資通安全管理

一、管理架構：

行政管理處-資訊部門人員負責統籌並執行資訊安全政策，宣導資訊安全訊息，提升員工資安意識，蒐集資訊安全管理系統績效及有效性之技術、產品或程序等。由稽核人員每年就內部控制制度—電腦化資訊處理循環，進行資訊安全查核，評估公司資訊作業內部控制之有效性。

二、資安政策：

(一)建立檔案及設備安全控制作業與主機及網路使用之管理機制。

(二)確保依據部門職能規範資料存取，防止未經授權之存取動作。

(三)訂定營運持續管理及備援備份還原之演練，確保公司業務持續運作。

(四)定期宣導資訊安全政策，推廣員工資訊安全之意識與強化其對相關責任之認知。

(五)建立資訊機房實體環境安全防護措施，並定期施以相關維護及保養。

(六)定期執行資安稽核作業，確保資訊安全能確實落實。

三、具體管理方法：

(一)網際網路資安管控：定期對電腦系統及資料儲存媒體進行病毒掃瞄；架設防火牆(Firewall)；定期電腦作業系統及密碼更新。

(二)資料存取管控：電腦設備皆有專人保管，並設定帳號與密碼；依業範圍與職務權責分別賦予不同存取權限；離職人員即取消原有權限；設備報廢前將機密性、敏感性資料備份。

(三)應變復原機制：建立系統備份機制，每年採定期與不定期方式執行系統復原計劃之測試。

(四)宣導及檢核：日常宣導資訊安全資訊，提升員工資安意識；定期執行資通安全檢查呈報。

(五)訂定保密條款：對委外維護廠商均於簽定之合約中，要求明訂「保密條款」以維公司資料安全及保密性

(六)機房安全控制：公司依職責劃分「機房門禁管制表」限非資訊單位人員嚴禁進出；另於機房內設置獨立空調設備、高架地板或櫃子、不斷電系統（UPS)、自動火警偵測及緊急照明設備等防護設備。