農漁會信用部電子銀行業務符合「金融機構辦理電子銀行業務安全控管作業基準」自評表

自評日期：___年___月___日

自評依據(請配合檢視時適用之「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)」，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

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，若採用經中華民國銀行商業同業公會全國聯合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。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
<u>提供使用者端程式，應遵循下列必要措施</u>【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，若採用經中華民國銀行商業同業公會全國聯合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，預計完成改善時間：__年__月__日 □不適用
<u>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」</u>。【安控基準第 10 條第 3 款】 **<u>金融機構提供行動裝置應用程式作業規範：</u>** 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		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
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。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
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。		
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,預計完成改善時間：__年__月__日 □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,預計完成改善時間：__年__月__日 □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--訊息完整性【安控基準第 6 條】 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。		□符合 □不符合，預計完成改善時間：__年__月__日 □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，預計完成改善時間：__年__月__日 □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，預計完成改善時間：__年__月__日 □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		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
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。		
<u>交易面之介面安全設計</u>【安控基準第 7 條第 1 款至第 3 款】 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。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
<u>交易面之介面安全設計</u>【安控基準第 7 條第 4 款】 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。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
<u>交易面之介面安全設計</u>【安控基準第 7 條第 5 款至第 7 款】 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		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
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 5 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。		

安全控管作業項目	本案作法說明	合規性評估
(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 1 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 1 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，其安全設計應符合前開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。		
<u>交易面之介面安全設計</u>【安控基準第 7 條第 8 款及第 9 款】 8.採用存款帳戶進行身分確認者，僅限應用於辦理開立數位存款帳戶或申請信用卡，其安全設計應確認申請人與該帳戶持有人為同一統一編號且係透過臨櫃方式開立，以確認該帳戶之有效性(如透過財金公司之跨行金融帳戶資訊核驗平台進行驗證)；辦理開立數位存款帳戶者並應依「銀行受理客戶以網路方式開立數位存款帳戶作業範本」之規定辦理。辦理申請信用卡者另應增加第 7 條第 1 款至第 5 款之任一款安全設計。 9.採用信用卡進行身分確認者，僅限應用於辦理開立數位存款帳戶或申請信用卡，其安全設計應確認申請人與信用卡持卡人為同一統一編號且係透過信用卡授權交易方式，確認該卡片之有效性(如預授權)；辦理開立數位存款帳戶者並應依「銀行受理客戶以網路方式開立數位存款帳戶作業範本」之規定辦理。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
交易面之介面安全設計【安控基準第 7 條第 10 款】 10.委由第三方進行身分確認者僅限應用於低風險交易，其驗證方式應符合上述安全規定並與第三方以契約約定雙方權利義務關係及賠償責任。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
交易類別之安全設計【安控基準第 8 條第 1 款】 1.「非電子轉帳及交易指示類」中「帳務類查詢」及「個人資料查詢」之限制 (1)應採用第 7 條第 1 款至第 3 款之任一款、第 7 條第 4 款之任一項技術、第 7 條第 5 款至第 7 款或第 7 條第 10 款之任一款安全設計進行身分確認(如簽入作業)。 (2)若涉及第三方居間代理者除以契約約定者外，金融機構與第三方之間其安全機制應具備「訊息來源辨識」之基本防護措施。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
交易類別之安全設計【安控基準第 8 條第 2 款第 1 目及第 2 目】 2.「電子轉帳及交易指示類」之安全設計 (1)應採用第 7 條第 1 款至第 10 款之任一款安全設計進行身分確認。 (2)辦理「限定性繳稅費」應遵循下列要求： A.以本人帳戶繳納本人帳單者，其交易指示雖未經客戶事先約定轉出帳戶，但因其轉入帳戶已限定為個別金融機構與個別事業單位事先以契約約定規範之，故金融機構得不使用第 7 條介面之安全設計；惟金融機構得斟酌透過帳務異動通知，達成客戶事後覆核，以提高其安全控管層次。 B.進行消費扣款之入帳帳戶，金融機構應事先與事業單位進行約定。 C.客戶辦理事業單位或金融機構發動交易指示之扣款約定時，扣款金融機構應採用第 7 條第 1 款至第 4 款之任一款安全設計進行客戶身分確認。 D.金融機構接受事業單位或其他金融機構發		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
動扣款約定或交易指示時，應符合第 5 條交易面之安全需求。 （詳如下表）		

