本會 105 年 10 月 14 日第 12 屆第 1 次理監事聯席會議核議通過
金管會 106 年 6 月 20 日金管銀國字第 10600142020 號函洽悉
本會 107 年 10 月 25 日第 12 屆第 21 次理監事聯席會議核議通過
金管會 107 年 11 月 20 日金管銀國字第 10701192550 號函洽悉
本會 109 年 3 月 12 日第 13 屆第 5 次理監事聯席會議核議通過
金管會 109 年 4 月 17 日金管銀國字第 1090134543 號函洽悉
本會 113 年 1 月 25 日第 14 屆第 13 次理監事聯席會議核議通過
金管會 113 年 5 月 3 日金管銀國字第 1130209228 號函修正後備查

附件一

金融機構提供行動裝置應用程式作業規範

第一條　中華民國銀行商業同業公會全國聯合會(以下簡稱本會)為確保金融機構提供客戶使用之行動裝置應用程式(以下簡稱應用程式) 之資訊安全，並保障消費者權益，特訂定本規範。

第二條　本規範用詞定義如下：

一、行動裝置：係指包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。

二、Root 與 Jailbreak：係指一種程序，經由此特定程序可取得行動裝置最高權限，藉以突破行動裝置作業系統之基本防護，可能導致遭植入惡意程式，竊取個資、金鑰及停用身分確認機制等。

三、USB debugging：係Android 提供一種用於開發工作之偵錯功能。開啟此功能可能會忽略螢幕保護及人臉辨識、被植入惡意程式等，增加資料外洩風險。

四、白箱加密法(White-box Cryptography；WBC)：係指將應用程式中加密運算之金鑰資訊得以充分被隱藏，降低演算法遭攻擊之機率。

五、程式碼混淆技術：係指將程式碼轉換為相同功能，且難於閱讀與理解之技術。此技術可運用於程式原始碼或編譯後之位元組碼(bytecode)，藉此以提升程式被逆向工程反組譯程式碼後之理解難度。

六、評估單位：係指「金融機構辦理電腦系統資訊安全評估辦法」之評估單位。

七、空中傳輸(Over The Air，OTA)：透過無線傳輸方式，進行軟體、參數、相關資料之下載或更新。

八、安全元件 (Secure Element，SE)：提供各種服務應用所需之安全運算及確保相關資料之隱密性，可用來存載金融卡、信用卡、儲值帳戶或金融機構帳戶等支付工具應用程式與相關資料；此媒介可為不同之形式，如 USIM、外接裝置、手機內建晶片及 MicroSD 等。

九、近距離無線通訊 (Near Field Communication，NFC)：是一種短距離之高頻無線通訊技術，允許電子裝置間進行非接觸式端點對端點資料傳輸。

十、應用伺服器：係指行動裝置應用程式所搭配之行動應用平台伺服器，其提供 Web、API(如 WebService)等存取介面。

第三條　應建立應用程式發布程序，由兩人以上或採用兩項(含)以上技術管控。

第四條　應於發布前檢視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資安、法遵及風控等單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務。

第五條　啟動應用程式時，如偵測行動裝置疑似遭破解(如 root、jailbreak、USB debugging 等)，應提示使用者注意風險並限制辦理電子轉帳及交易指示類之非約定轉帳服務。

第六條　應於顯著位置(如官網、應用程式下載頁面等)提示使用者於行動裝置上安裝防護軟體。

第七條　應於官網上提供應用程式之名稱、版本與下載位置。

第八條　應建立偽冒應用程式偵測、下架或告警機制。

第九條　金融機構每年應辦理下列檢測：

一、由合格實驗室依據行動應用資安聯盟「行動應用 APP 基本資安檢測基準」辦理並通過檢測。

二、針對應用程式及其應用伺服器之完整功能辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞。

三、由評估單位針對應用程式及其應用伺服器依據本作業規範及 OWASP 公布之 Mobile Application Security Checklist L2 項目辦理檢測。

應就前項合格實驗室及評估單位所提交之報告建立檢視機制，並送資安專責單位監控及執行資訊安全管理作業。如前項第二款及第三款因檢測結果與實際應用之解讀存有差異或因故無法修補者，金融機構得由資安專責單位進行評估相關漏洞是否列為可承擔之風險，如屬可承擔風險並留存該風險評估紀錄者，不在此限。OWASP 或「行動應用 App 基本資安檢測基準」要求如與本會規範衝突者，以本會規範為主。

第十條　應用程式及其應用伺服器新功能首次上線、系統架構異動或既有功能異動時應辦理下列檢測：

一、辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞，如屬前條第二項可承擔風險並留存該風險評估紀錄者，不在此限。

二、如與資金轉移相關或對客戶權益有重大影響之各類電子轉帳及交易指示者，依據 OWASP 公布之 Mobile Top 10 項目辦理之檢測，應修正中/高風險漏洞始得上線(或異動)，如因故需緊急上線者，應於一定期限內完成修正，於完成前應有相應之處置作為及控管機制。

第十一條　採用行動裝置儲存金鑰之安全設計，應符合下列要求：

一、應採用下列任一技術保護金鑰：

(一)採用晶片安全設計者，金鑰應儲存於符合我國國家標準 CNS 15408 EAL5、共通準則(Common Criteria)ISO/IEC 15408 v2.3 EAL 5 或 FIPS 140-2 Level 3 以上或其他安全強度相同之安全元件 (SE)內，並能防堵市面上常見之攻擊破解方法。

(二)採用軟體保護技術(如白箱加密法並搭配程式碼混淆技術)並經評估單位確認安全防護。

二、透過金鑰運算(如 OTP、TAC 等)應用於非約定轉入帳戶之轉帳交易，應確認金鑰儲存於客戶指定之行動裝置。

三、應於交易時增設存取控管或人工確認，限制由可信任行動應用程式存取金鑰，以防止遭受惡意程式發動阻斷服務攻擊或執行偽冒交易。

第十二條　採用空中傳輸(OTA)方式下載敏感資料前，應符合下列要求：

一、應確認使用者身分(如密碼)，並採用嚴密的技術防護措施，且能有效防範相關資料被竊取。

二、應確認行動裝置及應用程式之正確性，並進行端點(銀行端)對端點(應用程式)全程加密防護。

第十三條　採用安全元件儲存媒介(SE)作為儲存裝置時，應確認使用者指定之安全元件儲存媒介編號(如 SE ID)、並於 SE 內增設存取控管，限制由可信任應用程式存取。

第十四條　採用近距離無線通訊(NFC)技術進行付款交易資料傳輸前，應經由使用者人工確認（如密碼、圖形驗證碼)。

第十五條　依據金融機構辦理電子銀行業務安全控管作業基準第八條第二款辦理法人客戶高風險交易，採用行動裝置應用程式作為交易再確認機制者，應符合下列安全防護措施：

一、防入侵機制：避免使用疑似遭破解的行動裝置、確保 App 完整性、確保函式庫完整性、防止螢幕遭覆蓋、確保逆向工程無法取得重要機敏資料。

二、執行期間保護機制：防止應用程式被打包或監聽、防止執行未授權程式碼、防止使用螢幕快照或延伸螢幕、防止於模擬器上執行、如偵錯模式應提示使用者注意風險。

三、機敏資料保護機制：保護記憶體參數及儲存檔案、使用設備保護金鑰、防止設備被複製。

第十六條　本規範經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。