

資通安全管理

資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等：

- 1.資通安全風險管理架構：本公司由資訊部門負責資通安全相關軟、硬體之建置、更新、漏洞之防堵及對使用者進行宣導及教育。
- 2.資通安全政策：公司訂有電子計算機處理循環及資通安全檢查之控制等內部控制程序，俾確保本公司員工有資訊系統安全預防與網路傳輸資料安全之遵循，及危機處理相關事宜之能力。公司定期執行資訊安全稽核作業，檢視存取權限及資訊安全管理制度之落實，確保資訊系統、業務的持續運作正常，以降低相關風險。未來將會視營運規模及需要持續強化資安防護及培訓優質資安人才，建立安全可信賴之電子化作業環境，保障資訊安全。
- 3.具體管理方案及投入資通安全管理之資源：
 - (1)電腦系統安全管理：使用安裝來源合法的防毒軟體，並且定時更新病毒碼，以保持作業系統處於健全的防護程度。
 - (2)網路安全管理：定期變更驗證方式以及使用多種防護作為外，也需隨時保持資安警覺性。
 - (3)系統存取控制：定期檢查存取權限、使用者密碼管理、儲存媒體的保存。
 - (4)系統發展及維護安全管理：定期更新易耗損的硬體設備，備份重要資料，以及安裝備用電源，預防斷電造成的資料損失等。
 - (5)業務永續運作之規劃：評估各種人為及天然災害對公司正常業務運作之影響，以因應緊急狀況及回復作業程序。
- 4.投入資通安全管理之資源量化數據：設置人員總數 2 人，負責資訊安全規劃、管理與監控作業。