附件一

保險業電腦系統資訊安全評估作業原則

壹、前言

為確保保險業提供電腦系統具有一致性基本系統安全防護能力，擬透過各項資訊安全評估作業，發現資安威脅與弱點，藉以實施技術面與管理面相關控制措施，以改善並提升網路與資訊系統安全防護能力，訂定本辦法。

貳、評估範圍

一、 保險業應就整體電腦系統（含自建與委外維運）依據本作業原則建構一套評估計畫，基於持續營運及保障客戶權益，依資訊資產之重要性及影響程度進行分類，定期或分階段辦理資訊安全評估作業，並提交「電腦系統資訊安全評估報告」，辦理矯正預防措施，並定期追蹤檢討。

二、 評估計畫應報董（理）事會或經其授權之經理部門核定，但外國保險業在台分公司，得授權由在中華民國負責人為之。評估計畫至少每三年重新審視一次。

參、電腦系統分類及評估週期

一、 電腦系統依其重要性分為三類：

電腦系統類別	定義	評估週期
第一類	直接提供客戶自動化服務之系統（如網路投保、網路要保等系統）及核心資訊系統	每年至少辦理一次資訊安全評估作業
第二類	存放大量客戶資料之系統 （如檔案伺服器、資料倉儲、客服及行銷等系統）	每三年至少辦理一次資訊安全評估作業
第三類	非核心資訊系統 （如人資、總務等系統）	每五年至少辦理一次資訊安全評估作業

二、 單一系統而為數眾多且財產權歸屬於公司之設備得以抽測方式辦理，抽測比例每次至少應占該系統全部設備之 10%或 100 台以上。

三、 單一系統發生重大資訊安全事件，應於三個月內重新完成資訊安全評估作業。

肆、資訊安全評估作業

一、 資訊安全評估作業項目：

（一）資訊架構檢視

1. 檢視網路架構之配置、資訊設備安全管理規則之妥適性等，以評估可能之風險，採取必要因應措施。
2. 檢視單點故障最大衝擊與風險承擔能力。
3. 檢視對於持續營運所採取相關措施之妥適性。
4. 適時參考金融資安資訊分享與分析中心(F-ISAC)所發布之資安威脅情資及資安防護建議，並採取相關措施。

（二）網路活動檢視

1. 檢視網路設備、伺服器及物聯網設備之存取紀錄及帳號權限，識別異常紀錄與確認警示機制。
2. 檢視資安設備（如：防火牆、入侵偵測或防禦、惡意軟體防護、資料外洩防護、垃圾郵件過濾、網路釣魚偵測、網頁防護等）之監控紀錄，識別異常紀錄與確認警示機制。
3. 檢視網路是否存在異常連線或異常網域名稱解析伺服器(Domain Name System Server，DNS Server)查詢，並比對是否為已知惡意 IP、中繼站或有符合網路惡意行為的特徵。

（三）網路設備、伺服器、終端設備及物聯網設備等設備檢測

1. 辦理網路設備、伺服器、終端設備及物聯網設備等設備的弱點掃描與修補作業。
2. 檢測終端機及伺服器是否存在惡意程式。
3. 檢測系統帳號登入密碼複雜度；檢視外部連接密碼（如檔案傳輸（File Transfer Protocol, FTP）連線、資料庫連線等）之儲存保護機制與存取控制。

（四）網路設備、伺服器及物聯網等設備且連線至 Internet 者應辦理下列事項

1. 進行滲透測試。
2. 進行伺服器應用系統之程式原始碼掃描或黑箱測試。
3. 檢視伺服器目錄及網頁之存取權限。
4. 檢視系統是否有異常的授權連線、CPU 資源異常耗用及異常之資料庫存取行為等情況。

（五）客戶端應用程式檢測

針對保險業交付給客戶之應用程式進行下列檢測：

1. 提供 http, https, FTP 者應進行弱點掃描。
2. 程式原始碼掃描或滲透測試。
3. 敏感性資料保護檢測（如記憶體、儲存媒體）。
4. 金鑰保護檢測。

（六）安全設定檢視

1. 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」設定。
2. 檢視防火牆是否開啟具有安全性風險的通訊埠或非必要通訊埠，連線設定是否有安全性弱點。
3. 檢視系統存取限制(如存取控制清單 Access Control List)及特權帳號管理。
4. 檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新設定及更新狀態。
5. 檢視金鑰之儲存保護機制與存取控制。

