安全控管作業基準要求項目與營業計畫書內容對照說明

檢核單位：○○○○○○○○

檢核日期：　　年　　月　　日

本中心/本農（漁）會網路銀行服務系統，係遵循金融機構辦理電子銀行業務安全控管作業基準之規範，以下就安控基準各項要求逐一對照說明本中心/本農（漁）會網路銀行安全設計。

一、交易面之安全需求及安全設計

(一)交易面之安全需求

交易面之安全需求依安全防護措施之不同分述如下：

1、訊息隱密性(Confidentiality)：係指訊息不會遭截取、窺竊而洩漏資料內容致損害其秘密性。

2、訊息完整性(Integrity)：係指訊息內容不會遭篡改而造成資料不正確性，即訊息如遭篡改時，該筆訊息無效。

3、訊息來源辨識(Authentication)：係指傳送方無法冒名傳送資料。

4、訊息不可重複性(Non-duplication)：係指訊息內容不得重複。

5、無法否認傳送訊息(Non-repudiation of sender)：係指傳送方無法否認其傳送訊息行為。

6、無法否認接收訊息(Non-repudiation of receiver)：係指接收方無法否認其接收訊息行為。

(二)各訊息傳輸途徑所應達到之安全防護措施如下：

訊息傳輸途	金融機構專屬網路			網際網路		
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
	高風險性之交易	低風險性之交易		高風險性之交易	低風險性之交易	
訊息隱密性	非必要	非必要	非必要	必要	必要	備註一
訊息完整性	必要	必要	非必要	必要	必要	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

訊息不可重複性	必要	必要	非必要	必要	必要	非必要
無法否認傳送訊息	必要	非必要	非必要	必要	非必要	非必要
無法否認接受訊息	必要	非必要	非必要	必要	非必要	非必要

【備註】

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，應具備訊息隱密性防護措施。

(三)交易面之安全設計

係指客戶發送訊息時，其介面及訊息之通訊傳輸應達到之安全防護措施之設計方法，亦即金融機構於系統開發設計時，應加以考量或應具備之基本原則及項目。

1、介面之安全設計：

（1）使用晶片金融卡簽入之安全設計應符合晶片金融卡交易驗證碼之安全設計。

本中心/本農（漁）會：

（2）使用一次性密碼（One Time Password，OTP）之安全設計，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，金融機構應能防止該密碼被側錄或再應用，方可應用於簽入或低風險交易。因不具有無法否認傳送訊息及無法否認接受訊息，無法符合高風險交易需求。

本中心/本農（漁）會：

（3）使用憑證簽章之安全設計，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。於簽入作業時，應簽署足以識別該個人之資料(如：身分證字號)；於帳務交易時，應簽署完整付款指示；於憑證展期時，應簽署展期訊息。

本中心/本農（漁）會：

（4）使用「兩項(含)以上技術」之安全設計，應具有下列兩項(含)以上技術：

◆客戶與銀行所約定的資訊，且無第三人知悉（如設備密碼、登入密碼等）。

◆客戶所持有的設備，金融機構應確認該設備為客戶與銀行所約定持有的實體設備（如密碼產生器、密碼卡、晶片卡、電腦、手機、憑證載具等）。

◆客戶所擁有的生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈等)。

本中心/本農（漁）會：

（５）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，其應具備之安全設計原則如後，惟若金融機構另佐以其他簽入驗證或交易驗證者，得將下述密碼之安全設計列為最低要求。

