農漁會信用部行動支付業務符合「金融機構辦理電子銀行業務安全控管作業基準」有關行動支付業務之安全控管作業自評表

自評日期：___年___月___日

農漁會名稱：

所屬資訊共用中心：

自評依據(請配合申辦行動支付時適用之「金融機構辦理電子銀行業務安全控管作業基準(下稱安控基準)」及「金融機構提供行動裝置應用程式作業規範(下稱作業規範)」，為必要之調整)：

■ 金融監督管理委員會 107 年 3 月 14 日同意備查，中華民國銀行商業同業公會全國聯合會(下稱銀行公會)所修訂之安控基準

■ 金融監督管理委員會 106 年 6 月 20 日同意備查，銀行公會所修訂之作業規範

壹、交易面

安全控管作業項目	本案作法說明	合規性評估
提供網際網路應用系統，應遵循下列必要措施【安控基準第 10 條第 1 款】： 1.載具密碼不應於網際網路上傳輸，機敏資料於網際網路傳輸時應全程加密。 2.應設計連線(Session)控制及網頁逾時(TimeOut)中斷機制，客戶超過 10 分鐘未使用應中斷其連線或採取其他保護措施。 3.應辨識外部網站及其所傳送交易資料之訊息來源及交易資料正確性。 4.應辨識客戶輸入與系統接收之非約轉交易指示一致性，若採用經銀行公會審核之確認型讀卡機或載具並可人工確認交易內容者，得不執行本措施。 5.應設計於客戶進行身分確認與交易機制時，如需使用亂數函數進行運算，須採用安全亂數函數產生所需亂		□符合 □不符合 □不適用

安全控管作業項目	本案作法說明	合規性評估
數。 6.應避免存在網頁程式安全漏洞(如 Injection、Cross-Site Scripting 等)。 7.應偵測網頁與程式異動時，進行紀錄與通知措施。 8.採用固定密碼進行身分確認登入個人網路銀行者，應加強安全機制，如於登入成功及失敗均及時通知客戶、採用人工確認(如圖形驗證碼)進行登入或登入身分確認資料採逐步驗證等機制。		
提供使用者端程式，應遵循下列必要措施【安控基準第 10 條第 2 款】: 1.應採用被作業系統認可之數位憑證進行程式碼簽章(CodeSign)。 2.執行時應先驗證網站正確性。 3.應避免儲存機敏資料，如有必要應採取加密或亂碼化等相關機制保護並妥善保護加密金鑰，且能有效防範相關資料被竊取。 4.於低風險非約定轉入帳戶轉帳或高風險交易時，須於客戶端經由人工確認(如插拔卡、特殊按鍵等)交易內容後才完成交易；或於交易過程增加額外具「兩項以上技術」之介面設計認證機制，若採用經銀行公會審核之確認型讀卡機或載具並可人工確認交易內容者，得不執本措施。		□符合 □不符合 □不適用
提供行動裝置應用系統，應遵循「金融機構提供行動裝置應用程式作業規範」。【安控基準第 10 條第 3 款】 **作業規範：** 1.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。 2.應於發布前檢視應用程式所需權		□符合 □不符合 □不適用

安全控管作業項目	本案作法說明	合規性評估
限應與提供服務相當，首次發布或權限變動應綜合評估是否符合「個人資料保護法」之告知義務。 3.應參照經濟部「行動應用 APP 基本資安自主檢測推動制度」每年委由專業機構完成安全檢測。 4.啟動應用程式時，如偵測行動裝置疑似遭破解，應提示使用者注意風險。 5.應於顯著位置(如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。 6.應於官網上提供應用程式之名稱、版本與下載位置。 7.應建立偽冒應用程式偵測機制，以維客戶權益。 8.採用憑證技術進行傳輸加密時，應用程式應建立可信任憑證清單並驗證完整憑證鏈及其憑證有效性。 9.採用行動裝置儲存金鑰之安全設計，應符合下列要求： (1)應採用下列任一技術保護金鑰： A.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 2 (含)以上或其他安全強度相同之安全儲存媒介(SE)內，並能防堵市面上常見之攻擊破解方法。 B.採用軟體保護技術(如白箱加密法並搭配程式碼混淆技術)並經評估機構確認安全防護。 (2)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		

