附件一

本會99年7月29日第9屆第28次理監事聯席會議討論通過
金管會99年8月31日金管銀國字第09900311870號函洽悉
本會102年3月28日第10屆第26次理監事聯席會議討論通過
金管會102年6月3日金管銀國字第10200120550號函洽悉
本會103年11月27日第11屆第13次理監事聯席會議討論通過
金管會104年1月13日金管銀國字第10300348710號函洽悉
本會105年1月28日第11屆第25次理監事聯席會議討論通過
金管會105年3月18日金管銀國字第10500036310號函洽悉
本會105年6月30日第11屆第29次理監事聯席會議討論通過
金管會105年8月16日金管銀國字第105 00193690號函洽悉
本會105年12月22日第12屆第3次理監事聯席會議討論通過
本會106年2月23日第12屆第5次理監事聯席會議討論通過
金管會106 年5月11日金管銀國字第10600092510號函洽悉
本會106年11月30日第12屆第3次理監事聯席會議討論通過
金管會107 年3月14日金管銀國字第10702029320號函洽悉
本會107年10月25日第12屆第21次理監事聯席會議討論通過
金管會108 年2月18日金管銀國字第10702255770號函洽悉
本會108年6月27日第12屆第6次理事會議討論通過
金管會108 年10月23日金管銀國字第1080216776號函洽悉
本會109年6月18日第13屆第7次理監事聯席會議討論通過
金管會109年7月7日金管銀國字第10901401891號函洽悉
本會109年8月14日第13屆第8次理監事聯席會議討論通過
金管會109年12月24日金管銀國字第1090143726號函洽悉
本會110年3月4日第13屆第12次理監事聯席會議討論通過
金管會110年4月15日金管銀國字第11001337391號函洽悉
本會111年1月20日第13屆第18次理監事聯席會議討論通過
金管會 111 年 5 月 16 日金管銀國字第 1110205052 號函洽悉
本會 111 年 12 月 22 日第 14 屆第 3 次理監事聯席會議討論通過
金管會 112 年 6 月 14 日金管銀國字第 1120202881 號函洽悉
本會 113 年 12 月 19 日第 14 屆第 6 次理事會議核議通過
金管會 114 年 3 月 18 日金管銀國字第 1130152842 號函洽悉

金融機構辦理電子銀行業務安全控管作業基準

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）為確保金融機構辦理電子銀行業務具有一致性基本準則之安全控管作業，特訂定本基準。

第二條　本基準用詞定義如下：

一、電子銀行(Electronic Banking)業務：係指在金融機構與客戶(自然人及法人)間，透過各種電子設備及通訊設備，客戶無須親赴金融機構櫃台，即可直接取得金融機構所提供之各項金融服務。

二、存款帳戶：係指金融機構受理客戶臨櫃申請所開立之存款帳戶（含以多功能視訊櫃檯開立之新臺幣活期及定期存款帳戶）及以網路方式所開立之數位存款帳戶。

三、概括約定繳稅費：係指客戶透過電子銀行、授權事業單位或金融機構發動交易指示，由客戶事先約定本人之轉出帳戶繳納政府機關或事業單位之各類稅費。

四、限定性繳稅費：係指客戶透過電子銀行、授權事業單位或金融機構發動交易指示，由客戶之轉出帳戶繳納政府機關、金融機構或事業單位之各類稅費及投資款項。

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

六、行動應用程式(mobile application；以下簡稱行動 APP)：係指安裝於行動裝置上之應用程式。

中華民國銀行商業同業公會全國聯合會
金融業務電子化委員會
1140318 版本

七、銷售端末設備(Point Of Sale；以下簡稱 POS)：係指一設備可讀取商品資訊、連結付款機制、記錄商品銷售行為並將資料傳送至後台進行帳務處理。

八、應用程式與應用程式間資料傳輸(Application to Application；以下簡稱 AP2AP)：係指金融機構與客戶端事先約定應用系統相互傳輸通訊與規格，以達到自動化資訊交換，並執行各項查詢或交易行為。

九、雙音多頻訊號(Dual-Tone Multi-Frequency)：係指將電話撥號按鍵之每一按鍵設定成一組高頻與低頻兩個聲音，透過按鍵傳送訊息。

十、常用密碼學演算法如下：

(一) 對稱性加解密系統：指採用資料加密標準(Data Encryption Standard；以下簡稱 DES)、三重資料加密標準(Triple DES；以下簡稱 3DES)、進階資料加密標準(Advanced Encryption Standard；以下簡稱 AES)等運算進行資料加密。

(二) 非對稱性加解密系統：指採用 RSA 加密演算法(Rivest, Shamir and Adleman Encryption Algorithm；以下簡稱 RSA)、橢圓曲線密碼學(Elliptic Curve Cryptography；以下簡稱 ECC)等運算進行資料加密。

(三) 訊息鑑別系統：指採用訊息鑑別碼(Message Authentication Code；以下簡稱 MAC；如 DAA、HMAC)、雜湊函式(Hash Function；如 SHA256)等運算，將不定長度資料產生固定長度之資料進行比對。