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
訊息來源辨識	必要	非必要	非必要	必要	非必要	非必要
訊息不可重複	必要	必要	非必要	必要	必要	非必要
無法否認傳送	必要	非必要	非必要	必要	非必要	非必要
無法否認接受	必要	非必要	非必要	必要	非必要	非必要

【表格說明】

- 必要（Mandatory）：係指金融機構必須具備該項防護措施。
- 非必要（Conditional）：係指金融機構得視情況自行決定是否需要具備該項防護措施。

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）。

E.客戶向事業單位或金融機構終止扣款約定後，無需承擔遭冒用之損失，金融機構或事業單位應於 14 日內返還帳款，客戶應配合協助後續調查作業。

交易類別之安全設計【安控基準第 8 條第 2 款第 3 目】 2.「電子轉帳及交易指示類」之安全設計 (3)辦理授信業務應採用第 7 條第 1 款至第 7 款之任一款安全設計，但辦理下列業務，應遵循下列要求：		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
A.辦理本會新戶但為他金融機構既有非數位存款、貸款或信用卡客戶，同意金融機構查詢聯徵中心信用資料（申請階段），應採用下列任一方式之安全設計： (A)採用第7條第1款憑證簽章之安全設計。 (B)採用第7條第5款視訊會議，上傳身分證影像檔，並搭配第7條第2款非數位存款帳戶晶片金融卡之安全設計。 B.辦理本會既有數位存款帳戶之貸款契約成立，應採用下列任一方式之安全設計： (A)本會既有第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶者，應採用第7條第1款至第7款之任一款安全設計方式辦理簽約對保。 (B)本會既有第一類適用低風險交易之數位存款帳戶，應採用第7條第1款之硬體憑證簽章及第7條第5款視訊會議之方式辦理簽約對保。 (C)本會既有第三類數位存款帳戶，如採第7條第5款視訊會議辦理簽約對保者，限將款項撥入本人非數位存款帳戶，如採用第7條第1款之硬體憑證簽章，得撥入本人存款帳戶。 C.辦理本會既有信用卡客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計： (A)採用第7條第1款憑證簽章及第7條第5款視訊會議。 (B)採用第7條第3款一次性密碼，得將款項撥入本人非數位存款帳戶、第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶。 (C)採用第7條第3款一次性密碼及第7條第5款視訊會議，得將款項撥入本人第一類適用低風險交易之數位存款帳戶及第三類數位存款帳戶。 (D)依「長期使用循環信用持卡人轉換機制」		

