資訊安全政策

資訊安全風險管理架構

- 本公司資訊安全之權責單位為資訊室，負責規劃、執行資訊安全管理事項、推廣資訊安全意識，並由管理階層參與衡量整體風險成本。
- 本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。
- 資訊安全管理系統依據規劃（Plan）、執行（Do）、查核（Check）及調整（Act）之滾動模式實施，在風險成本權衡下循序漸進地執行，確保資訊業務運作之有效性及持續性。

資訊安全政策

為強化資訊安全管理，建立安全及可信賴之作業環境，確保資料、系統、設備及網路安全，以達成企業永續經營目的，特訂定本政策，以作為實施資訊安全措施之依據。

- 政策要點：

1. 執行各項作業時，應遵循主管機關頒布之各種法令及本公司相關之規定。
2. 工作分派應考量職能分工，職務責任範圍應予區分，以避免資訊遭未授權修改或誤用。
3. 與本公司往來之協力廠商、委外廠商、顧問或客戶，應視業務性質於必要時要求其簽訂保密合約。
4. 針對所有內部員工辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升本公司資訊安全水準。
5. 所有員工有義務保護本公司機密敏感資料，禁止未授權的情況下接觸、使用或是將該資訊揭露、告知與業務無關之同仁、廠商及其他客戶。
6. 為防範電腦病毒及惡意程式之攻擊，應安裝合法防毒軟體與防火牆，並持續更新病毒碼及掃毒引擎。
7. 公司內重要資料應建立完整備份機制，重要系統應建置備援機制。
8. 員工違反資訊安全相關規定，其應負之資訊安全責任依公司內部相關辦法處理。

- 具體管理措施

管理項目	措施內容
網路安全管理	• 對外網路配置防火牆，阻擋外部攻擊與入侵。
存取控制	• 資訊系統皆須設定登入帳號、密碼，密碼定期更改。 • ERP 系統及雲端槽區均依職務設置權限。
電腦與主機安全管理	• 個人電腦與主機安裝防毒軟體，並保持防毒作業持續更新。 • 主機架高並配有 UPS。
郵件安全防護	• 開啟垃圾郵件過濾機制。 • 加強郵件帳號安全性，加入可偵測偽造信的電子郵件閘道。
資料備份	• 資料庫每日進行備份。 • 員工個人電腦工作槽區每日進行備份。 • 定期對主機備份資料作異地備份。
可靠度管理	• 每日對主機、雲端槽區、ERP 系統進行可運作檢測。 • 定期對 ERP 備份資料進行可用性及完整性測試。