十一、訊息傳輸途徑：客戶端利用電子設備及通訊設備與金融機構進行訊息傳輸時所使用之網路型態，區分如下：

(一)專屬網路：指透過撥接(Dial-Up)、專線(Lease-Line)或虛擬私有網路(Virtual Private Network)等方式進行訊息傳輸。

(二)網際網路(Internet)：指世界各地不同之網路，以 TCP/IP 通訊協定互相連線，提供連線者互通信息，互傳資料與共享各類資源。

(三)加值網路(Value Added Network)：指提供網路附加價值之服務，如自動錯誤偵測及修復、通訊協定轉換及訊息儲存及後送等；惟實際運用時應依個別加值網路服務業者與金融機構間傳輸途徑之不同，分別納入前述專屬網路或網際網路傳輸途徑予以規範。

(四)行動網路：指透過無線網路服務(如 4G、WiFi)進行訊息傳輸。惟實際運用時應依個別服務業者與金融機構間傳輸途徑之不同，分別納入前述專屬網路或網際網路傳輸途徑予以規範。

(五)公眾交換電話網路(Public Switched Telephone Network)：指透過電信服務業者(Telecom)提供之傳輸設備與線纜，將聲波訊

息經由各區域間佈建之交換機房(telecom room)或基地台(base station)，傳送至金融機構之電信交換機進行訊息傳輸。

十二、訊息防護措施區分如下：

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

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

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

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

(五) 訊息不可否認性（ Non-repudiation）：指無法否認其傳送或接收訊息行為。

十三、公開金鑰基礎建設(Public Key Infrastructure)成員如下：

(一)憑證機構(Certification Authority；以下簡稱 CA)：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。

(二)註冊中心(Registration Authority)：係指擔任驗證憑證申請人及憑證請求等資訊正確性之工作。

(三)憑證用戶(Subscriber)：係指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰(Private Key)者。憑證用戶可以是自然人或組織。

(四)信賴憑證者(Relying Party)：係指相信憑證主體名稱與該主體公開金鑰及私密金鑰連結關係之個人或組織。

十四、一次性密碼技術：係指以下三種方式擇一辦理

(一)基於時間因子演算的一次性密碼：係指一種以金鑰與當前時間計算而產生的一次性密碼。

(二)基於計數器數值演算的一次性密碼：係指一種以金鑰與當前計數器數值計算而產生的一次性密碼。

(三)基於來源訊息演算的一次性密碼：係指一種以金鑰與接收資料計算而產生的一次性密碼。

十五、插拔卡：為一種人工確認方式。可於交易確認時，用以確認由人工進行交易，無法以惡意程式模擬。此設計應要防止避免系統組態或服務之改變而誤判。

十六、特殊按鍵：為一種人工確認方式。可於交易確認時，用以確認由人工進行交易，無法以惡意程式模擬。此設計應要防止可由程式模擬特殊按鍵。

十七、安全元件(Secure Element)：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、行動裝置內建晶片及 MicroSD 等。

十八、網路 ATM(Electronic ATM；以下簡稱 eATM)：於網際網路上透過卡片讀卡機，以軟體程式存取 PC/SC 讀卡機，提供除現金提存外之實體 ATM 功能。

十九、可信賴執行環境(Trusted Execution Environment)：係指獨立於行動裝置作業系統的一個受信任的執行環境，允許受信任的應用程式通過安全軟體授權在此環境執行，達到與其他部分的隔離。

二十、結構型商品：係指

(一)「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」(以下簡稱衍商辦法)第二條所稱之結構型商品。

(二)「信託業營運範圍受益權轉讓限制風險揭露及行銷訂約管理辦法」第二十二條之一所稱之境內結構型商品及「境外結構型商品管理規則」第二條所稱之境外結構型商品。

二十一、消費扣款：係指客戶向實體或虛擬之特約商店進行物品、勞務或其他交易時，使用發卡機構核發之金融卡或透過電子銀行/行動銀行，委託發卡機構直接由客戶之指定帳戶即時扣款，轉入收單機構或特約商店指定帳戶之功能；前述金融卡包含但不限於磁條金融卡、晶片(感應式)金融卡、行動金融卡。

二十二、程序演練(Table Top Exercise, TTX)：係指一種紙上驗證作業程序的方法，用於假想情境發生並推估局勢發展，依據事先規劃的作業程序模擬執行，以驗證情境應變之完整性。

二十三、多功能視訊櫃檯(Video Teller Machine；以下簡稱 VTM)：係指一具有視訊、掃描及證件之辨識模組、具有可觀察客戶親簽及周邊之環境監控模組、24 小時保全及直接連結金融機構內部網路之設備。

二十四、客戶端電腦應用程式：係指金融機構提供並安裝於客戶端電腦(如 Windows, UNIX, MacOS)之應用程式(如 EXE,OCX,SCR,COM,DLL 等)。

二十五、臨櫃辦理：係指透過面對面，由本人親自辦理或持有授權文件之代理人親自辦理。

二十六、C3 憑證：指符合我國電子簽章法且經本會認可之臺灣網路認證公司簽發第三級商務 EC+憑證、第三級商務 XML 憑證(含商務 XML Plus)或中華電信公司簽發第三級 Public CA 憑證，其註冊中心應為金融機構。

二十七、信賴等級機制：係參考 ISO 29115 框架，以身分登錄、信物管理、身分驗證三個面向，依據安全設計與交易風險區分為最高、高、中、低、最低等五個信賴等級。

