農漁會信用部行動支付業務符合「金融機構辦理行動金融卡安全控管作業規範」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「金融機構辦理行動金融卡安全控管作業規範(下稱作業規範)」及「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)」，為必要之調整)：

- ■ 金融監督管理委員會 106 年 12 月 29 日同意備查，由中華民國銀行商業同業公會全國聯合會所訂定之作業規範
- ■ 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所修訂之安控基準

安全控管作業項目	本案作法說明	合規性評估
線上申辦及空中傳輸作業要求【作業規範第 3 條規定】 1. 發卡對象限已申請實體金融卡之開立第一類、第二類數位存款帳戶或非數位存款帳戶者。 2. 第一類行動金融卡： (1)線上申辦應依據安控基準第 7 條第 1 款至第 4 款任一款安全設計進行身分確認。若以行動電話門號 OTP 驗證，設定該門號應採兩項以上技術機制。 安控基準第 7 條第 1 款至第 4 款身分確認方式 1. 使用憑證簽章得應用於高風險交易，其安全設計應簽署適當內容並確認該憑證之合法性、正確性、有效性、保證等級及用途限制。 2. 使用晶片金融卡僅限應用於低風險交易，其安全設計應符合晶片金融卡交易驗證碼之安全設計。 3. 使用一次性密碼（One Time Password，OTP）僅限應用於低風險交		□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
易，其安全設計係運用動態密碼產生器（Key Token）、晶片金融卡或以其他方式運用 OTP 原理，產生限定一次使用之密碼者。 4.使用「兩項以上技術」僅限應用於低風險交易，其安全設計應具有下列三項之任兩項以上技術： (1)客戶與金融機構所約定之資訊，且無第三人知悉（如密碼、圖形鎖、手勢等）。 (2)客戶所持有之設備，金融機構應確認該設備為客戶與金融機構所約定持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等）。 (3)客戶提供給金融機構其所擁有之生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），金融機構應直接或間接驗證該生物特徵。間接驗證係指由客戶端設備（如行動裝置）驗證或委由第三方驗證，金融機構僅讀取驗證結果，必要時應增加驗證來源辨識。		
(2)第一類行動金融卡可應用於安控基準第 4 條低風險之第 2、4、5、7、10 項，其限額要求如下，應用於非約定轉帳交易時，每筆最高限額為 3 萬元、每日累計最高限額為 3 萬元、每月累計最高限額為 10 萬元；應用於提款交易時，每筆最高限額為 2 萬元、每日累計最高限額為 2 萬元、每月累計最高限額為 2 萬元。 安控基準第 4 條低風險交易： 2.辦理 ATM 存提款之服務。 4.辦理約定轉入帳戶之轉帳。 5.辦理客戶直接向金融機構或間接透過金融資訊服務事業、票據交換所等平台，進行概括約定繳稅費及限定性繳款之扣款約定及扣款服務。 7.同一統一編號帳戶間轉帳。 10.非約定轉入帳戶 (1)ATM、POS 等之低風險性交易，其限額應符合現行 ATM 作業及 POS 作業相		

