# 財產保險業辦理資訊安全防護自律規範

103.1.28 金管保綜字第 10202163711 號函准予備查
104.2.16 金管保綜字第 10402562871 號函准予備查
105.12.2 金管保產字第 10502119220 號函准予備查

第一條

中華民國產物保險商業同業公會（以下簡稱本公會）為督促會員公司(保險局週邊單位除外)資訊業務與相關資訊資產之安全，發揚自律精神，防範資訊處理作業過程發生影響資訊及系統機密性、完整性及可用性之安全事件，確保各會員公司資訊處理作業能安全有效地運作，特訂定本自律規範。

第二條

本自律規範用詞定義如下

一、資訊資產：包含軟體、硬體、環境、文件、通訊、資料、人員等。

二、行動裝置（Mobile device)：亦稱為移動設備、流動裝置或手持裝置（handheld device）等，係指一種可攜帶的計算裝置。
典型的行動裝置如智慧型手機、攜帶型遊樂器與平板電腦、筆記型電腦等。

三、員工攜帶自有設備上班 BYOD（Bring Your Own Device)；指公司政策允許員工可以在公司內使用自己的筆電、手機、平板等行動裝置來連接到公司網路取用資料，或進行公務處理。

第三條

各會員公司辦理資訊安全規範，除應依據各該公司訂立之資安處理程序規定及其應注意事項辦理外，並應依本自律規範辦理。

第四條

各會員公司辦理資訊安全規範，應至少遵循下列規定：

一、應要求所聘任之員工簽署資訊安全保密切結書、雇佣契約、工作手冊，明訂員工應遵守資訊安全保密協定。

二、有委外業務者，應於委外契約中明訂資訊安全保密協定。

三、應透過定期、適當之教育訓練或宣導，告知內部人員應遵循之資訊安全規範。

四、管理階層應督導員工遵循公司既定之資訊安全規範。

五、員工職務異動時，應依既定程序辦理資訊資產退回與存取權限之變更或取消。

六、設備(含行動裝置)報廢前應將機密性、敏感性資料及授權軟體予以移除、實施安全性覆寫或實體破壞，應確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，應簽訂保密合約。

第五條

各會員公司應訂定使用行動裝置（含 BYOD）之相關規範，其內容應至少包含下列項目：

一、行動裝置管理。

二、行動裝置使用人員管理。
三、行動裝置之安全控管。

第六條

各會員公司應訂定使用社群媒體相關規範，其內容應至少包含下列項目：
一、使用社群媒體管理與監督機制。
二、若屬該公司之社群媒體者，應揭露相關資訊，至少包含下列事項：
(1)公司名稱。
(2)主營業場所地址、通訊連絡方式。
三、申訴處理機制。

第七條

各會員公司應訂定使用雲端服務（含私有雲）之相關規範，其內容應至少包含下列項目：
一、雲端服務安全管理。
二、訂定雲端服務提供者遴選機制。
三、雲端服務持續營運管理。

第八條

各會員公司若有建置或開發行動應用程式(App)，需依據財產保險業行動應用程式(App)資訊安全作業準則如附件辦理，以確保行動應用程式(App)安全防護能力，並保障消費者權益。。

第九條

各會員公司若有建置管理系統及有關個資之資安資料，應建立資安防禦機制，並依據產險業辦理電腦系統資訊安全評估作業原則如附件辦理各項資訊安全評估作業，以改善並提升網路與資訊系統安全防護能力。

第十條

各會員公司應加強資訊安全事故管理。
各會員公司應依資訊安全事件通報應變作業實施原則，若發生資訊安全事件時，應依相關規定通報本公會及主管機關，並採取適當處理措施，以控制資安事件影響範圍之擴大。

第十一條

各會員公司應將本自律規範內容，納入內稽內控制度中，並定期辦理自行查核。

第十二條

各會員公司如有違反本自律規範之情事，經本會自律監控委員會查核屬實且違反情節較輕者，得先予書面糾正；如情節較重大者，並經裁處者，提報經本會理事會通過，處以新台幣 5 萬元以上，20 萬元以下之罰款；前述處理情形並應於 1 個月內報主管機關。

第十三條

本規範由中華民國產物保險商業同業公會訂定，經理事會決議通過報主管機關備查後施行，修正時亦同。

附件一

# 財產保險業行動應用程式(App)資訊安全作業準則

第一條　（適用範圍）

一、本準則為本會會員公司中有提供消費者下載行動應用程式者之基本資訊安全準則，各會員公司可依不同應用類別之行動應用程式對於安全性有不同之要求，參酌遵循。

二、會員公司應依個人資料保護法於行動應用程式下載前，明確告知消費者對於個人資料蒐集處理利用之法定事項及消費者得要求刪除資料之權利等事項，以保護消費者權益。

第二條　（行動應用程式發布、更新及問題處理）

一、　應於可信任來源之行動應用程式商店發布，且應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限與所提供之服務用途，並提供版本更新機制。