安全控管作業項目	本案作法說明	合規性評估
行動裝置。 10.採用空中傳輸(OTA)方式下載敏感資料前，應符合下列要求： (1)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。 (2)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。 11.採用安全儲存媒介(SE)作為儲存裝置時，應確認使用者指定之安全儲存媒介編號(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。 12.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)。		
訊息傳輸之安全設計--訊息隱密性--1.訊息處理【安控基準第 6 條】 可採對稱性加解密系統或非對稱性加解密系統。 1.對稱性加解密系統其應至少採用金鑰有效長度為 112 位元以上之三重資料加密演算法(Triple DES)或金鑰有效長度為128位元以上之進階資料加密演算法(AES)或其他安全強度相同之演算法。 2.非對稱性加解密系統其應至少採用金鑰長度為2048位元以上之RSA演算法或金鑰長度為 256 位元以上之橢圓曲線演算法(Elliptic curve cryptography，ECC)或其他安全強度相同之演算法。 3.須全文加密。		□符合 □不符合 □不適用

安全控管作業項目	本案作法說明	合規性評估
訊息傳輸之安全設計--訊息隱密性--2.金鑰交換【安控基準第 6 條】 採對稱性加解密系統時，其金鑰交換可分訊息加密金鑰與金鑰保護金鑰之交換。 1.訊息加密金鑰交換：訊息加密金鑰乃用來對訊息做加密，不應以明碼或人工方式直接交換此金鑰，應使用對稱性加解密系統(如 DES)或非對稱性加解密系統(如 RSA)或依協商訊息加密金鑰(如採 Diffie-Hellman Key Agreement)交換之。安全強度同前述「訊息隱密性」有關訊息處理 1 及 2 之規定。 2.金鑰保護金鑰交換：金鑰保護金鑰乃用來對訊息加密金鑰做加密(如採 DES、RSA)或依此協商訊息加密金鑰(如採 Diffie-Hellman Key Agreement)。 (1)對稱性金鑰保護金鑰之交換應採離線交換(如以碼單或寫入具安全防護之媒體)，以降低該金鑰洩漏之風險；當採碼單交換時，應將金鑰拆分成兩個以上，利用秘密分持(如分 A、B 碼)進行交換；當採媒體交換時，應將媒體及保護機制(如密碼)分持進行交換。 (2)非對稱性金鑰保護金鑰之交換，其公開金鑰可透過憑證或其他通道交換，惟透過非信賴之通道交換應輔以其他可信賴之驗證機制，以確保所取得公開金鑰之正確性。		□符合 □不符合 □不適用
訊息傳輸之安全設計--訊息隱密性--3.金鑰生命週期【安控基準第 6 條】 金鑰應於使用一段期間後更換之，以確保其安全性。		□符合 □不符合 □不適用
訊息傳輸之安全設計--訊息完整性【安控基準第 6 條】		□符合 □不符合

