資訊安全風險管理架構

1.【資訊安全目的與範圍】：

目的：本公司為強化資訊安全管理、確保業務永續運作特訂定本規範。

範圍：為確保本公司資訊安全，保障資訊安全維護。

2.【資訊安全風險架構】：

- 由本公司財務行政處副總經理與資訊部門召集成立跨部門資訊安全管理小組，以確認本公司各單位皆落實資訊安全管理辦法，及資訊安全管理運作之有效性。
- 本小組負責制定資訊安全管理政策，定期檢討修正。
- 每年定期向董事會報告執行情形。2022年度已於12月14日提報董事會。

3.【資訊安全政策目標】：

- 確保本公司營運業務持續運作，且本公司提供的資訊服務可穩定使用。
- 確保本公司所保管的資訊資產之機密性、完整性與可用性，並保障人員資料之隱私。
- 建立資訊業務永續運作計畫，執行符合相關法令或法規要求之資訊業務活動運作。
- 所有使用資訊系統之人員，每年接受資訊安全宣導課程，另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。
- 資訊部門主管取得資通安全專業證照清單中的 Certified Ethical Hacker (CEH)，並維持證照的有效性。

4.【資訊安全控制措施】：

本公司實施之資訊安全管理措施，包含如下：

類型	說明	相關作業
人員管理與教育	使用者管理	人員帳號權限管理與審核
	教育訓練	新人報到時進行新人訓
實體與環境安全	電腦機房管理	設定允入清單及進出紀錄
	辦公區域管理	依照行政區與實驗區動線
	辦公桌面管理	依照行政區與實驗區需求
網路安全管理	防火牆管理	密碼長度與密碼生命週期
	伺服器管理	定時連線檢測與更新
	個人電腦管理	每年檢查軟體安裝與抽樣
	軟體下載管理	依照防火牆設定
	電子郵件管理	安裝伺服器更新程式
系統存取控制	資訊系統存取控制	帳號權限申請單
	使用人員存取管理	帳號權限申請單
業務永續運作	業務永續運作規劃	資訊安全管理辦法

5.【運作情形】：

本公司於 111 年 12 月 14 日董事會報告本公司資訊安全管理小組運作情形。