安全控管作業項目	本案作法說明	合規性評估
申辦信用貸款方案者，採用第 7 條第 1 款至第 7 款之任一款安全設計。 (E)辦理新戶申請信用卡，僅限採用第 7 條第 1 款、第 8 款或第 9 款之任一款安全設計。		
<u>交易面之安全設計--採用第 7 條第 1 款憑證簽章</u> 【安控基準第 9 條第 1 款】 1.應採用經銀行公會認可之憑證機構及其所簽發之憑證，並遵循憑證機構之憑證作業基準檢核其憑證措施，以加強安控機制，維護網路交易安全。 2.使用憑證應用於「電子轉帳及交易指示類」時，應確認憑證之合法性、正確性、有效性、保證等級及用途限制。 3.接受他金融機構憑證訊息時，應使用經銀行公會認可之憑證機構簽發之憑證並遵循「金融 XML 憑證共用性技術規範」且於高風險交易時必須使用硬體裝置儲存金鑰。接受他金融機構憑證載具時，應使用經銀行公會審核通過之中介軟體所支援之憑證載具。 4.憑證線上更新時，須以原使用中有效私密金鑰對「憑證更新訊息」做成簽章傳送至註冊中心提出申請。 5.應用於簽入作業時，應簽署足以識別該個人之資料(如：統一編號)；於帳務交易時，應簽署完整付款指示。 6.應用於高風險交易或依據「銀行受理客戶以網路方式開立數位存款帳戶作業範本」開立第一類帳戶並採用高風險之介面安全設計進行身分驗證者，憑證私鑰應儲存於經第三方認證之硬體裝置。該裝置之晶片應符合我國國家標準 CNS 15408 EAL 4+(含增項 AVA_VLA.4 及 ADV_IMP.2)或共通準則(Common Criteria)ISO／IEC 15408 v2.3 EAL 4+(含增項 AVA_VLA.4 及 ADV_IMP.2)或 ITSEC level E4 或 FIPS 140-2 Level 3 以上或其他相同安全強度之認證，以防止該私鑰被匯出或複製。若晶片與產生交易指示為同一設備，則應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		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
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。 7.擔任憑證註冊中心受理客戶憑證註冊或資料異動時，其臨櫃作業應增加額外具「兩項以上技術」之安全設計或經由另一位人員審核。		
交易面之安全設計--採用第7條第2款晶片金融卡簽章【安控基準第9條第2款】 1.於簽入作業時，應由原發卡行驗證交易驗證碼始得簽入(如：餘額查詢交易)。 2.系統應依每筆交易動態產製不可預知之端末設備查核碼，並檢核網頁回傳資料之正確性與有效性。 3.於帳務性交易時，系統應每次輸入卡片密碼產生交易驗證碼。 4.元件於存取卡片時應設計防止第三者存取。 5.應提示收回卡片妥善保管。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
交易面之安全設計--採用第7條第3款一次性密碼【安控基準第9條第3款】 1.採用軟體OTP(含簡訊傳送OTP)不得運用於設定約定轉入帳戶。 2.所產生之一次性密碼，如應用於低風險非約定轉帳交易時，且該密碼與交易內容無關者，應限定該密碼於產生時起120秒內有效。應用於ATM無卡提款產生之一次性「提款序號」，其有效時限可由個別金融機構考量風險承擔之能力與客戶便利性斟酌訂定與調整，惟應不逾該序號產生時起30分鐘。 3.考量電腦或行動裝置，可能同時遭植入惡意程式竊取登入密碼及OTP，應用於非約定轉入帳戶轉帳交易時，應加強防護機制(如設備指定、推播確認、郵件回覆、採用非交易設備確認交易內容等)。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
交易面之安全設計--採用第7條第4款生物特徵【安控基準第9條第4款】 金融機構應依據其風險承擔能力調整生物特徵之錯誤接受度，以能有效識別客戶身分，必要時應增		□符合 □不符合，預計完成改善時間：__年__

安全控管作業項目	本案作法說明	合規性評估
加其他身分確認機制(如密碼)；採用間接驗證者，應事先評估客戶身分驗證機制之有效性。		月__日 □不適用
<u>交易面之安全設計--採用第 7 條第 5 款視訊會議</u> 【安控基準第 9 條第 5 款】 1.應確認真實視訊環境(如隨機問答)，以防止透過科技預先錄製影片。 2.應依相關規定留存影像或照片，以利後續查證。 3.若依規定須驗證留存證件者應核對確認。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
<u>交易面之安全設計--採用採用第 7 條第 6 款知識詢問或第 7 條第 7 款固定密碼</u>【安控基準第 9 條第 6 款】 1.僅限應用於非首次之認識客戶作業、非首次之客戶風險承受度測驗、信託業推介及終止推介同意書、信用卡業務(新戶申辦信用卡除外)、貸款申請、約定轉入帳戶轉帳、概括約定繳稅費之扣款、限定性繳稅費之扣款、同一統一編號帳戶間轉帳、共同行銷、不涉及帳務通知或交易之個人資料異動。 2.應用於信用卡申辦或貸款申請之契約成立時，應增加另一照會機制(如簡訊 OTP、兩項以上技術等)。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
<u>交易訊息之安全限制—行動裝置之安全規定</u>【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，預計完成改善時間：__年__月__日 □不適用
<u>交易訊息之安全限制—行動裝置之安全規定</u>【安		□符合 □不符合，預計