安全控管作業項目	本案作法說明	合規性評估
1.訊息處理：可採訊息鑑別系統、對稱性加解密系統或非對稱性加解密系統。 (1)訊息鑑別系統應採用 160 位元以上之 SHA 演算法、採用 64 位元以上之 DAA 運算或其他安全強度相同之演算法。 (2)對稱性加解密系統同前述「訊息隱密性」有關訊息處理之對稱性加解密系統規範。 (3)非對稱性加解密系統同前述「訊息隱密性」有關訊息處理之非對稱性加解密系統規範。 2.金鑰交換：同前述「訊息隱密性」有關金鑰交換之規範。 3.金鑰生命週期：同前述「訊息隱密性」有關金鑰生命週期之規範。		□不適用
訊息傳輸之安全設計--訊息來源辨識【安控基準第 6 條】 1.訊息處理：同前述「訊息完整性」有關訊息處理之規範。 2.金鑰交換：同前述「訊息隱密性」有關金鑰交換之規範。 3.金鑰生命週期：同前述「訊息隱密性」有關金鑰生命週期之規範。		□符合 □不符合 □不適用
訊息傳輸之安全設計--訊息不可重複性【安控基準第 6 條】 如使用序號、一次性亂數、時間戳記等機制。		□符合 □不符合 □不適用
訊息傳輸之安全設計--無法否認傳送訊息及無法否認接受訊息【安控基準第 6 條】 1.訊息處理：須針對交易訊息使用數位簽章(Digital Signature)或採用其他訊息簽章認證等機制，同前述「訊息隱密性」有關訊息處理之非對稱性加		□符合 □不符合 □不適用

安全控管作業項目	本案作法說明	合規性評估
解密系統規範。 2.公開金鑰交換：訊息簽章使用對應之公開金鑰須透過憑證交換，且此憑證須由憑證機構所核發。 3.金鑰生命週期：同前述「訊息隱密性」有關金鑰生命週期之規範。		
交易訊息之安全限制—行動裝置之安全規定【安控基準第 9 條第 7 款第 1 目】 採用行動裝置儲存金鑰之安全設計 1.應採用下列任一技術保護金鑰： (1)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。 (2)採用軟體保護技術(如白箱加密法並搭配程式碼混淆技術)。 (3)經第三方機構確認其安全防護。		□符合 □不符合 □不適用
交易訊息之安全限制—行動裝置之安全規定【安控基準第 9 條第 7 款第 2 目及第 3 目】 採用行動裝置儲存金鑰之安全設計 2.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。 3.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，以防止遭受惡意程式發動阻斷服務攻擊或偽冒交易。		□符合 □不符合 □不適用

貳、管理面

安全控管作業項目	本案作法說明	合規性評估
建立安全防護策略【安控基準第 11 條第 2 款】 應以下列方式處理及管控： 1.系統應依據網路服務需要區分網際網路、非武裝區(Demilitarized Zone；以下簡稱 DMZ)、營運環境及其他(如內部辦公區)等區域，並使用防火牆進行彼此間之存取控管。機敏資料僅能存放於安全的網路區域，不得存放於網際網路及 DMZ 等區域。對外網際網路服務僅能透過 DMZ 進行，再由 DMZ 連線至其他網路區域。 2.應檢視防火牆及具存取控制(Access control list，ACL)網路設備之設定，至少每年一次；針對高風險設定及六個月內無流量之防火牆規則應評估其必要性與風險；針對已下線系統應停用防火牆規則。 3.應建立入侵偵測或入侵防禦機制並定期更新惡意程式行為特徵。 4.應建立病毒偵測機制並定期更新病毒碼。 5.應建立上網管制措施，限制連結非業務相關網站，以避免下載惡意程式。 網際網路應用系統應以下列方式處理及管控： 1.應偵測網頁與程式異動，紀錄並通知相關人員處理。 2.應偵測惡意網站連結並定期更新惡意網站清單。 得以下列方式處理及管控： 1.建置安全防護軟硬體。(如：安控軟體、偵測軟體等) 2.設計存取權控制(Access Control)如使用密碼、身分證字號、磁卡、IC 卡		□符合 □不符合 □不適用

