資訊安全風險管理架構

本公司因應資訊安全之管理，擬定**『資訊安全規範』**並訂有運作管理計畫(內含實施辦法及施行細則、運作計畫管理及罰則等)，以利網路資訊安全之管理及稽核標準化作業。

考量資安險仍是新興險種，涉及資安等級檢測機構、理賠鑑識機構及不理賠條件等相關配套，因此尚在進行資安險的評估，雖尚未投保資安險，但擬定相關預防措施，持續強化資安防護與建立聯防機制，尤其在培訓優質資安人才，提升專業職能及訂定相關培訓計畫。

本公司由資訊部主管擔任資安負責人，定期評估資訊安全風險，本公司資訊安全評估重點如下： (一)資訊架構檢視、(二)網路活動檢視、(三)網路設備、伺服器及終端機等設備檢測、(四) 網站安全檢測、(五)安全設定檢視、(六) 郵件社交工程演練等作業項目。各項主要評估項目與具體管理方案分述如下：

(一)資訊架構檢視

1.檢視對於持續營運所採取相關措施之妥適性 檢視相關措施之架構與維運機制是否存在單點失效之風險，及針對業務持續運作之妥適性進行風險分析，並提出資訊架構安全評估之結果與建議。

2.檢視單點故障之最大衝擊與風險承擔能力 評估衝擊是否在風險承受度內，若否，研議與執行改善之方案。

(二)網路活動檢視

檢視設備之存取紀錄及帳號權限檢視網路設備、資安設備及伺服器之存取紀錄、帳號權限之授予與監控機制是否符合內控作業規範;以最小權限原則清查該等設備之帳號權限及存取紀錄，識別異常紀錄與確 認警示機制。

(三)網路設備、伺服器及終端機等設備檢測

弱點掃描與修補作業定期或適時辦理網路設備、伺服器及終端機的弱點掃描，並針對所發現之弱點進行改善、修補作業。評估弱點掃描作業之範圍、作業模式及弱點改善計畫與修補情形，針對掃描 結果提出評估建議，重點在於找出架構中可能存在的弱點與漏洞，予以改善及修補，降低整體之資安風險。

(四)網站安全檢測

針對網站進行滲透測試滲透測試分為資料蒐集、資訊分析、目標滲透等三個步驟；執行方式則模擬駭客攻擊行為，利用安全檢測工具(如：Nessus、Nmap、Ixia BreakingPoint)，針對開放外部連結之 網站進行滲透測試，俾利儘早發現網站暴露於外之弱點，並進行修復。

(五)安全設定檢視

伺服器安全性原則設定檢視伺服器(如：網域服務 Active Directory)有關「密碼設定原則」與「帳號鎖定原則」之設定，透過工具分析及人工作業，檢視相關網域安全性原則設定是否符合內控規範。

(六) 郵件社交工程演練

針對資訊作業人員，於內部安全監控範圍內，寄發演練郵件，測試、宣導及強化資通安全教育。主要評估項目為： 1.郵件內容與附件檔案 2.郵件派送時間及方式 3.郵件開啟率及點閱率 4.後續改善機制演練目標主要在於讓同仁瞭解使用電子郵件之風險，提高同仁防範社交 工程攻擊之危機意識，持續演練以降低社交工程攻擊所造成之風險，進而達到保護客戶 資料及重要營運資訊與服務之目的。