安全控管作業項目	本案作法說明	合規性評估
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。		完成改善時間：__年__月__日 □不適用
交易訊息之安全限制【安控基準第 9 條第 8 款】 應用於信用卡申辦或貸款申請時，客戶意思表示同意金融機構查詢聯徵中心信用資料，系統應留存記錄(如日期、來源 IP 或電話號碼、同意內容或版本、身分驗證結果等)。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
交易訊息之安全限制【安控基準第 9 條第 9 款】 1.個人資料顯示應採取隱碼機制。 2.例外情形： (1)系統已對客戶進行身分確認者(如簽入作業)，得不隱碼其確認交易之必要資訊。 (2)已採取本基準第 7 條第 1 款至第 4 款之任一安全設計者，變更個人資料欄位得不予隱碼處理。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用
交易訊息之安全限制【安控基準第 9 條第 10 款】 應用於法人客戶之高風險交易且未依據無法否認傳送訊息與無法否認接收訊息之訊息傳輸安全設計使用數位簽章者，應遵循下列必要措施： 1.應針對金融機構本身及客戶進行風險評估，訂定交易額度與管控機制，並提報董(理)事會或經其授權之經理部門核定，但外國銀行在臺分行，得由總行授權之人員為之。 2.應提供客戶交易再確認機制，並確保在安全實體環境下交付給客戶(如雙通道啟用)，客戶端應於每筆交易須經由至少兩人以上進行交易內容再確認，包含一位交易建檔人員及一位以上授權人員。 3.交易再確認機制應採用第 7 條第 2 款至第 4 款任		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
一介面之安全設計，並使用硬體設備保護敏感資料。 (1)硬體設備為防止敏感資料外洩得採用資料輸出管控機制、遮蔽作用之塗層保護機制、破壞偵測與歸零清除保護機制、開機自我測試機制、防止電磁干擾保護機制或其他足以保護設備內敏感資料之安全設計。 (2)若硬體設備具對外連結介面者(如 USB、藍芽、ISO 7816)需限定單一操作程序並符合我國國家標準 CNS 15408 EAL 4+(含增項 AVA_VLA.4 及 ADV_IMP.2)、共通準則(Common Criteria)ISO/IEC 15408 v2.3 EAL 4+(含增項 AVA_VLA.4 及 ADV_IMP.2)、ITSEC level E4、FIPS 140-2 Level 3 以上或其他相同安全強度之認證。 4.應提供完整交易之身分確認、交易再確認、交易異動、訊息通知等軌跡紀錄。 5.應提供額度授權機制，經由客戶妥善評估後授權其指定交易人員，藉以協助管理之帳戶與交易額度。 6.應建置防偽冒與洗錢防制偵測系統之風險分析模組與指標，於異常交易行為發生時立即告警並妥善處理；該風險分析模組與指標應定期檢討修訂。 7.傳輸敏感資料時，應提供端點對端點加密機制(如 end-to-end encryption, E2EE)，於客戶端輸入資料時立即加密，傳送至金融機構端符合 FIPS 140-2 Level 3 以上之硬體安全模組(如 HSM)內進行解密，以避免中間人(Man In The Browser、Man In The Middle)竊取；傳輸固定密碼者須於硬體安全模組內進行驗證。 8.應建立通知機制，於進行交易再確認或敏感資料異動時立即通知客戶。 9.應偵測釣魚網站，提醒客戶防範網路釣魚。 10.應提供客戶安全教育宣導，強化風險認知與交易確認要求。		

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，預計完成改善時間：__年__月__日 □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，預計完成改善時間：__年__月__日 □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，預計完成改善時間：__年__月__日

