資通安全管理架構與具體管理方案

資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等：

1.資通安全風險管理架構：本公司訂有資訊安全政策管理辦法，由專責的資訊部門，負責公司日常資通安全。另為有效推行資訊安全工作，成立資訊安全委員會，統籌資訊安全政策、計畫、資源調度等協調及研議事項。前項委員會召集人，由總經理指定之副總經理或高階主管擔任，負責資訊安全管理事項之協調及推動；委員會成員由總管理處、財會部、管理部、法務部及資訊部等單位主管擔任。

2.資通安全政策：為維護資通安全，遵循以下原則處理公司之資安

(1) 遵循公司所訂定之內部控制(包括但不限於 CM-資訊循環)與相關核決權限規定。

(2) 對員工進行資訊安全教育及訓練。

(3) 使用合法軟體。

(4) 公司資料庫進行備份、異地備援。

(5) 建立防火牆，購買合法防毒軟體，並定時更新相關病毒碼及掃毒引擎。

(6) 建立災難復原計畫。

(7) 保護員工及交易對象之個人資料。

(8) 其他法令所規定事項。

3.具體管理方案：為確保本公司資訊的合法存取，於可能遭受外力入侵時，亦能提供完整、未中斷之資訊系統運作；於事故發生時，作迅速必要之應變處置後，能在最短時間內回復正常運作，以降低該事故可能帶來之損害。資通安全管理範圍如下：

(1) 資訊安全權責分工

(2) 人員安全管理及資訊安全教育訓練。

(3) 電腦系統安全管理。

(4) 網路安全管理。

(5) 系統存取控制管理。

(6) 系統發展及維護安全管理。

(7) 資訊資產安全管理。

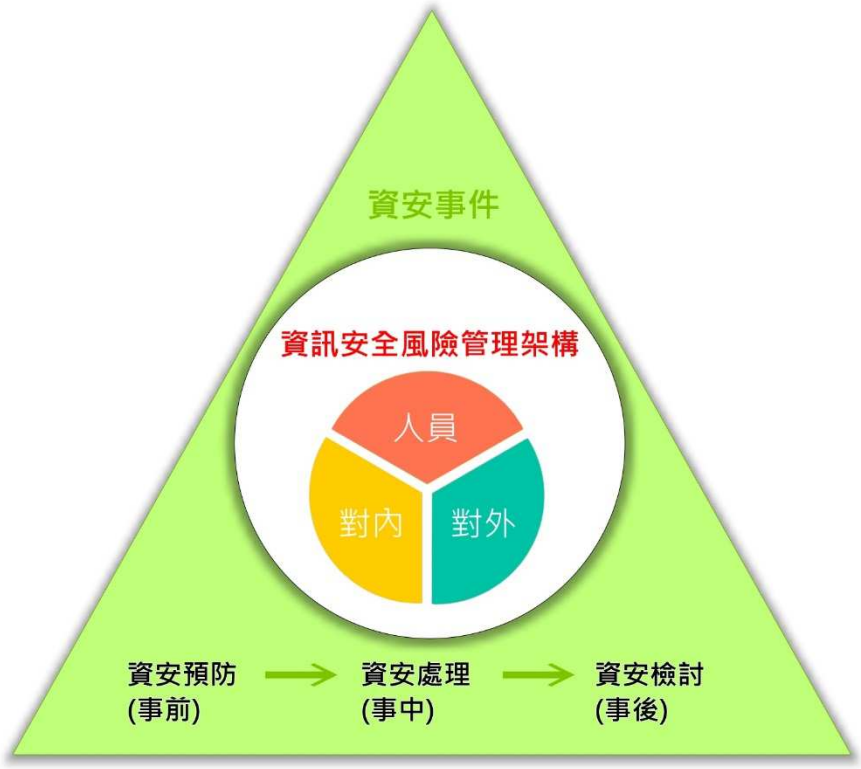
(8) 實體及環境安全管理。

(9) 業務永續運作計畫管理。

(10) 其他資訊安全管理事項。

4. 投入資通安全管理之資源：因應公司發展配置建置資訊部門，設有專責人員兩位；依公司人數採購足量軟體、購置防毒及防火牆軟硬體、舉辦資訊安全教育及訓練等宣導活動、建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

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：