二、　會員公司應提供回報問題之管道，並於適當期間內回覆。

第三條　（敏感性資料保護）

一、如需蒐集、處理、利用、儲存及分享敏感性資料，應於首次使用前取得使用者同意，並提供使用者拒絕之權利。

二、如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼，並應提醒使用者定期更改通行碼。

三、儲存之敏感性資料，應僅用於其使用聲明之用途，並防止其他應用程式未經授權之存取。

四、透過網路傳輸敏感性資料，應使用適當的安全加密機制。

第四條　（身分認證、授權與連線管理）

一、應有適當之身分認證機制，確認使用者身分，並依使用者身分授權。

二、連線時應避免使用具有規則性之交談識別碼。

三、如需使用伺服器憑證，應確認伺服器憑證之有效性，且為可信任之憑證機構、政府機關或企業之簽發並應避免與未具有效憑證之伺服器，進行連線與傳輸資料。

第五條　（行動應用程式碼安全）

一、應避免含有惡意程式碼，於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌第二條相關規定。

二、行動應用程式上架前
，應建立安控檢測程序。

三、應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。

附錄：用語及定義

1. 行動應用程式（Mobile Application）
   指一種設計給智慧型手機、平板電腦和其他行動裝置使用之應用程式。
2. 行動應用程式商店（Application Store）
   指行動裝置使用者透過內建在裝置中之行動應用程式商店或透過網站對應用程式、音樂、雜誌、書籍、電影、電視節目進行瀏覽、下載或購買。
3. 敏感性資料（Sensitive Data）
   指依使用者行為或行動應用程式之運作，建立或儲存於行動裝置及其附屬儲存媒介之資訊，而該資訊之洩漏有對使用者造成損害之虞，包括但不限於個人資料、通行碼、即時通訊訊息、筆記、備忘錄、通訊錄、地理位置、行事曆、通話紀錄及簡訊。
4. 個人資料（Personal Data）
   指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動、國際行動設備識別碼（International Mobile Equipment Identity, IMEI）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）及其他得以直接或間接方式識別該個人之資料。
5. 通行碼（Password）
   指能讓使用者完全或有限度之使用系統或取得一組資料之識別使用者身分用之字元串，包括但不限於本機儲存資料加密檔案密碼、自身帳號密碼、遠端網路服務帳號密碼。
6. 交談識別碼（Session Identification, Session ID）
   指在建立連線時，指派給該連線之識別碼，並做為連線期間之唯一識別碼；當連線結束時，該識別碼可釋出並重新指派給新之連線。
7. 伺服器憑證（Certificate）
   指載有簽章驗證資料，提供伺服器身分鑑別及資料傳輸加密使用。
8. 憑證機構（Certificate Authority）
   指簽發憑證之機關、法人。
9. 惡意程式碼（Malicious Code）
   指在未經使用者同意之情況下，侵害使用者權益，包括但不限於任何具有惡意特徵或行為之程式碼。
10. 函式庫（Library）
    指將一些繁複或者牽涉到硬體層面之程式包裝成函式（Function）或物件（Object）收集在一起，編譯成二進位碼提供程式設計者使用。
11. 注入攻擊（Code Injection）
    指因行動應用程式設計缺陷而執行使用者所輸入之惡意指令，包括但不限於命令注入（Command Injection）、資料隱碼攻擊（SQL Injection）

附件二

# 「產險業辦理電腦系統資訊安全評估作業原則」

壹、前言

為確保產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、產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） | 每年至少辦理一次資訊安全評估作業 |
| 第二類 | 產險核心資訊系統 | 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、單一系統發生重大資訊安全事件致影響消費者權益，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。

(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、防毒軟體、資料防護等）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、伺服器及終端設備等檢測

1. 辦理網路設備及伺服器的弱點掃描與修補作業。
2. 檢測終端設備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)外部網站安全檢測

1. 針對網站進行滲透測試及弱點掃描。
2. 檢視網站目錄及網頁之存取權限。
3. 檢視網站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。

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、資訊系統可靠性與安全性侵害之對策

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。

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，其資格應符合下列條件之一：

1. 通過國內外學術機構或團體所舉辦有關資訊安全管理知識考試及格取得證書者。
2. 參加國內外學術機構或團體所舉辦有關資訊安全管理知識教育訓練達一定時數並取得教育訓練合格證明文件者。
3. 具相關工作經驗且於金融業工作達一定年資者。

（二）具備資訊安全技術能力，其資格應符合下列條件之一：

1. 通過國內外學術機構或團體所舉辦有關資訊安全技術能力考試及格取得證書者。
2. 參加國內外學術機構或團體所舉辦有關資訊安全技術能力教育訓練達一定時數並取得教育訓練合格證明文件者。
3. 具相關工作經驗且於金融業工作達一定年資者。

（三）具備模擬駭客攻擊能力，其資格應符合下列條件之一：

1. 通過國內外學術機構或團體所舉辦有關模擬駭客攻擊能力考試及格取得證書者。
2. 參加國內外學術機構或團體所舉辦有關模擬駭客攻擊能力教育訓練達一定時數並取得教育訓練合格證明文件者。
3. 具相關工作經驗且於金融業工作達一定年資者。

（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

「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。