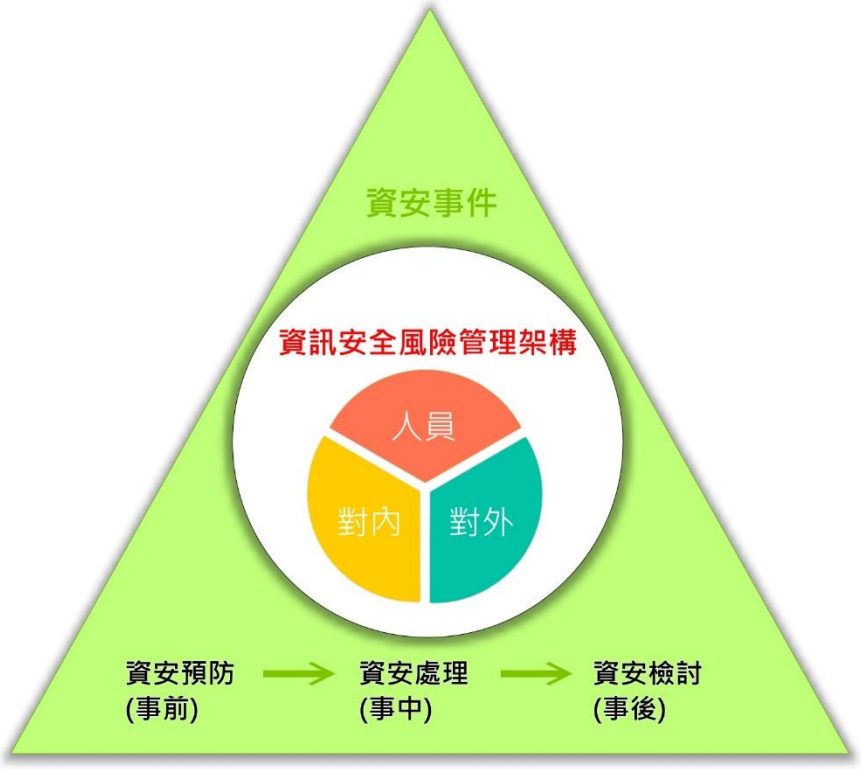
資訊安全風險管理架構



本公司資訊安全風險管理架構針對人員、對內及對外進行風險管理。

- 人員：資安政策、訓練及宣導、權限管控
- 對內：網路管控、防毒、資料保護
- 對外：防火牆、人侵防禦系統、日誌記錄

且對於資訊安全事件之預防準備、發生處理及事後調查檢來討進行因應。

1. **資安預防(事前)**
   - 人員：加強人員對於資安事件認知及防範
   - 基礎建設：建立更安全、穩定和快速的網路環境及設施服務
   - 資料：加強資料存取安全性及完整性
2. **資安處理(事中)**
   - 事件的即時處理、控制及阻止
   - 網路及服務的回復
   - 資料的保全、備份及回復

3. 資安檢討(事後)

- 證據保存及事件調查
- 調查結果檢討及改善

並依循資訊安全風險管理運作：

並達到以下之標的：

1.落實資通安全管理政策。

2.培訓資訊人力資通安全專業能力。

3.強化資通安全環境及資訊安全應變能力。

4.達成資訊安全管理政策量測指標。

具體管理方案

本公司目前資訊安全風險管理具體管理方案：

1. 管理政策

目前公司定訂資訊安全政策等，以確保資料、系統、設備及網路之使用安全，相關資料存取及服務使用均需依流程規定進行申請及審核。並定期的稽核部門及事務所人員查核，必要時成立資訊安全委員會。

2. 技術

公司使用防火牆、人侵防禦系統、防火牆進行內外網路安全。

使用網路負載’、機房消防設施與不斷電系統來加強基礎建設。

公司郵件以加密方式進行通訊、存取資料進行身分權限管控、定期資料備份及災難回復演練。

3. 人員

一般使用者：不定期進行資安政策訓練及宣導，提升員工資安意識提升。

管理者：吸收資安相關資訊、參與資安相關會議，提升資安專業知識和技能。

決策高層：定期與各部門舉行議會，下層人員並每週進行工作報告。