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。		□不適用
<u>建立安全防護策略--自動櫃員機</u>【安控基準第 12 條第 2 款】 1.自動櫃員機金庫裝置應符合美規 UL291 LEVEL 1 標準或歐規 CEN L 或日本自動販賣協會 Level 3 或其他相同安全強度之金庫標準。自動櫃員機之附屬設備(如硬幣存款機)其外殼材質與厚度應符合 1.35mm 厚度之無塗層鋼板或 1.42mm 之鍍鋅鋼板或 1.91mm 厚度之銅或鋁板等標準，以提供基本安全防護。 2.自動櫃員機鍵盤(KEY BOARD/PIN PAD)應符合亂碼化鋼製安全鍵盤(EPP)規格。 3.自動櫃員機讀卡機(CARD READER)應符合下述之標準： (1)ISO 標準 1/2/3 軌磁卡讀寫功能 (2)ISO 7816 4.自動櫃員機應具備 H/ W DES 亂碼化裝置(Triple DES)。 5.自動櫃員機應具備斷電卡片自動退出裝置。 6.自動櫃員機應具備卡片沒收裝置。 7.自動櫃員機應具備標準通訊介面。 8.運用自動櫃員機(CD/ATM)處理卡片交易時，應符合下述規範： (1)卡片內含錄碼及資料，除帳號/卡號、有效期限、交易序號及查證交易是否發生之相關必要資料外，其他資料一律不得儲存於自動櫃員機。 (2)應確定自動櫃員機協力廠商應與金融機構簽訂資料保密協定。並應		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
將參與自動櫃員機安裝、維護作業之人員名單交付金融機構造冊列管，如有異動，應隨時主動通知金融機構更新之。 (3)自動櫃員機協力廠商人員至自動櫃員機裝設現場作業時，均應出示經由金融機構認可之識別證件。除安裝、維護作業外，並應配合金融機構隨時檢視自動櫃員機硬體是否遭到不當外力入侵或遭裝置側錄設備。 (4)不定時派員抽檢行內外之自動櫃員機，檢視該硬體是否遭到不當外力入侵，並檢視其軟體是否遭到不法竄改。 (5)應與裝設地點之商家訂立檢核契約。 (6)應確保自動櫃員機之合法性。自動櫃員機應有唯一之ID(端末設備代號)，且針對晶片卡交易應依每筆交易動態產製不可預知之端末設備查核碼，並檢核資料之正確性與有效性。 9.自動櫃員機及其附屬設備應具備辨識新臺幣鈔券或硬幣真偽之功能。		
<u>建立安全防護策略--運用銷售端末設備（POS）處理交易</u>【安控基準第12條第2款】 實體卡片運用銷售端末設備(POS)處理交易時，應符合下述規範： 1.卡片內含錄碼及資料，除帳號／卡號、有效期限、交易序號及查證交易是否發生之相關必要資料外，其他資料一律不得儲存於銷售端末設備。 2.應確保銷售端末設備之合法性。銷售端末設備應有唯一之ID(端末設備代號)，且針對晶片卡交易應依每筆交易動態產製不可預知之端末設備查核		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

安全控管作業項目	本案作法說明	合規性評估
碼，並檢核資料之正確性與有效性。 3.應確定銷售端末設備協力廠商應與金融機構簽訂資料保密協定。並應將參與銷售端末設備安裝、維護作業之人員名單交付金融機構造冊列管，如有異動，應隨時主動通知金融機構更新之。 4.銷售端末設備協力廠商人員至特約商店現場作業時，均應出示經由金融機構認可之識別證件。除安裝、維護作業外，並應配合金融機構隨時檢視端末設備硬體是否遭到不當外力入侵或遭裝置側錄設備。 5.不定時派員抽檢安裝於特約商店之銷售端末設備，檢視該硬體是否遭到不當外力入侵，並檢視其軟體是否遭到不法竄改。 6.應與商家訂立檢核契約。		
提高系統可靠性之措施【安控基準第12條第2款】 得以下列方式處理及管控： 1.規劃備援線路。 2.規劃備援電路或 UPS。		□符合 □不符合，預計完成改善時間：__年__月__日 □不適用

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
卡片之安全設計--建立安全防護策略 【安控基準第 13 條第 2 款】 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，預計完成改善時間：__年__月__日 □不適用
卡片之安全設計--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，預計完成改善時間：__年__月__日 □不適用
卡片之安全設計--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，預計完成改善時間：__年__月__日 □不適用

評估人：_____　　部門主管：_____　　內部稽核：_____　　負責人：_____