「保險代理人公司(含兼營保險代理人業務之銀行)行動裝置應用程式作業原則」

遵奉金融監督管理委員會105年4月8日保局(綜)字第10510906620號函示辦理
遵奉金融監督管理委員會105年10月25日保局(綜)字第10500087180號函示辦理
遵奉金融監督管理委員會保險局106年5月5日保局(綜)字第10602024110號函示辦理
107年2月22日第7屆第5次理監事聯席會議決議
遵奉金融監督管理委員會保險局107年6月5日保局(綜)字第10704139480號備查

壹、前言

為提升保險代理人公司(含兼營保險代理人業務之銀行)於建置或使用行動裝置應用程式基本安全防護能力，透過本作業原則之重點要項，強化資訊安全意識，並逐步完善所提供之行動裝置應用程式安全防護能力。

貳、適用範圍

一、 本作業原則為保險代理人公司(含兼營保險代理人業務之銀行)提供行動應用程式之基本資訊安全準則。

二、 行動裝置應用程式首次使用前，應明確告知使用者個人資料蒐集處理及利用之法定事項。

參、用語及定義

一、 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。

二、 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。

三、 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。

四、 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。

五、 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。

六、 付費資源（Payment Resource）:指透過行動應用程式內建購買功能取得之額外功能、內容及訂閱項目。

七、 交談識別碼（Session Identification, SessionID）: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。

八、 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。

九、 憑證機構（Certificate Authority）:指簽發憑證之機關、法人。

十、 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。

十一、 資訊安全漏洞（Vulnerability）:指行動應用程式安全方面之缺陷，使得系統或行動應用程式資料之保密性、完整性、可用性面臨威脅。

十二、 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。

十三、 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）。

肆、技術要求

一、行動應用程式資訊安全技術要求事項

(一)行動應用程式發布、更新與問題回報

1. 行動應用程式發布:應於可信任來源之行動應用程式商店或網站發布，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用途。
2. 應於發布前檢視行動應用程式所需權限應與提供服務相當，首次發布或權限變動應經負責個人資料保護相關單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務。
3. 行動應用程式更新:應於可信任來源之行動應用程式商店或網站發布更新且提供更新機制，並於有安全性更新時主動公告。
4. 行動應用程式問題回報:開發者應提供回報安全性問題之管道於適當期間內回覆問題並改善。
5. 行動應用程式應於上架前建立資安檢測與評估
   (1)建立行動應用程式資安檢測程序，行動應用程式上架前，應通過資安檢測程序，並針對檢測發現可能影響敏感性資料被竊取或竄改之弱點完成改善。
   (2)行動應用程式之資安評估：行動應用程式依本作業原則伍、安全分類，其屬第三類、具交易功能者，應納入本自律規範(附件一保險代理人公司資訊安全作業控管自律規範之第一類電腦系統，定期辦理評估作業。)
6. 行動應用程式下載、安裝與首次啟動
   (1) 行動應用程式如有涉及敏感性資料蒐集、利用，應於下載、安裝或首次啟動應用程式時明確告知使用者，所涉敏感性資料的使用目的、資料類別、使用方式及刪除方式，並加強資安風險意識之宣導。
   (2) 行動應用程式所要求使用者對其個人敏感性資料蒐集、利用之授權，應與所提供之服務相當。

(二)敏感性資料保護

1. 敏感性資料存取同意：行動應用程式應於蒐集、利用、儲存、傳輸、分享敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
2. 敏感性資料利用:行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼並提醒使用者定期更改通行碼。
3. 敏感性資料儲存:
   (1)應僅用於其使用聲明之用途，並避免將敏感性資料儲存於暫存檔或紀錄檔中。
   (2)應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。
   (3)應避免出現於行動應用程式之程式碼。
4. 敏感性資料傳輸:透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。
5. 敏感性資料分享：行動裝置內之不同行動應用程式間，於分享敏感性資料時，應避免未授權之行動應用程式存取。
6. 敏感性資料刪除：如涉及儲存使用者敏感性資料，應提供使用者刪除之功能。

(三)付費資源控管安全

1. 應於使用付費資源前主動通知使用者，並提供使用者拒絕之權利。
2. 應於使用付費資源前進行使用者認證，並記錄使用之付費資源與時間。

(四)身分認證、授權與連線管理安全

1. 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。
2. 應避免使用具有規則性之交談識別碼。
3. 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，應避免與未具有效憑證之伺服器，進行連線與傳輸資料。

(五)行動應用程式碼安全

1. 防範惡意程式碼與避免資訊安全漏洞：
   (1)行動應用程式應避免惡意程式碼。
   (2)行動應用程式應避免資訊安全漏洞。

2. 行動應用程式完整性：行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性。
3. 函式庫引用安全：行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本。
4. 使用者輸入驗證：行動應用程式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。

二、伺服端資訊安全技術要求事項應依據本會所訂「保險代理人公司辦理電腦系統資訊安全評估作業原則」肆、一、(三)、網路設備、伺服器及終端機等設備檢測辦理。

伍、安全分類

(一)不同類型行動應用程式之資訊安全要求事項進行區分，共分為三類，分別為：

第一類、純功能性:僅提供離線公開資訊檢視功能。

第二類、具認證功能與連網行為:具認證功能與連網行為，能夠執行本機端或伺服器端資料之查詢、新增、修改與刪除。

第三類、具交易功能與客戶個人資料處理（包括認證功能及連網行為）:具認證功能與連網行為，能夠執行交易、將個人資料下載至行動設備端或執行伺服器端客戶資料之查詢、新增、修改與刪除。

(二)針對每一安全分類，定義應符合資訊安全技術要求事項之最小集合，即行動應用程式應符合其所屬分類中之所有資訊安全技術要求事項。各安全分類之資訊安全技術要求事項詳如表 1。

表1 各安全分類之資訊安全技術要求事項：

編號	資訊安全技術要求事項	安全分類		
		一	二	三
1	行動應用程式發布	V	V	V
2	行動應用程式更新	V	V	V
3	行動應用程式安全性問題回報	V	V	V
4	行動應用程式上架資安檢測與評估	V	V	V
5	行動應用程式下載、安裝與首次啟動	V	V	V
6	敏感性資料存取同意		V	V
7	敏感性資料利用		V	V
8	敏感性資料儲存		V	V
9	敏感性資料傳輸		V	V
10	敏感性資料分享		V	V
11	敏感性資料刪除		V	V
12	付費資源使用			V
13	付費資源控管			V
14	使用者身分認證與授權		V	V
15	連線管理機制		V	V
16	防範惡意程式碼與避免資訊安全漏洞	V	V	V
17	行動應用程式完整性			V
18	函式庫引用安全	V	V	V
19	使用者輸入驗證		V	V