二十八、個人統一編號：係指內政部核發之國民身分證統一編號及外來人口統一證號。

二十九、統一編號：係指個人統一編號、營利事業機構與非營利機構的法人身分代號。

第三條　訊息分類

一、公開資訊：包含但不限於官網之匯利率。

二、個人資訊：個人資料保護法之個人資料，包含但不限於銀行帳號，惟排除個人統一編號及特種個資(包含病歷、醫療、基因、性生活、健康檢查、犯罪前科)。

三、身分識別資訊：個人統一編號、網銀登入之用戶代號及使用者代號。

四、身分核驗資訊：固定密碼、生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)。

五、機敏資訊：製卡個人化資料、非對稱式加密之私密金鑰、對稱式加密之加密金鑰、個人資料保護法之特種個資。

第四條　訊息保護

一、訊息加密機制：可採用下列任一機制進行全訊息加密。

(一)對稱性加解密：應至少採用 3DES 112bits 以上、AES 128bits 以上或其他安全強度相同之演算法；惟應用於 TLS 時，不得使用 3DES 演算法並建議使用數據認證加密模式(Authenticated Encryption with Associated Data, AEAD)。

(二)非對稱性加解密：應至少採用 RSA 2048bits 以上、ECC 256bits 以上或其他安全強度相同之演算法。

二、端點對端點加密機制：係指於客戶端(如瀏覽器)輸入資料後立即加密，傳送至金融機構可信任網段(如經兩道防火牆隔離之獨立網段)於經第三方認證(至少符合 FIPS 140-2 Level 3 或同等規格以上)之硬體安全模組內進行解密，並於硬體安全模組內或於無洩漏解密資料疑慮之安全環境進行驗證。

三、金鑰交換機制：採對稱性加解密時，其金鑰交換可分訊息加密金鑰與金鑰保護金鑰之交換，應遵循下列要求：

(一)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。安全強度應依據第一款訊息加密機制辦理。

(二) 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) ；惟應用於 TLS 時，建議使用 Elliptic Curve Diffie-Hellman Exchange 方式進行金鑰交換。

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。

四、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。

第五條　訊息處理

一、訊息傳輸：

(一)於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機制。採用用戶代號及固定密碼進行網路銀行身分確認(如簽入作業)且該用戶代號如為個人統一編號者，其使用者代號仍應加強防護(如雜湊、加密、混淆)，又該固定密碼應採用第四條第二款端點對端點加密機制。

(二)於公眾交換電話網路(Public Switched Telephone Network)上以雙音多頻訊號傳輸身分核驗資訊之固定密碼者，應以干擾訊號或其他機制防止遭側錄。

(三)於內部網路(Intranet)上傳輸客戶之身分核驗資訊或機敏資訊應採用如雜湊、加密、混淆、編碼等機制加強防護。

二、訊息儲存：

(一)身分核驗資訊之固定密碼應先進行不可逆運算(如雜湊)，另為防止透過預先產製雜湊值推測密碼，可採用加密、混淆等機制加強防護。

(二)身分核驗資訊之生物特徵、機敏資訊應採用訊息加密機制。

(三)前二目採用加密演算法者，其金鑰應儲存於經第三方認證(至少符合 FIPS 140-2 Level 3 或同等規格以上)之硬體安全模組內並限制明文匯出功能。

三、訊息顯示：

(一)個人資料顯示應採取隱碼機制。但如系統已對客戶進行身分確認者(如簽入作業)，得不隱碼其帳號及確認交易之必要資訊，或已

採取本基準第七條第一款至第四款之任一款安全設計者，變更個人資料欄位得不予隱碼處理。

(二)須取得客戶同意，始得顯示其同意之個人資料(如自然人戶名)給交易對方，以利交易確認。

第六條　交易類別及風險

客戶端利用電子設備及通訊設備以連線方式發送訊息至金融機構進行交易指示之交易類別，並依據其執行結果對客戶權益之影響區分風險之高低，區分如下：

一、電子轉帳及交易指示類

係指該交易指示直接涉及資金轉移或直接影響客戶權益者。

(一)服務項目

1、電子交易、轉帳授權、帳務通知，其服務項目如下：存提款、轉帳、匯兌、匯款、消費、投資（如基金、債票券、結構型商品）、款項繳納、授信、付款指示等交易。

2、申請指示，其服務項目如下：

(1)外匯業務：開發信用狀申請、修改信用狀申請。

(2)存款業務

甲、客戶得申辦數位存款帳戶、同意金融機構查詢聯徵中心信用資料。

乙、已開立存款帳戶者得申辦結清銷戶、約定轉入帳號、受理客戶傳真指示扣款無須再取得客戶扣款指示正本、晶片金融卡、非約定轉帳。

丙、客戶得以多功能視訊櫃檯開立之新臺幣活期及定期存款帳戶。

(3)授信業務

甲、本行既有個人客戶及新戶得申辦個人貸款、同意金融機構查詢聯徵中心個人信用資料。

乙、本行既有法人客戶、法人新戶及法人戶之負責人得申辦無涉及抵押權或質權設定之貸款、同意金融機構查詢聯徵中心信用資料。

丙、既有貸款戶得申辦授信條件變更。

丁、保證人得申辦同意金融機構查詢聯徵中心信用資料、成立保證契約。

戊、法人戶依信保基金規定應查詢之關係人(如配偶)得申辦同意金融機構查詢聯徵中心信用資料。

(4)信用卡業務

甲、新戶得申辦信用卡、同意金融機構查詢聯徵中心信用資料。

乙、已開立存款帳戶者或既有信用卡戶或既有貸款戶得申辦信用卡、同意金融機構查詢聯徵中心信用資料。

丙、既有信用卡戶得申辦長期使用循環信用持卡人轉換機制、同意信用卡分期產品約款。

(５)財富管理業務：

甲、認識客戶作業(KYC)。

乙、客戶風險承受度測驗。

丙、衍商辦法結構型商品業務之同意推介或終止推介、同意成為專業客戶、專業客戶聲明已充分審閱而無須適用審閱期。

(６)信託業務：

甲、已開立存款帳戶者得申辦各類信託開戶(含簽約)及變更、增補或終止信託契約

乙、認識客戶作業(KYC)