（５・１）用戶代號之安全設計：

（５・１・１）金融機構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。

（５・１・２）不應少於六位。

（５・１・３）不應訂為相同的英數字、連續英文字或連號數字。

（５・１・４）客戶於申請後若未於一個月（日曆日）內變更密碼，則不得再以該用戶代號執行簽入。

（５・１・５）客戶同一時間內只能登入一次密碼。

（５・１・６）如增設使用者代號，至少應依下列方式辦理：

（５・１・６・１）不得為客戶之顯性資料。

（５・１・６・２）如輸入錯誤達五次，金融機構應做妥善處理。

（５・１・６・３）新建立時不得相同於用戶代號及密碼；變更時，亦同。

本中心/本農（漁）會：

（５・２）密碼之安全設計：

（５・２・１）不應少於六位。若搭配交易密碼使用則不應少於四位。

（５・２・２）建議採英數字混合使用，且宜包含大小寫英文字母或符號。

（５・２・３）不應訂為相同的英數字、連續英文字或連號數字，預設密碼不在此限。

（５・２・４）密碼與代號不應相同。

（５・２・５）密碼連續錯誤達五次，不得再繼續執行交易。

（５・２・６）變更密碼不得與前一次相同。

（５・２・７）首次登入時，應強制變更預設密碼。

（５・２・８）密碼超過一年未變更，金融機構應做妥善處理。

本中心/本農（漁）會：

２、網際網路應用系統之安全設計：金融機構提供網際網路應用系統，應遵循下列必要措施：

（１）載具密碼不應於網際網路上傳送。

本中心/本農（漁）會：

（２）系統應設計連線(Session)控制及網頁逾時(TimeOut)中斷機制。

本中心/本農（漁）會：

（３）系統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。

本中心/本農（漁）會：

（４）系統應辨識客戶輸入與系統接收之非約轉交易指示一致性。

本中心/本農（漁）會：

（５）系統應避免存在網頁程式安全漏洞(如 Injection、Cross-Site Scripting 等)。

本本中心/農（漁）會：

（６）系統應偵測網頁與程式異動時，進行紀錄與通知措施。

本中心/本農（漁）會：

（７）元件應驗證網站正確性。

本中心/本農（漁）會：

（８）元件應採用被作業系統認可之數位憑證進行程式碼簽章(CodeSign)。

本中心/本農（漁）會：

（９）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(如抽拔卡、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(含)以上技術」之介面設計認證機制。

本中心/本農（漁）會：

（１０）採用經本會審核之確認型讀卡機或載具並可人工確認交易內容者，得不執行本安全設計之第(4),(9)等必要措施項目。

本中心/本農（漁）會：

（１１）一有駭客入侵時，金融機構即應依狀況關閉服務、伺服器或網站，以確保交易安全。

本中心/本農（漁）會：

３、訊息傳輸之安全設計：

防護措施	安全設計之基本原則/基本配備
訊息隱密性	(１)訊息處理： 可採對稱性加解密系統或非對稱性加解密系統。 (１・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(含以上)之三重資料加密演算法(Triple DES)或金鑰有效長度為 128 位元(含以上)之進階資料加密演算法(AES)或其他安全強度相同之演算法。 (１・２)非對稱性加解密系統其應至少採用金鑰長度為 1024 位元(含以上)之 RSA 演算法或金鑰長度為 256 位元(含以上)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。 （１・３)須全文加密。 (２)金鑰交換： 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。 （２・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)或非對稱性加解密性統(如RSA)或依協商訊息加密金鑰(如採Diffie-Hellman Key Agreement)交換之。安全強度應符合上述(１・１)及(１・２)之規定。 （２・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)。 （２・２・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)，當採明碼交換時,應利用秘密分持(如分A、B碼)，以降低該金鑰洩漏之風險。 （２・２・２)非對稱性金鑰保護金鑰之交換,其公開金鑰可透過憑證(Certificate)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。 (３)金鑰生命週期： 金鑰應於使用一段期間後更換之，以確保其安全性。 本中心/本農（漁）會：
訊息完整性	(１)訊息處理： 可採對稱性加解密系統或非對稱性加解密系統。 (１・１)對稱性加解密系統如 DES(使用押碼(Message Authentication Code，MAC))等機制，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。 (１・２)非對稱性加解密系統如 RSA(使用數位簽章(Digital Signature))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)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。 本中心/本農（漁）會：
訊息來源辨識	(１)訊息處理： 可採對稱性加解密系統或非對稱性加解密系統。 對稱性加解密系統如 DES(使用押碼(Message Authentication Code，MAC))等機制，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。 (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。 本中心/本農（漁）會：
訊息不可重複性	如使用序號、時戳等機制。 本中心/本農（漁）會：
無法否認傳送訊息	(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透過憑證交換，且此憑證須由憑證機構(Certification Authority，CA)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。 本中心/本農（漁）會：
無法否認接受訊息	同前述「無法否認傳送訊息」規範。 本中心/本農（漁）會：

