附件二

保險經紀人辦理電腦系統資訊安全評估作業原則

112.9.13 保局(綜)字第 1120431623 號函備查

壹、前言

為確保保險經紀人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、保險經紀人應就整體電腦系統（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，但外國保險經紀人公司在台分公司，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或對營運有重大影響之系統	每年至少辦理一次資訊安全評估作業
第二類	經人工介入以直接或間接提供客戶服務之系統（如客戶服務、保單行政系統等系統）	每三年至少辦理一次資訊安全評估作業
第三類	未接觸客戶資訊或服務且對營運無影響之系統（如人資、財會、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。

四、保險經紀人如有第一類電腦系統，全部核心資通系統至少每二年辦理一次業務持續運作演練。

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)或其他資安廠商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、防毒軟體、資料外洩防護、垃圾郵件過濾、網路釣魚偵測、網頁防護）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，並比對是否有符合網路惡意行為的特徵。

(三)網路設備、伺服器及終端機等設備檢測

1.檢視網路設備、伺服器及終端機的弱點與修補。

2.檢視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)網站安全檢測

1.針對網站進行滲透測試或針對網站及客戶端軟體進行弱點掃描、程式原始碼掃描或黑箱測試。

2.檢視網站目錄及網頁之存取權限。

3.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)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。

（六）存取機制檢視

1.檢視帳號管理:

(1)帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。

(2)已逾期之臨時或緊急帳號應刪除或禁用。

(3)資通系統閒置帳號應禁用。

(4)定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。

2.檢視最小權限：採最小權限原則，僅允許使用者（或代表使用者行為之系統程序）依業務需求取得所需之存取權限。

3.檢視遠端存取:

(1)通過授權檢查後始可放行，並建立相關使用限制、組態需求及連線需求，包含使用者身分類型、來源位址、連線人數上限、網路連線類型、開放時段、允許存取的功能資源及任何先

備條件等限制。
(2)於伺服器端完成使用者之權限檢查作業。
(3)監控遠端存取公司內部網段或資通系統後臺之連線。
(4)採用加密機制建立安全通道。
(5)遠端存取之來源應為公司已預先定義及管理之存取控制點。
（七）事件日誌機制檢視
1.檢視紀錄事件:
(1)訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。
(2)確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。
(3)記錄資通系統管理者帳號所執行之各項功能。
(4)定期審查公司所保留資通系統產生之日誌掌握期間是否曾發生重要資安事件 。
2.檢視日誌紀錄內容應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊。
3.檢視日誌儲存容量：依據日誌儲存需求，配置充足之儲存容量。
4.檢視日誌處理失效之回應
(1)資通系統於日誌處理失效致無法順利產生或留存時，應採取適當之行動。
(2)日誌處理失效事件發生時，資通系統於規定時效內，對特定人員提出告警。
5.檢視時戳及校時
(1)資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
(2)系統內部時鐘應定期與基準時間源進行同步。
6.檢視日誌資訊之保護:
(1)對日誌之存取管理，僅限於有權限之特定人員。
(2)應運用雜湊或其他適當方式確保日誌未遭竄改。
（八）系統備份檢視:
1.訂定可容忍資料損失之時間要求。
2.定期執行系統源碼 含原始程式碼、目的程式等與資料備份。
3.應在與運作系統不同地點之安全處所，儲存備份資料，並定期測試備份資料為可用。
（九）系統備援檢視：
1.訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。
2.應規劃適當的備援機制，於原服務中斷時，由備援設備或其他方式取代並提供服務。
(十)合規檢視
檢視整體電腦系統是否符合本作業原則「伍、資訊系統可靠性與安全性管理對策」之規範。
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、資訊系統可靠性與安全性管理對策
一、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：
（一）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。
（二）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。
（三）提升營運可靠性之對策。
（四）故障之早期發現與早期復原對策。
（五）災變對策