丙、客戶風險承受度測驗

丁、同意信託業務之推介或終止推介

戊、同意成為專業投資人之簽署

己、專業投資人表示已充分審閱而無須適用審閱期之聲明。

庚、依信託契約約定之信託財產運用範圍，為申請運用指示：

i. 同一統一編號帳戶間轉帳、定存或投資(含交易取消)。

ii. 辦理約定轉入帳戶之付款。

iii. 辦理非約定轉入帳戶之付款指示。

iv. 受益人行使表決權。

辛、依信託契約約定由委託人或信託監察人行使同意權。

(７)共同行銷業務：同意共同行銷。

(二)交易指示

１、高風險交易：係指該訊息執行結果，對客戶權益有重大影響之各類電子轉帳及交易指示，包含非約定轉帳交易超過辦理低風險交易最高限額之交易指示。

２、低風險交易：係指該訊息執行結果對客戶權益無重大影響之各類電子轉帳及交易指示，內容包括下列各項：

(１)辦理前目第二子目之申請指示。

(２)辦理 ATM 之存提款服務。

(３)照會、認識客戶、協助電子支付機構確認客戶身分等作

業。

（４）辦理約定轉入帳戶之設定及轉帳。

（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、票據交換所平台，進行概括約定繳稅費及限定性繳稅費之扣款約定及扣款服務。

（６）任一金融機構同一統一編號帳戶間轉帳、定存或投資。

（７）貸款撥款至任一金融機構同一統一編號帳戶或學校之就學貸款指定帳戶。

（８）客戶非直接獲取金融機構之服務且需其人工確認客戶身分與指示內容之申請指示、交易指示及資料預處理。

（９）辦理非約定轉入帳戶之轉帳。

（１０）個人資料異動（如用於身分確認之密碼、用於非約轉交易之聯絡資訊、用於雙方約定之通知方式、國外提款之磁條密碼、網路銀行使用者代號等）。

二、非電子轉帳及交易指示類

係指與資金轉移無關或不直接影響客戶權益者。

(一)查詢

１、帳務類：餘額查詢、交易明細查詢、額度查詢、歸戶查詢、託收票據查詢、匯入匯款查詢、信用狀查詢、帳單查詢、借款繳息清單、繳費單、扣繳憑單、扣費憑單、補充保費等。

２、非帳務類：匯率查詢、利率查詢、共同基金查詢、金融法規查詢、股市行情查詢、投資理財資訊查詢、業務簡介查詢。

３、個人資料類：聯絡資訊等。

(二)通知

入扣帳通知、存款不足通知、存放款到期通知、放款繳息通知、託收票據狀況通知、消費通知等。

第七條　身分核驗安全設計及信賴等級

一、 憑證簽章

(一)安全設計符合下列要求者，為最高信賴等級機制：

１、身分登錄：應於臨櫃辦理或書面同意由法人客戶指定人員核驗身分後辦理。

２、身分驗證：

（１）應確認憑證之合法性、正確性、有效性、保證等級及用途限制。

（２）應簽署適當內容；於簽入作業時，應簽署足以識別該個人之資料(如：個人統一編號)、於書面同意時，應簽署依相關法令規定之指定書件；應用於交易指示時，應簽署完整付款指示。

3、信物管理：

（1）應採用經本會核可由臺灣網路認證公司或中華電信公司簽發之金融用戶憑證(以下簡稱金融 XML 憑證)。

（2）接受他行金融 XML 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」。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之憑證載具。

（3）金融 XML 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。

（4）擔任金融 XML 憑證註冊中心受理客戶憑證註冊或資料異動時，其人工作業應增加額外具「兩項以上技術」之安全設計或經由另一位人員審核。

（5）金融 XML 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。

(二)安全設計符合下列要求者，為最高信賴等級機制：

1、身分登錄：不適用。

2、身分驗證：應遵循前目第二子目要求。

3、信物管理：

（1）應採用內政部簽發之自然人憑證或經濟部簽發之工商憑證。

（2）應採用晶片憑證載具。

(三)安全設計符合下列要求者，為高信賴等級機制：

1、身分登錄：限法人客戶並應於臨櫃辦理或書面同意由法人客戶指定人員核驗身分後辦理。

2、身分驗證：

（1）應遵循第一目第二子目要求。

（2）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。

（３）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。

（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）應建立通知機制，於進行交易再確認或機敏資訊異動時立即通知客戶。

３、信物管理：

（１）得採用非我國憑證機構且通過 WebTrust 或 ETSI 認可憑證機構簽發之憑證。

（２）應採用於具密碼保護之安全元件(Secure Element)、可信賴執行環境(Trusted Execution Environment)、安全載具(如動態密碼產生器)或增強防護機制之行動裝置應用程式軟硬體設備，以保護機敏資訊，並遵循下列安全設計：

甲、安全元件應符合我國國家標準 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。

乙、可信賴執行環境應符合 Global Platform 標準或其他相同安全強度之認證。

丙、安全載具應具備資料輸出管控機制、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機敏資訊之安全設計。