安全控管作業項目	本案作法說明	合規性評估
關規定。 (2)網際網路之低風險性交易，以每一帳戶每筆不超過等值新臺幣五萬元、每天累積不超過等值新臺幣十萬元、每月累積不超過等值新臺幣二十萬元為限。 (3)透過網站、行動 APP、電子郵件、傳真、FTP 或 AP2AP 等方式傳送且未經金融機構人工確認客戶身分與指示內容者，其交易限額同（2）要求。 (4)配合採用各種嚴密之技術防護措施（如簡訊簡碼回傳），提供客戶確認交易內容並能防止身分確認資料與交易內容被竄改者，其非約定轉入帳戶之轉帳限額，可由個別金融機構視其風險承擔之能力斟酌予以適當提高，最高不超過當日累計等值新臺幣二佰萬元為限；若經客戶事先申請且由金融機構人工與客戶確認其指定人員之身分與指示內容者(如電話照會)，其交易限額不在此限。 3.第二類行動金融卡： (1)線上申辦應依據安控基準第 7 條第 1 款至第 7 款之任一款安全設計進行身分確認。 安控基準第 7 條第 5 款至第 7 款身分確認方式 5.使用視訊會議僅限應用於低風險交易，其安全設計應查驗本人並核對證件照片。 6.使用知識詢問僅限應用於低風險交易且應用範圍應符合第 9 條第 6 款之要求；其安全設計應利用客戶之其他資訊(如保單資訊、信用卡申請資料或繳款方式等)，以利有效識別客戶身分。 7.使用固定密碼僅限應用於低風險交易且應用範圍應符合第 9 條第 6 款之要求； (1)透過網際網路傳輸途徑並採用戶代號及固定密碼進行唯一驗證之簽入介面，其安全設計應具備之安全設計原則如下： A.用戶代號之安全設計： (A)不得使用客戶之顯性資料(如統一編號、身分證號、手機號碼、電子郵件		

安全控管作業項目	本案作法說明	合規性評估
帳號、信用卡號、存款帳號等）作為唯一之識別，否則應另行增設使用者代號以資識別。 (B)不應少於 6 位。 (C)不應訂為相同之英數字、連續英文字或連號數字。 (D)同一用戶代號在同一時間內僅能登入一個連線(session)控制之系統。 (E)如增設使用者代號，至少應依下列方式辦理： ■ 不得為金融機構已知之客戶顯性資料。 ■ 如輸入錯誤達五次，金融機構應做妥善處理。 ■ 新建立時不得相同於用戶代號及密碼；變更時，亦同。 B.固定密碼之安全設計： (A)不應少於 6 位，若搭配交易密碼使用則不應少於 4 位且交易密碼應符合本目相關規定。 (B)建議採英數字混合使用，且宜包含大小寫英文字母或符號。 (C)不應訂為相同之英數字、連續英文字或連號數字，預設密碼不在此限。 (D)不應與用戶代號、使用者代號、交易密碼相同。 (E)密碼連續錯誤達 5 次，不得再繼續執行交易。 (F)變更密碼不得與前一次相同。 (G)首次登入時，應強制變更預設密碼；若未於 30 日內變更預設密碼者，則不得再以該預設密碼執行簽入。 (H)密碼超過一年未變更，金融機構應做妥善處理。 (I)密碼於儲存時應先進行不可逆運算（如雜湊演算法），另為防止透過預先產製雜湊值推測密碼，可進行加密保護或加入不可得知的資料運算；採用加密演算法者，其金鑰應儲存於經第三方認證（如 FIPS 140-2 Level 3 以上）之硬體安全模組內並限制明文匯出功能。 (2)透過公眾交換電話網路傳輸途徑並採用戶代號及固定密碼進行唯一驗證之簽入介面，其安全設計應符合第一目網際網路有關用戶代號之（B）、（C）及固定密碼之安全設計，惟密碼長度不應少於 4 位。		