備註：憑證機構係指居公正客觀地位，查驗憑證申請人身分資料正確性及其與待驗證公開金鑰間之關連性，並據以簽發公開金鑰憑證之單位。

４、交易訊息之安全限制：

（１)「非電子轉帳及交易指示類」中「帳務類查詢」之限制透過網際網路執行「非電子轉帳及交易指示類」中「帳務類查詢」之交易指示訊息，其運用之安全機制應具備「訊息隱密性」之基本防護措施，若涉及第三方居間代理者除以契約約定者外，銀行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。

（２)「電子轉帳及交易指示類」之限制

（２・１）金融機構應與事業單位以契約規範「限定性繳費稅」業務。「限定性繳費稅」倘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前述介面之安全設計；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。

本中心/本農（漁）會：

（２・２）透過網際網路執行「電子轉帳及交易指示類」之低風險交易指示訊息，除限定性繳費稅交易外，其運用安全機制若不具備「無法否認傳遞訊息」、「無法否認接收訊息」等基本防護措施者，則其運用之對稱性加解密系統之金鑰長度不得小於 128 位元(如強制高加密型 SSL、EV SSL)，且必須增設安全設計(如固定密碼、OTP)，並配合採用各種嚴密的技術防護措施且能有效防範密碼資料被竊取或交易資料被竄改，以健全安全防護機制。

本中心/本農（漁）會：

（２・３）透過公眾交換電話網路(PSTN)無法提供加密功能者(如電話銀行交易)，因係以明碼資料於線上傳輸，故以約定轉出功能，且轉入帳號逐戶約定，公用事業費及各類稅費繳納以概括約定方式為限，惟倘屬限定性繳費稅之低風險性交易，得採非約定轉出功能；金融機構得增設安全設計(如固定密碼、OTP 等)，以健全安全防護機制。採用固定密碼安全設計者得以干擾訊號或其他機制防止密碼遭側錄。

本中心/本農（漁）會：

（３）採用憑證簽章安全設計之安全規定

（３・１）金融機構應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。

（３・２）使用憑證應用於「電子轉帳及交易指示類」時，金融機構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・３）接受他行憑證訊息時，應使用經本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。接受他行憑證載具時，應使用經本會審核通過之中介軟體所支援的憑證載具。

（３・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。

（３・５）應用於高風險交易時，憑證金鑰應儲存於符合 Common Criteria EAL 4+(至少包含增項 AVA_VLA.4 或 AVA_VAN.5)或 ITSEC level E4 或 FIPS

140-1 Level 2 或其他相同安全強度之認證等晶片硬體內，以防止該私鑰被匯出或複製，且該晶片硬體不得常駐於產生交易指示之設備，確保交易安全。

（３・６）金融機構擔任憑證註冊中心，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(含)以上技術」之安全設計或經由另一位人員審核。

本中心/本農（漁）會：

(４)採用晶片金融卡安全設計之安全規定

（４・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)。

（４・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。

（４・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(TAC，Transaction Authentication Code)。