丁、行動裝置之應用程式應符合「金融機構提供行動裝置應用程式作業規範」第十五條安全防護措施或其他足以保護設備內機敏資訊之安全設計。

(四)安全設計符合下列要求者，為低信賴等級機制：

１、身分登錄：應於臨櫃辦理、採用低信賴等級機制以上之安全設計核驗身分後辦理。

２、身分驗證：應遵循第一目第二子目之（２)要求。

3、信物管理：

（1）應採用金融 XML 憑證、C3 憑證或非對稱性加解密系統(如 PGP)。

（2）私鑰應經密碼保護，以確保金鑰儲存安全。

二、晶片金融卡

(一)安全設計符合下列要求者，為高信賴等級機制：

1、身分登錄：限法人客戶並應於臨櫃辦理或書面同意由法人客戶指定人員核驗身分後辦理。

2、身分驗證：

（1）應遵循第一款第三目第二子目之(2)至(7)要求。

（2）應由原發卡行依據交易類型核驗對應之交易驗證碼(如：簽入得採餘額查詢交易)。

（3）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）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。

（5）元件於存取卡片時應設計防止第三者存取。

（6）應提示收回卡片妥善保管。

3、信物管理：

（1）建立安全防護策略：

甲、晶片金融卡之晶片應至少符合「晶片金融卡規格安控等級」如我國國家標準 CNS 15408 EAL 5、共通準則(Common Criteria) ISO/IEC 15408 v2.3 EAL 5 或 ITSEC level E4 等，並能防堵市面上常見之攻擊破解方法。

乙、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碼作為驗證每筆交易之不可否認性，用以確保交易安全。

丙、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。

（2）提高系統可靠性之措施

甲、 應做卡片容量規劃。

乙、 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」。

丙、 使用各種晶片端末設備，均應經本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。

丁、 應確保卡片端點對端點之交易安全。

(３)制定作業管理規範

甲、建議密碼設定，不得與其個人顯性資訊(如生日、身分證、車號、電話號碼、帳號及相關資料號碼)相同。

乙、密碼資訊不應書寫於實體卡片上，並須定期變更密碼。

丙、與客戶之契約規定應載明持卡人應負責事項，如保管權、使用權、遺失主動通報權及不當操作致毀損責任等。

丁、應於卡片上揭示掛失、二十四小時客服專線及拾獲擲回地址等資訊，並於發卡時主動告知客戶。

戊、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。

己、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。

(二)安全設計符合下列要求者，為高信賴等級機制：

１、身分登錄：應於臨櫃核驗身分或依據第一類(不含限適用第六條低風險交易)數位存款帳戶開戶程序核驗身分後辦理。

２、身分驗證：應遵循第一目第二子目之(２)至(６)要求。

３、信物管理：應遵循前目信物管理相關要求。

(三)安全設計符合下列要求者，為中信賴等級機制：

１、身分登錄：應依據適用第六條低風險交易之第一類數位存款帳戶及第二類數位存款帳戶開戶程序核驗身分後辦理

２、身分驗證：應遵循第一目第二子目之(２)至(６)要求。

３、信物管理：應遵循第一目信物管理相關要求。

(四)安全設計符合下列要求者，為低信賴等級機制：

１、身分登錄：應依據第三類數位存款帳戶開戶程序核驗身分後辦理。

２、身分驗證：應遵循第一目第二子目之(２)至(６)。

３、信物管理：應遵循第一目信物管理相關要求。

三、一次性密碼(以下簡稱 OTP)

(一)安全設計符合下列要求者，為高信賴等級機制：

１、身分登錄：限法人客戶並應於臨櫃辦理或書面同意由法人客戶指定人員核驗身分後辦理。

２、身分驗證：

(１)應遵循第一款第三目第二子目之(２)至(７)要求。

(２)應運用一次性密碼技術產生並限制一次性使用。

３、信物管理：應遵循第一款第三目第三子目之(２)要求。

(二)安全設計符合下列要求者，為中信賴等級機制：

１、身分登錄：應於臨櫃辦理、採用中信賴等級機制以上之安全設計或依據第一類(不含限適用第六條低風險交易)數位存款帳戶、適用第六條低風險交易之第一類數位存款帳戶或第二類數位存款帳戶開戶程序核驗身分後辦理。

２、身分驗證：

(１)應運用一次性密碼技術產生並限制一次性使用。

(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、信物管理：

(１)用於產生一次性密碼之金鑰應依據第五條訊息處理方式辦理。

(２)採用簡訊傳輸一次性密碼並應用於電子轉帳交易指示類時，發送端之電話門號應與發送行銷廣告之門號有所區隔，以利客戶識別。

(３)採用簡訊傳送一次性密碼並應用於開立第二類數位存款帳戶時，手機號碼之設定應於臨櫃辦理，另異動應採用臨櫃或第七條第一款至第五款任一款進行設定，惟排除透過軟體 OTP 或簡訊傳送 OTP 之安全設計。

(４)採用簡訊傳送一次性密碼並應用於非約定轉入帳戶轉帳交易者，應遵循下列要求：

甲、手機號碼之異動應採用臨櫃或第一款至第五款任一款進行設定。

乙、考量客戶交易使用之電腦或行動裝置，可能遭植入惡意程式竊取 OTP 等身分核驗資訊或機敏資訊，應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容或依金融機構風險評估至少具相同安全強度之安全機制)，並應留存評估紀錄及核決層級)。