安全控管作業項目	本案作法說明	合規性評估
(2)第二類行動金融卡僅可應用於消費交易。 4.金融卡消費額度應由金融機構訂定，其風險控管機制應將行動金融卡併入管理。 5.應控管每一存款帳戶申請之行動金融卡數量。 6.執行金融卡個人化作業時，於處理或傳輸金融卡個人化資料後，不得留存製卡個人化資料。 7.個人化資料在空中傳輸過程，應符合安控基準第5條訊息隱密性及訊息完整性之安全需求。 8.下載個人化資料前，應確認使用之行動裝置或安全儲存媒介，為申請人申辦時指定之行動裝置或安全儲存媒介。 9.行動金融卡下載後，應以原留存發卡行之通訊管道（如簡訊或電子郵件）或雙方約定方式通知申請人。		
<u>執行亂碼化作業控管要求</u>【作業規範第4條規定】 1.伺服器端若儲存或處理交易主金鑰，應採用硬體安全模組（HSM，Hardware Security Module）處理加解密相關作業，且該設備應通過FIPS 140-2 Level 3以上或其他相同安全強度之認證。 2.有關對稱性金鑰，應依金鑰之用途及不同之通信單位，建立各自之獨立金鑰，避免不同用途或不同單位共用相同之金鑰。 3.金鑰之使用、儲存、備份、傳送與銷毀，應確保其內容不以任何形式洩露。 4.保存金鑰之設備或媒體，於更新或報廢時，應具適當之存取控管程序，以		□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
確保金鑰無洩露之虞。 5.金鑰交換應符合安控基準第5條訊息隱密性及訊息完整性之安全需求【註】。		
<u>行動裝置端之金鑰管理作業控管要求</u> 【作業規範第5條規定】 1.金鑰採硬體保護技術且應用於第一類行動金融卡時，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、FIPS 140-2 Level 3 以上或其他相同安全強度之安全元件（SE）內，並能防堵市面上常見之攻擊破解方法。若應用於第二類行動金融卡時，金鑰應儲存於符合 EMVCo Security Evaluation Process 或其他相同安全強度之安全元件內，並能防堵市面上常見之攻擊破解方法。 2.金鑰採軟體保護技術時，應符合下列控管要求： (1)第一類行動金融卡採遠端交易與近端交易應使用不同的金鑰或採不同演算法。 (2)行動裝置所存放之交易金鑰，一次可存放多把，並限制每把金鑰可使用次數。 (3)交易金鑰更新時，系統應比對確認為客戶與金融機構所約定持有之行動裝置，如發現異常，應進行監控。 (4)交易金鑰使用時，應於使用者裝置端進行驗證（如密碼、指紋）。 (5)交易金鑰更新時，行動裝置與伺服器端應通過雙向確認且相關資料的傳輸過程應符合安控基準第 5 條訊息隱密性及訊息完整性之安全需求【註】。 (6)第一類行動金融卡遠端交易所使用		□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
的交易金鑰之控管機制應較近端交易更為嚴謹（如減少每次下載的金鑰數量或縮短效期等）。		
<u>應用系統控管要求</u>【作業規範第6條規定】 1. 應設定可容忍交易錯誤次數之邊界值，應對此邊界值建立相關警示監控機制。 2. 當使用者驗證錯誤累積錯誤次數達設定之邊界值時，必須暫時停止該卡片之使用。 3. 於交易驗證時，交易驗證碼之交易序號應大於前次留存的交易序號。		□符合 □不符合 □不適用

【註】安控基準第5條訊息隱密性及訊息完整性之安全需求

訊息傳輸途徑	專屬網路			網際網路及公眾交換電話網路		
交易類別 / 防護措施	電子轉帳及交易指示類		非電子轉帳及交易指示類	電子轉帳及交易指示類		非電子轉帳及交易指示類
	高風險	低風險		高風險	低風險	
訊息隱密性	非必要	非必要	非必要	必要	網際網路：必要 公眾交換電話網路：備註二	網際網路：必要 公眾交換電話網路：備註一
訊息完整性	必要	必要	非必要	必要	網際網路：必要 公眾交換電話網路：備註三	非必要

備註一：透過網際網路傳送非電子轉帳及交易指示類之足以識別該個人之資料訊息時，應具備訊息隱密性之防護措施；透過公眾交換電話網路（如語音、傳真）時，因此網路之特性無須符合訊息隱密性之安全需求。

備註二：透過公眾交換電話網路（如語音、傳真）時，因此網路之特性無須符合訊息隱密性之安全需求，惟若以雙音多頻訊號傳送固定密碼者，應以干擾訊號或其他機制防止該頻率遭側錄。

備註三：透過公眾交換電話網路（如語音、傳真）時，因此網路之特性不易透過各項演算法驗證訊息完整性，應採用其他方式告知使用者並進行交易內容確認（如雙向簡訊、語音播報再確認）。

_____資訊共用中心（請蓋印信）：

負責人：