資通安全管理

一、資通安全風險管理架構

本公司設有資安專責單位由資訊管理部主管人員負責資訊安全管理事項的協調及推動，並視需要成立資訊安全推動小組，資訊安全推動小組由總經理為召集人，資訊管理部主管負責執行每年安全性評估報告。組織團隊包含資訊安全處理小組與資安審查小組；資訊安全處理小組負責執行資訊安全政策、計畫及技術規範之建置及安全評估等事項管理；資安審查小組配合公司稽核單位進行資訊機密維護及稽核管理等事項工作；資訊使用單位負責辦理資料及資訊安全需求提出、使用管理及保護等事項。

二、資通安全政策

1、強化人員資安認知。

2、避免機敏資料外洩。

3、落實日常維運有效。

4、確保營運永續運作。

三、具體管理方案

項　目	內　　容
人員安全與管理	●接觸機敏類、機密類資訊時，經適當安全評估。 ●不同職級人員定期資訊安全教育訓練及宣導。 ●新進人員職前電腦網路及資訊安全宣導。 ●人員離調時，相應存取權限及時調整。
資產分類及控制	●建立資訊資產清冊，訂定資訊資產的專案、保管人等維護更新。 ●因應資訊外洩對公司衝擊為考量基礎，訂定資訊安全等級管制。
存取控制	●訂定資訊系統存取控制規定，限制使用者在授權範圍內存取網路系統服務。 ●使用者存取管理:註冊管理、特別權限管理、通行碼原始碼管理、存取權限、委外廠商遠端登入管控。 ●對機敏類及敏感類資訊，考量建置獨立或專屬作業環境。
電腦處理個資保護事項	●員工獨立登入帳號及密碼控管。 ●定期審查使用者權限及定期備份資料。 ●報廢電腦之硬碟資料銷毀程序與離職員工儲存設備回收管理。
委外資訊安全	●外部連線安全控管機制。 ●第三者存取之安全契約。
資料安全保護技術強化	●文件及資料加密控管及追蹤。 ●郵件外寄控管。 ●安全防護軟硬件管控。
確保營運系統持續運作	●系統備份。 ●復原演練。 ●應急防範措施。
宣導與評估	●每年定期執行安全評估。

項　目	內　　容
檢核	●每年對資訊安全政策評估，以反應法令、技術及業務等發展現況 針對不同職級人員定期進行資安教育訓練及宣導。

四、投入資通安全管理之資源

本公司針對資訊安全政策、計畫及技術規範之建置及評估等事項，由資訊管理 課電腦通訊組人員負責辦理，每年至少一次對資訊使用者、資訊系統及資訊設備等進行安全評估，以確保其遵行資訊安全政策及規定；對於資訊安全政策，安排每年評估一次，以反應法令、技術及業務等最新發展現況，確保資訊安全。

五、緊急通報程序

當發生資訊安全事件時，發生單位通報"資訊安全推動小組"，判斷事件類型並找出問題點，即時處理並留下紀錄。本公司也將持續落實資訊安全管理政策目標，並定期實施復原計劃演練，保護公司重要系統與資料安全。