(三)安全設計符合下列要求者，為低信賴等級機制：

1、身分登錄：應於臨櫃辦理、採用低信賴等級機制以上之安全設計、依信用卡業務機構管理辦法核發信用卡或依據第三類數位存款帳戶開戶程序核驗身分後辦理。

2、身分驗證：應遵循前目身分驗證相關要求。

3、信物管理：應遵循前目信物管理相關要求，惟應用於第三類數位存款帳戶之手機號碼異動應採用低信賴等級機制以上之安全設計核驗身分後辦理。

四、 兩項以上技術(以下簡稱 2FA)

(一) 安全設計符合下列要求者，為高信賴等級機制：

1、身分登錄：應於臨櫃辦理、VTM 辦理、書面同意由法人客戶指定人員辦理或依據第一類(不含限適用第六條低風險交易)數位存款帳戶開戶程序核驗身分後辦理。

2、身分驗證：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、SIM 卡認證、晶片護照、金鑰等)。

(3) 客戶提供給金融機構其所擁有之生物特徵，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。

甲、 採用直接驗證生物特徵技術者，應確認真人及本人辦理並符合「金融機構運用新興科技作業規範」有關生物特徵資料安全控管要求。又金融機構應依據其風險承擔能力調整生物特徵參數(如近似率、錯誤接受率、錯誤拒絕率)，以期有效識別客戶身分；若無法有效確認真人或本人時應加強其他安全設計，並應透過第三方依據 ISO/IEC 30107 攻擊樣態逐一進行檢測，以確保感測器所擷取的生物特徵是客戶的真實生物特徵，而非經過變造或偽冒。

乙、 採用間接驗證生物特徵技術者，應事先評估客戶身分驗證機制之有效性，善盡告知客戶使用上之風險，並提供間接驗證機制關閉管道；若該機制出現偽冒風險時，應加強其他安全設計(如交易密

碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)。

3、信物管理：前述兩項以上技術之約定資訊、設備或生物特徵應遵循第一款第三目第三子目之(2)要求。

(二) 安全設計符合下列要求者，為中信賴等級機制：

1、身分登錄：應於臨櫃辦理、採用中信賴等級機制以上之安全設計或依據適用第六條低風險交易之第一類數位存款帳戶或第二類數位存款帳戶開戶程序核驗身分後辦理。

2、身分驗證：應遵循前目身分驗證相關要求。

3、信物管理：應用於電子轉帳交易指示類並以簡訊傳送一次性密碼重新綁定兩項以上技術者，應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)，該機制應排除固定密碼或電子郵件認證。

(三) 安全設計符合下列要求者，為低信賴等級機制：

1、身分登錄：應於臨櫃辦理、採用低信賴等級機制以上之安全設計、依信用卡業務機構管理辦法核發信用卡或依據第三類數位存款帳戶開戶程序核驗身分後辦理。

2、身分驗證：應遵循前目身分驗證相關要求。

3、信物管理：應遵循前目信物管理相關要求。

五、視訊會議

(一)安全設計符合下列要求者，為高信賴等級機制：

1、身分登錄：不適用。

2、身分驗證：

(1)應留存政府核發用於身分識別之證件(如國民身分證、居留證或護照等)影像檔並進行驗證；若客戶係本國籍未成年人，應增加核驗其法定代理人之上述證明文件。

(2)應導入機制協助確認真人及本人，以防止透過科技預先錄製影片、製作面具、模擬影像或深度偽造(deepfake)等機制偽冒身分。

(3)應由金融機構人工確認客戶指示內容與其意思表示。

3、信物管理：

（1）VTM 之金融卡金庫（如提供現金提存功能者）、鍵盤、讀卡機及處理卡片交易時，應比照自動櫃員機之安全設計。

（2）VTM 應具備確認客戶本人申辦業務之舉證能力及方法（如照片、影像或聲音），並留存驗證紀錄與交易軌跡，遇有爭議時則可調閱相關紀錄。

（3）VTM 應具備身分證相關規範辨識要項進行辨識之模組並能協助辨識身分證明文件以利判斷真偽，其中應能檢視國民身分證防偽特徵，惟排除手觸(壓凸觸摸圖形)及翻轉(折光變色油墨)兩項防偽設計。

（4）VTM 應能檢視環境，並提供即時檢視現場影像及收音，輔助後台人員觀察有無異常舉止或遭脅迫。

（5）VTM 應直接連結金融機構內部網路並建置必要防護措施（如防火牆、防毒偵測、入侵偵測等），並關閉不必要服務。

（6）VTM 如產製或存取晶片金融卡或簽帳金融卡，應遵循下列要求：

甲、 卡片發卡、個人化或金鑰管理，其金鑰應儲存於經第三方認證(至少符合 FIPS 140-2 Level 3 或同等規格以上)之硬體安全模組；如放置於無人看管處應增加保全 24 小時監控。

