資訊安全政策

1. 目的

為維護資訊之機密性、完整性及可用性，降低資訊安全風險並維持業務持續運作，本公司將資訊安全視為企業營運與永續發展之重要基礎，依營運需求、相關法令及 ISO/IEC 27001 國際標準建立資訊安全管理制度，持續提升資訊安全治理能力，保障公司及利害關係人之資訊安全。

2. 範圍

本政策適用於本公司資訊資產、資訊系統、網路及相關資訊安全管理活動，並涵蓋執行相關業務之內部及外部人員。

3. 資訊安全治理與權責

本公司建立資訊安全管理組織及權責機制，由資訊安全委員會督導資訊安全管理制度之推動，並定期召開「資安管理審查會議」，檢視資訊安全績效、風險及改善事項，持續提升資訊安全管理成效。

4. 核心管理原則

本公司依營運需求及資訊安全風險持續推動資訊安全管理，並遵循下列原則：

- 資訊保護：維護公司及利害關係人資訊之機密性、完整性及可用性，降低資訊安全風險。
- 風險管理：持續辨識及評估資訊安全風險，並依風險程度採取適當之管理及防護措施。
- 事件應變：建立資訊安全事件通報及應變機制，降低事件對營運及利害關係人之影響。
- 營運持續：建立營運持續及復原機制，降低中斷風險，提升營運韌性。
- 第三方管理：管理供應商及第三方資訊安全風險，降低供應鏈資訊安全風險。
- 新興科技：關注人工智慧（AI）等新興科技風險，兼顧創新應用與資訊安全。
- 安全意識：持續推動資訊安全教育、訓練及宣導，提升全體人員之資訊安全意識及責任。
- 法令遵循：遵循適用之法令、法規、契約及資訊安全相關要求。
- 持續改善：定期檢視資訊安全管理績效、風險及環境變化，持續改善資訊安全管理制度。

5. 資訊安全目標

本公司依營運需求及資訊安全風險訂定資訊安全目標，配置適當資源並定期監督及評估達成情形，以持續提升資訊安全管理成效。

6. 政策制訂與修訂

本政策每年至少檢討一次，必要時修訂；相關修訂應經適當管理階層審核及核定後實施。