資通安全管理政策

1. 目的

本公司致力於保護其資訊與通訊資產，並維護一個安全且具韌性的營運環境。本政策旨在概述管理資訊安全風險、強化組織韌性，以及支持負責任與永續商業營運的治理框架。本框架參考了 ISO 27001、國內法規及國際公認實務。

2. 範圍

本政策適用於本公司管理的所有資訊與通訊資產，包括硬體、軟體應用程式、網路基礎設施、雲端服務，以及委外服務。所有使用者及經授權人員均應遵守本政策。

3. 治理架構

本公司已建立由上而下的治理框架，以監督資訊安全管理，確保問責性、透明度及有效的風險監督。

3.1 資訊安全委員會

委員會由總經理擔任主席，並由相關部門高階主管組成。委員會每年召開會議，審查策略、評估風險態勢，並監督安全措施的有效性。

3.2 資訊安全長（CISO）

由資訊部門主管擔任，CISO 負責協調資訊安全管理、報告風險狀況，並支持持續改善工作。

3.3 支援團隊

- 資安事件應變小組：處理事件通報、遏制、調查與復原，並進行定期演練。
- 安全管理小組：監督日常安全營運、訓練、政策執行與稽核追蹤。
- 內部稽核小組：執行稽核、評估合規性，並提供改善建議。

4. 資訊安全管理核心原則

本公司遵循「規劃–執行–查核–行動」（Plan–Do–Check–Act, PDCA）循環，以支持網路安全成熟度的持續提升。關鍵領域包括：

- **持**續改善：定期審查風險、控制措施與政策相關性。
- 安全政策合規：遵守 ISO 27001 及適用法律。
- 風險管理：識別與評估威脅、弱點及控制措施的有效性。
- 存取治理：應用最小權限原則、多重要素驗證及定期存取審查。
- 事件管理：實行即時通報、協調的應變及復原機制。
- 業務永續與災害復原：確保在發生服務中斷時能及時恢復服務。
- 第三方管理：要求供應商遵守安全標準與合約義務。
- 監管合規：確保遵守個人資料保護與資訊安全要求。

5. 營運安全實踐

- 核心營運識別：根據風險等級對關鍵業務功能與系統進行分類。
- 資產清單與風險評估：維護更新的清單，並依國際標準執行評估。

- 安全系統開發：應用標準化的 SDLC 實務，包括安全測試與程式碼審查。
- 存取控制：嚴格執行最小權限存取，並定期審查帳戶權限。
- 日誌記錄與監控：依法律要求保留日誌，並實施監控以強化偵測與應變能力。

6. 委外作業與供應商管理

- 供應商標準 ：供應商必須展現足夠的安全能力，例如持有 ISO 27001 認證。
- 評估與合約要求：進行預先審查，並在合約中包含安全要求、通報義務、稽核權利及服務水準預期。
- 存取監督：基於最小權限原則授予存取權，並定期稽核存取日誌。
- 事件處理：要求立即通報安全事件並進行影響評估；重大事件可能影響服務範圍或合約條款。

7. 業務持續與災害復原

- 風險評估與業務影響分析 BIA：識別業務風險並定義復原目標。
- 復原策略：維護異地備份，並採用具韌性的基礎設施以確保連續性。
- 緊急應變：建立結構化的緊急情況溝通與協調程序。
- 測試與演練：每年至少執行一次災害復原演練以驗證準備度。

8. 事件通報與應變

- 通報機制：實施基於嚴重程度的分級通報結構。
- 應變執行：隔離受影響系統、評估根本原因，並實施矯正措施。
- 事後分析與改善：根據事件審查結果，更新風險評估與控制措施。

9. 稽核與審查

本公司執行定期內部稽核、風險評估 及必要訓練，以確保持續合規性與能力改善。

10. 政策管理

本政策經董事長核准後生效，任何修訂應遵循相同的核准程序。