乙、 應具備卡片沒收裝置。

(二)安全設計符合下列要求者，為中信賴等級機制：

1、身分登錄：不適用。

2、身分驗證：應遵循前目身分驗證相關要求。

3、信物管理：

（1）採用客戶行動裝置者，應符合「金融機構提供行動裝置應用程式作業規範」，採用客戶端其他設備者，應符合本規範相關要求。

（2）採用銀行提供裝置者(如平板、電腦、行動裝置)，應符合「金融機構資通安全防護基準」。

六、知識詢問，安全設計符合下列要求者，為最低信賴等級機制：

（一）身分登錄：不適用。

（二）身分驗證：應核驗客戶所知悉之靜態資訊(如國小就讀學校)或動態資訊(如前次繳款紀錄)。

（三）信物管理：不適用。

七、固定密碼，安全設計符合下列要求者，為最低信賴等級機制：

(一) 身分登錄：應於臨櫃辦理、採用最低信賴等級機制以上之安全設計或依據數位存款帳戶開戶程序核驗身分後辦理。

(二) 身分驗證：

1、應核驗與客戶所約定之密碼。

2、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：

(1)用戶代號之安全設計：

甲、不得使用客戶之顯性資料(如個人統一編號、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。

乙、不應少於六位。

丙、不應訂為相同之英數字、連續英文字或連號數字。

丁、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。

戊、如增設使用者代號，至少應依下列方式辦理：

(甲)不得為金融機構已知之客戶顯性資料。

(乙)如輸入錯誤達五次，金融機構應做妥善處理。

(丙)新建立時不得相同於用戶代號及密碼；變更時，亦同。

(丁)變更時得核驗原使用者代號後辦理且不得與原使用者代號相同。

(2)固定密碼之安全設計：

甲、不應少於六位，若搭配交易密碼使用則不應少於四位且交易密碼應符合本目相關規定。

乙、建議採英數字混合使用，且宜包含大小寫英文字母或符號。

丙、不應訂為相同之英數字、連續英文字或連號數字，系統預設密碼不在此限。

丁、不應與用戶代號、使用者代號、交易密碼相同。

戊、密碼連續錯誤達五次，不得再繼續執行交易。

己、變更時得核驗原密碼後辦理且不得與原密碼相同。

庚、首次登入時，應強制變更系統預設密碼；若未於30日內變更者，則不得再以該密碼執行簽入。

辛、密碼超過一年未變更，金融機構應做妥善處理。

(3)採用圖形鎖或手勢之安全設計：

甲、連續錯誤達五次，不得再繼續執行交易。

乙、變更不得與原設定相同。

3、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，其固定密碼之安全設計，應遵循前子目身分驗證相關要求，惟密碼長度不應少於四位。

(三)信物管理：應用於電子轉帳交易指示類並以簡訊傳送一次性密碼重新設定固定密碼者，應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)，該機制應排除固定密碼或電子郵件認證。

八、存款帳戶，安全設計符合下列要求者，為低信賴等級機制：

(一)身分登錄：不適用。

(二)身分驗證：

1、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。

2、驗證他行存款帳戶有效性時，應採用符合財金公司之「跨行金融帳戶資訊核驗」機制辦理，以有卡方式核驗者應驗證晶片金融卡交易驗證碼，以無卡方式核驗者應發送簡訊或推播驗證一次性密碼。

(三)信物管理：不適用。

九、信用卡，安全設計符合下列要求者，為最低信賴等級機制：

(一)身分登錄：不適用。

(二)身分驗證：

1、確認申請人與信用卡持卡人為同一個人統一編號且係透過信用卡授權交易方式，以確認該卡片之有效性(如預授權)。

2、驗證他行信用卡有效性時，應透過聯合信用卡處理中心及財金公司之「信用卡輔助持卡人身分驗證平臺」辦理。

(三)信物管理：不適用。

十、電信認證，安全設計符合下列要求者，為最低信賴等級機制：

(一) 身分登錄：不適用。

(二) 身分驗證：確認申請人與該門號租用人為同一個人統一編號且係透過用戶身分模組（Subscriber Identity Module，SIM）連線至該電信業者，確認該 SIM 之有效性。

(三) 信物管理：應要求電信業者或電信認證服務提供者遵循下列事項：

1、 應為客戶至電信業者直營門市臨櫃申辦，交付國民身分證及具辨識力之第二身分證明文件並完成親簽後申辦之門號，且應排除儲值卡、親子卡、預付卡、企業卡、委託代辦等無法辨識本人親辦親簽之門號。

2、 如自電信業者取得門號相關個人資料(如姓名、住址、電話、電子郵箱、繳款紀錄、電信評分等)者，金融機構應要求電信業者或電信認證服務提供者須取得門號租用人個資提供第三人之同意，金融機構亦需向客戶取得個資蒐集、處理及利用之同意。

第八條　交易類別安全設計

一、「非電子轉帳及交易指示類」：辦理帳務類、個人資料類之查詢應採用第七條第一款至第三款之任一款、第七條第四款之任一項技術、第七條第五款至第七款之任一款安全設計進行身分確認。

二、「電子轉帳及交易指示類」之交易指示：採用第七條第一款第一目安全設計進行身分確認者得辦理高風險交易；採用第七條第一款第一目、第一款第三目、第二款第一目或第三款第一目之任一目安全設計進行身分確認者得辦理法人高風險交易；採用第七條第一款第一目、第七條第一款第三目、第二款至第七款之任一款安全設計進行身分確認者得辦理低風險交易，但辦理下列低風險交易業務，應遵循下列要求：

(一) 辦理「ATM 存提款服務」應遵循下列要求：

1、 辦理ＡＴＭ無卡提款業務，於申請時應採用第七條第一款第一目憑證簽章、第二款該帳戶之晶片金融卡、第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』進行身分確認，於交易時應採用第七條第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』之任一款安全設計進行身分確認」，其提款金額應符合第八條第二款第四目第二子目低風險交易之限額規定，且與晶片金融卡之提款限額併計。

2、 個人辦理實體ＡＴＭ轉帳業務，每筆達等值新臺幣一萬元(含)以上時，應以簡訊、APP 推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。