二、會員公司應就資訊安全性侵害研擬相關對策，其內容包括：

（一）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。

（二）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。

（三）防止非法程式：包含防禦、偵測與復原對策。

三、會員公司應就系統與資訊完整性研擬相關對策，其內容包括：

(一)漏洞修復：

1.應定期進行軟體元件漏洞修復與更新，包含作業系統、資通系統伺服器、開發框架，以及第三方函式庫等軟體元件。並於更新前評估可能風險，避免對系統服務造成預期外的影響。

2.應注意安全漏洞訊息(如 F-ISAC 情資或其他資安廠商、CVE 相關網站、廠商安全通告等)，如有資通系統相關漏洞應儘快修復。

(二)資通系統監控：

1.應建立資通安全通報機制，如有發現資通系統有被入侵跡象時，應通報公司特定人員。

2.應建立資通監控機制(如 Web 應用程式防火牆、入侵偵測系統、入侵防禦系統、惡意程式碼防護軟體、掃描工具，日誌監控軟體、網路監控軟體等)，以偵測惡意攻擊與未授權之連線，並發現未經授權之使用行為。

(三)軟體及資訊完整性：

1.應使用適當工具，檢查重要軟體及資訊內容是否被惡意竄改。

2.使用者輸入資料之合法性檢查(如字元集、長度、數值範圍及可接受值等)，應置於應用系統伺服器端 。

3.發現違反完整性時，應進行事件通報、緊急應處及復原等安全保護措施。

四、會員公司應就識別與鑑別研擬相關對策，其內容包括：

（一）資通系統應具有身分驗證機制識別及鑑別公司使用者或代表公司使用者行為之程序之功能，採帳號密碼者，應禁止使用共用帳號。

（二）身分驗證管理：

1.使用預設密碼登入系統時，應於登入後要求立即變更。

2.身分驗證相關資訊不以明文傳輸。

3.具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用公司自建之失敗驗證機制。

4.使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。

5.密碼變更時，至少不可以與前三次使用過之密碼相同。

6.身分驗證機制應防範自動化程式之登入或密碼更換 。

7.密碼重設機制 除 對使用者重新身分確認外應發送一次性及具有時效性符記 Token 。

（三）資通系統應遮蔽輸入過程之鑑別資訊如密碼以*取代 。

（四）資通系統密碼應經加密或雜湊處理後儲存。

五、會員公司應就營運持續研擬相關對策，其內容包括：

（一）系統備份：

1.訂定可容忍資料損失之時間要求 。

2.定期執行系統源碼（含原始程式碼、目的程式等）與資料備份。

3.應在與運作系統不同地點之安全處所，儲存備份資料，並定期測試備份資料為可用。

（二）系統備援：

1.訂定資通系統從中斷後至重新恢復服務之可容忍時訂間要求。

2.應規劃適當的備援機制，於原服務中斷時，由備援設備或其他方式取代並提供服務。

六、會員公司應就系統與服務獲得研擬相關對策，其內容包括：

（一）系統發展前，應先依機密性、完整性、可用性評定所需安全控制措施需求 。
（二）系統開發應避免產生具安全弱點之程式碼 。
（三）定期執行系統主機作業系統及應用程式執行「弱點掃描」安全檢測、「滲透測試」安全檢測，並進行漏洞修補 。
（四）系統相關軟體元件應進行版本更新與漏洞修補並關閉不必要服務及埠口。
（五）資通系統不使用預設密碼。
（六）資通系統開發如委外辦理，應將系統發展生命週期各階段依 系統安全等級所需之防護基準納入委外契約。
（七）開發、測試及正式作業環境應為區隔。
（八）應儲存與管理系統發展生命週期之相關文件。

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，應與提供、維護資安評估標的之機構無利害關係，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或可採用獨立電腦系統（弱點掃描工具、原碼掃描平臺、滲透測試工具、原碼掃、社交工具平臺、惡意程式或防毒軟體檢測平臺…等）輔助進行評估。
二、辦理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：
（一）參加相關資訊安全管理課程訓練達一定時數並取得教育訓練合格證明文件者或具備相關證照者。
（二）熟悉金融領域作業流程或具備相關經驗者。
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

「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，且應送稽核單位進行缺失改善事項之追蹤覆查。該報告應併同缺失改善等相關文件至少保存五年。