安全控管作業項目	本案作法說明	合規性評估
等。 3.簽入(Login)時間控制。 4.單次簽入(Single-Sign-on)。 5.撥接控制(Dial-up Control)。 6.專線(Lease-Line)使用。 7.記錄客戶查詢電話。 8.控制密碼錯誤次數。 9.電腦系統密碼檔加密。 10.留存交易紀錄(Transaction Log)及稽核追蹤紀錄(Audit Trail)；針對網際網路應用系統應將其作業系統、網路設備及資安設備之日誌及稽核軌跡集中管理，進行異常紀錄分析，設定合適告警指標並定期檢討修訂。 11.分級。 12.業務面控制如約定帳戶、限定金額等。 13.系統提供各項服務功能時，應確保個人資料保護措施。		
提高系統可靠性之措施【安控基準第 11 條第 2 款】 應以下列方式處理及管控： 1.應避免採用已停止弱點修補或更新之系統軟體與應用軟體，如有必要應採用必要防護措施。 2.定期更換提供給操作者之應用軟體及作業系統密碼。 3.系統應設計個人資料檔案及資料庫之存取控制與保護監控措施。 4.系統應將重要參數檔加密防護。(如：電腦系統密碼檔)。 網際網路應用系統應以下列方式處理及管控：		□符合 □不符合 □不適用

安全控管作業項目	本案作法說明	合規性評估
1.應避免於營運環境安裝程式原始碼。 2.應建立回存測試機制，以驗證備份之完整性及儲存環境的適當性。 3.應建立系統安全強化標準，並落實系統安全設定。 4.每季應進行弱點掃描，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果與處理情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式。 5.系統僅得開啟必要之服務及程式，客戶僅能存取已被授權使用之網路及網路服務。內部網址及網路架構等資訊，未經授權不得對外揭露。 6.系統首次上線前及每半年應針對異動程式進行程式碼掃描或黑箱測試，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，執行矯正、紀錄處理情形並追蹤改善。 7.使用遠端連線進行系統管理作業時，應使用足夠強度之加密通訊協定，並不得將通行碼紀錄於工具軟體內。 8.應建立 DDoS 攻擊監控與事故應變機制，並每年進行程序演練。 得以下列方式處理及管控： 1.建立備援及故障預防措施： (1)預備主機、伺服器、通訊設備、線路、週邊設備等備援裝置。 (2)放置網路伺服器於上鎖密室中。		
制定作業管理規範【安控基準第 11 條第 2 款】 1.制定安全控管規章含設備規格、安控機制說明、安控程序說明等。		□符合 □不符合 □不適用

安全控管作業項目	本案作法說明	合規性評估
2.編寫客戶端之操作手冊及制訂完整契約，應於 eATM 交易畫面揭示使用 eATM 金融交易之風險。		

參、支付工具面

安全控管作業項目	本案作法說明	合規性評估
建立安全防護策略【安控基準第 13 條第 2 款】 卡片之安全設計： 1.運用晶片之運算技術，每次交易均由晶片內部自動產生一組唯一之交易驗證碼(TAC)作為驗證每筆交易之不可否認性，用以確保交易安全。 2.發行多功能卡片(兩種以上功能)，其連線(on-line)金融交易至少應符合上述安全措施，俾達到由發卡金融機構端至客戶端安全。		□符合 □不符合 □不適用
提高系統可靠性之措施【安控基準第 13 條第 1 款】 1.晶片金融卡之發卡及相關軟硬體安全應至少符合「晶片金融卡規格安控等級」。 2.使用各種晶片端末設備，均應經銀行公會晶片端末驗證小組測試通過，確保系統運作之互通性及可靠性。 3.應確保卡片端點對端點之交易安全。		□符合 □不符合 □不適用
制定作業管理規範【安控基準第 13 條第 2 款】 1.編寫客戶實體卡片之操作指示手冊，並制訂完整合約述明客戶及金融機構之權利義務關係。 2.制定「金融機構晶片金融卡交貨流程」與「安全模組控管作業原則」，除管制外包製卡作業外亦落實實體卡片之安全控管。		□符合 □不符合 □不適用

_____資訊共用中心（請蓋印信）：

負責人：