資訊安全風險管理：

一、架構及權責：本公司已設置資安小組，負責執行資通安全事件之預防、通報及處理等相關作業，並一年一次向董事會報告。成員與權責如下：

職務	成員	權責
召集人	法務長	督導應變計畫執行成效、核定資事件應變處理事宜。
資安處理人員	資訊部門成員	維護及執行資安防禦、判斷與緊急應變資安事件。
內部稽核人員	稽核部門成員	實施資通安全稽核、評估資安風險、提出改善建議。

二、資訊安全政策：確保本公司電腦資訊係統之安全與正確運作，維護本公司營業秘密及機敏資料，促進資訊之有效利用，並遵守「資訊安全管理辦法」、「公用磁碟機管理辦法」、資訊系統權限管理辦法及「資通安全事故應變辦法」，以保障投資人權益和維護公司信譽。

三、資訊安全具體管理方案：

1. 新式防火牆更換：強化網路控管與偵測能力，分析傳輸內容，針對可疑、惡意或未經授權之網址即時防禦攔阻，強化對抗勒索軟體、病毒感染或殭屍電腦之能力(目前皆已完成汰換)。
2. 評估新式文件加密系統：提升擋案主動防護力，檔案需要在加密的環境中才可閱讀，外寄已加密檔案需要授權解密，外部人員無法任意開啟內部檔案。
3. 資安風險轉嫁：採購年度資安險，降低資安事件造成的損失。
4. 資通安全事故應變能力強化：建立資通安全事故應變辦法、成立資安小組，明訂資安事件發生時的應變措施 SOP。
5. 內網流量資安分析：分析內網流量，強化偵測與感知能力，即時將內部感染與攻擊行為阻斷于終端，降低風險擴散機率。
6. 系統更新汰換：伺服器主機及個人作業系統更新汰換，強化弱點防禦能力。
7. 持續改善：定期舉辦資安教育訓練，並進行社交工程演練，提升內部同仁的資安意識。