（七）資訊系統可靠性與安全性侵害之對策

1. 會員公司應就提升資訊系統可靠性研擬相關對策，其內容包括：

（1） 提升硬體設備之可靠性：包含預防硬體設備故障與備用硬體設備設置之對策。

（2） 提昇軟體系統之可靠性：包含提升軟體開發品質與提升軟體維護品質對策。
（3） 提升營運可靠性之對策。
（4） 故障之早期發現與早期復原對策。
（5） 災變對策。

2. 會員公司應就資訊安全性侵害，研擬相關對策，其內容包括：
（1） 資料保護：包含防止洩漏、防止破壞篡改與相對應檢測之對策。
（2） 防止非法使用：包含存取權限確認、應用範圍限制、防止非法偽造、限制外部網路存取及偵測與因應之對策。
（3） 防止非法程式：包含防禦、偵測與復原對策。

3. 檢視電腦系統是否符合「保險業辦理資訊安全防護自律規範」、「保險業經營電子商務自律規範」、「保險業辦理電子保單簽發作業自律規範」、「保險業經營行動投保業務自律規範」及主管機關相關函文之要求。

4. 如有使用 SWIFT 系統者，需檢視電腦系統之 SWIFT 系統是否符合 SWIFT 公布之 Customer Security Programme 規範及公會相關函文之要求，若與本作業原則衝突，依 SWIFT 公布為主。

二、 第一類電腦系統應依前項辦理資訊安全評估作業，第二類及第三類電腦系統辦理資訊安全評估作業則依系統特性選擇前項必要之評估作業項目。

伍、分散式阻斷服務攻擊(DDoS)演練

辦理電子商務業務者，應訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序，並定期辦理 DDoS 實地演練。

陸、社交工程演練

每年應至少一次針對使用電腦系統人員，於安全監控範圍內，寄發演練郵件，加強資通安全教育，以期防範惡意程式透過社交方式入侵。

柒、評估單位資格與責任

一、 評估單位可委由外部專業機構或由會員公司內部單位進行。如為外部專業機構，該機構應與資安評估標的無利害關係，若為內部單位，應獨立於原電腦系統開發與維護等相關單位。

二、 辦理第一類電腦系統資訊安全評估作業之評估單位應具備下列各款資格條件；辦理第二類及第三類電腦系統資訊安全評估作業者，依評估作業項目需要，具備下列相關資格條件之一：

（一）具備資訊安全管理知識，如持有國際資訊安全經理人(Certified Information Security Manager, CISM）證書或通過國際資安管理系統主導稽核員（Information Security Management System Lead Auditor, ISO 27001 LA）考試合格等。

（二）具備資訊安全技術能力，如國際資訊安全系統專家（Certified Information Systems Security Professional, CISSP）證書等。

（三）具備模擬駭客攻擊能力，如滲透專家（Certified Ethical Hacking, CEH）證書或事件處理專家（Certified Incident Handler, CIH）證書等。

（四）熟悉金融領域載具應用、系統開發或稽核經驗。

三、相關檢視文件、檢測紀錄檔、組態參數、程式原始碼、側錄封包資料等與本案相關之全部資料，評估單位應簽立保密切結書並提供適當保護措施，以防止資料外洩。

四、評估單位及人員不得隱瞞缺失、不實陳述、洩露資料及不當利用等情事。

捌、評估報告

一、「電腦系統資訊安全評估報告」內容應至少包含評估人員資格、評估範圍、評估作業項目與標的、評估紀錄、評估時所發現之缺失項目、缺失嚴重程度、缺失類別、風險說明、具體改善建議及社交演練結果。

二、會員公司應依據評估報告內容缺失程度區分風險等級，並擬定各風險對應之控管措施及處理時限，送稽核單位進行缺失改善事項之追蹤覆查。

三、評估報告缺失覆查應提報董（理）事會或經其授權之經理部門，但外國保險業在台分公司，得由總公司授權之人員為之，以落實由高階管理階層督導缺失改善。

四、評估報告應併同缺失改善等相關文件至少保存五年。