（４・４）元件於存取卡片時應設計防止第三者存取。

（４・５）應提示收回卡片妥善保管。

本中心/本農（漁）會：

（５）採用行動裝置之安全規定

（５・１）採用晶片金融卡安全設計者，基碼應儲存於安全元件(SE)內，其晶片應符合「晶片金融卡規格安控等級」。

（５・２）行動裝置安全元件(SE)因其長期於連接網際網路之環境，應於交易時增設存取控管，以防止遭受惡意程式發動阻絕服務攻擊(DoS)或偽冒交易。

本中心/本農（漁）會：

（６）個人資料之保護透過網際網路呈現個人資料，金融機構應採用「兩項(含)以上技術」等技術保護，有效防範資料被竊取，以落實個人資料保護。

本中心/本農（漁）會：

５、雙因素認證：以上所述採用「兩項(含)以上技術」係指伍、一、(三)、1、(4)所述技術。

本中心/本農（漁）會：

二、管理面之安全需求及安全設計

(一)管理面之安全需求

金融機構應依其內部相關規範辦理，並加強系統上線前之相關測試檢核措施。本安全需求係著重於防範金融機構電腦資源，遭外部以電子銀行相關管道入侵威脅及破壞；期能有效地維護電腦資源之整體性及其隱密性，並保護電腦系統作業安全及維持其高度可使用性。

防護措施	目的
建立安全防護策略	為保障系統安全，唯有經授權之客戶得以存取系統資源,並降低非法入侵之可能性。
提高系統可靠性之措施	提昇電腦系統之可靠性及高度可使用性，亦即減少電腦系統無法使用之機會。
制定作業管理規範	作業管理規範包含金融機構及客戶端兩部分，目的在確定金融機構內部之責任制度、核可程序及確定客戶與金融機構間之責任歸屬。

(二)管理面之安全設計

系統管理面之安全設計係指針對金融機構於系統開發設計時，於系統管理面應加以考量或應具備之基本原則及基本項目。

防護措施	安全設計
建立安全防護策略	應以下列方式處理及管控： 1、系統應依據網路服務需要區隔出獨立的邏輯網域(如 Internet, DMZ, Intranet)，每個網域皆有既定的防護措施並有通訊閘道管制過濾網域間資料的存取。 本中心/本農（漁）會： 2、系統應採用入侵偵測與防護措施，提高資安防護。 本中心/本農（漁）會： 3、系統應將重要參數檔加密防護。(如：電腦系統密碼檔)

	本中心/本農（漁）會： 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) 本中心/本農（漁）會： 2、設計存取權控制(Access Control)如使用密碼、身分證字號、磁卡、IC卡等。 本中心/本農（漁）會： 3、簽入(Login)時間控制。 本中心/本農（漁）會： 4、單次簽入(Single-Sign-on)。 本中心/本農（漁）會： 5、撥接控制(Dial-up Control)。 本中心/本農（漁）會： 6、專線(Lease-Line)使用。 本中心/本農（漁）會： 7、記錄使用者查詢電話。 本中心/本農（漁）會： 8、控制密碼錯誤次數。 本中心/本農（漁）會：

	9、電腦系統密碼檔加密。 本中心/本農（漁）會： 10、留存交易紀錄(Transaction Log)及稽核追蹤紀錄(Audit Trail)。 本中心/本農（漁）會： 11、分級。 本中心/本農（漁）會： 12、業務面控制如約定帳戶、限定金額等。 本中心/本農（漁）會： 13、系統提供各項服務功能時，應確保個人資料保護措施。 本中心/本農（漁）會：
提高系統可靠性之措施	應以下列方式處理及管控： 1、建置病毒偵測軟體(Virus Detection Software)，定期對網路節點及伺服器進行掃毒並應定期更新病毒碼。 本中心/本農（漁）會： 2、系統應進行弱點掃瞄與修補。 本中心/本農（漁）會： 3、系統應配合作業系統修正檔公佈，盡速修補系統漏洞。 本中心/本農（漁）會： 4、定期更換提供給操作者之應用軟體及

	作業系統密碼。 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。 本中心/本農（漁）會： （2）放置網路伺服器於上鎖密室中。 本中心/本農（漁）會：
制定作業管理規範	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。 本中心/本農（漁）會： 2、 編寫客戶端之操作手冊及制訂完整契約，金融機構應於 eATM 交易畫面揭示使用 eATM 金融交易之風險。 本中心/本農（漁）會：