■ 資通安全管理

1. 風險管理架構

本公司由資訊部設置專責資安主管與資安人員針對資訊安全之防駭、防毒、防災進行規劃，制定公司資安政策與因應措施，執行相關資安作業，定期彙整提供稽核進行查核，如需改善，由資訊部提出改善計畫並進行改善與追蹤。

2. 資通安全政策

本公司之資安政策目標為『持續保護、強化應變、自動偵測、快速復原』，根據此政策制定相關資安管理辦法，並根據實際狀況隨時修正管理辦法與目標以達成完善之資通安全目標。

(1) 資料存取控管

- 員工所使用系統帳號及其所設定密碼應符合系統複雜度原則，並定期更新密碼，並依職能設定各系統權限以作為有效控管機制、製作檢核表以記錄各系統設備問題處理...等。

(2) 設備安全

- 設備機房得設置溫度控制、異常警告等相關安全監控措施並應考量地震、火災等不可抗力事故發生時之緊急應變措施。
- 公司配屬電腦設備皆應安裝防毒軟體，並維持最新病毒碼。
- 禁止使用未經授權軟體，員工內部電腦軟體統一由資訊部監控，並依工作型態配置預設軟體。

(3) 宣導及檢核

- 隨時宣導資訊安全資訊，並每年進行一次全員資通安全政策宣導事宜。
- 定期內外稽、並由稽核人員報告董事會。

3. 具體管理方案

(1) 於公司內部控制制度之電腦資訊循環中訂有資通安全檢查之控制作業，作為同仁遵行依據，同時不定期檢討內控制度之有效性，進一步強化及落實。

(2) 稽核人員每年對公司資訊安全管理進行稽查，以了解資安運作狀況，評估對各項風險控制及異常事項之改善是否確實，以降低及避免相關資安風險。

4. 投入資通安全管理之資源

(1) 網路硬體設備：防火牆、AD 網域控制站、NAS 備份系統與相關服務之硬體設備等。

(2) 建置相關資安監控機制，隨時監控電腦設備的狀況以預先預防並即時處理可能的資安問題。

(3) 投入人力：每日各系統狀態檢查、定期備份及備份媒體異地存放之執行、每年系統災難復原執行演練、資訊人員不定時進行資安課程進修，新進人員皆須簽定資通安全保密協定。

5. 本公司近兩年度無重大資通安全事件。