(二) 辦理「限定性繳稅費」應遵循下列要求：

1、 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七條各款安全設計；惟金融機構應以簡訊、APP 推播、電子郵件或其他方式通知，以利客戶事後覆核。

2、 進行消費扣款之入帳帳戶，事業單位應指定一用於款項收取作業之活期性存款帳戶，客戶無需輸入該存款帳戶以避免遭竄改，另以行動 APP 進行每筆達等值新臺幣五千元以上之消費扣款時，應以簡訊、APP 推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。

3、 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七條第一款第一目、第二款至第四款之任一款安全設計進行客戶身分確認。

4、 金融機構接受事業單位或其他金融機構發動扣款約定或交易指示時，應依據第五條訊息處理方式辦理。

5、 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十四日內返還帳款，客戶應配合協助後續調查作業。

（三）辦理「結構型商品交易」應遵循下列要求：

1、 交易及扣款帳戶以同一統一編號為限。

2、 限非首次辦理之同類型結構型商品交易。

3、 金融機構應提供交易內容供客戶確認，並考量電子交易風險承受度，單筆交易超過等值新臺幣一仟萬、每日累計交易金額超過等值新臺幣三仟萬以上之交易應採用第七條第一款第一目憑證簽章進行客戶身分確認，以防止交易糾紛。

4、 金融機構應留存客戶辦理交易指示及確認風險揭露相關紀錄（如:日期、同意內容或版本及身分驗證結果等）。

（四）辦理「非約定轉入帳戶」應遵循下列要求：

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，其交易限額同前一子目要求。

4、非約定轉帳交易每筆應採用第七條第一款第一目、第二款至第四款之任一安全設計進行身分確認。若採用之技術防護措施（如憑證簽章、晶片金融卡、非簡訊傳送之一次性密碼、視訊會議、第三人覆核、簡訊簡碼回傳、直接人臉辨識軌跡等、或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級），提供客戶確認該筆交易內容並能防止身分確認資料與交易內容被竄改者，該筆非約定轉入帳戶之轉帳限額，可由個別金融機構視風險承擔之能力斟酌予以適當提高，最高該轉出帳號不超過當日累計等值新臺幣三佰萬元為限，並留存該技術評估紀錄。

5、若經客戶事先以臨櫃或視訊會議申請指定照會人員且由金融機構人工確認其指定人員之身分與指示內容者(如電話照會)，其交易限額由雙方依據風險承受度約定之。

（五）辦理依信託契約約定之信託財產運用範圍申請「非約定轉入帳戶之付款指示」，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，如超過限額不得以高風險交易方式辦理。

（六）採用第七條第六款知識詢問或第七條第七款固定密碼之安全設計時，僅限應用於辦理非電子轉帳及交易指示類及下列電子轉帳及交易指示類之業務：

1、存款業務

（1）約定轉入帳戶轉帳。

（2）概括約定繳稅費之扣退款。

（3）限定性繳稅費之扣退款與設定(如基金定期定額、信用卡繳款)。

（4）同一統一編號帳戶間轉帳、定存或投資。

2、授信業務(新戶除外)。

3、信用卡業務（新戶除外）。

4、財富管理業務

（1）非首次之認識客戶作業。

（2）非首次之客戶風險承受度測驗。

（3）衍商辦法結構型商品業務之同意推介或終止推介、同意成為專業客戶、專業客戶聲明已充分審閱而無須適用審閱期。

5、信託業務

（1）非首次之認識客戶作業。

（2）非首次之客戶風險承受度測驗。

(３)同意信託業務之推介或終止推介。

(４)同意簽署為專業投資人。

(５)專業投資人聲明表示已充分審閱而無須適用審閱期之規定。

(６)依信託契約約定之信託財產運用範圍，為申請運用指示：

甲、同一統一編號帳戶間轉帳、定存或投資(含交易取消)。

乙、辦理約定轉入帳戶之付款。

丙、受益人行使表決權。

(７)依信託契約約定由委託人或信託監察人行使同意權。

６、共同行銷業務。

７、不涉及帳務通知或交易指示之個人資料異動。

８、協助電子支付機構確認客戶身分。

三、「電子轉帳及交易指示類」之申請指示

(一)辦理存款業務應採用第七條第一款第一目、第一款第二目、第一款第四目、第二款至第七款之任一款安全設計，但辦理下列業務，應遵循下列要求：

１、臨櫃開立存款帳戶之存戶得線上首次申請晶片金融卡並親赴銀行櫃檯確認身分後辦理領卡。

２、辦理已持有晶片金融卡舊戶申請補換發晶片金融卡者應採用下列任一方式之安全設計：

(１)客戶應先登入網路銀行、行動銀行或網路 ATM 並採用第七條第三款一次性密碼或第四款「兩項以上技術」之安全設計進行身分確認、再郵寄至原留存通訊住址，客戶啟用新卡方式須透過該銀行 ATM 以舊卡並以系統驗證新舊卡內帳戶號碼係為一致或採多功能視訊櫃檯(VTM)或以視訊會議核驗身分方式辦理，其中採用視訊會議者，應搭配第七條第一款、第三款、第四款之任一款安全設計進行身分確認，惟排除第三款之軟體 OTP 或透過簡訊傳送 OTP 之安全設計。(如有一晶片金融卡設定多個帳戶號碼之情形，應以該卡片之主要帳戶號碼做驗證。)

(２)適用高風險交易之第一類數位存款帳戶，須採用高信賴等級以上之安全機制。

(３)適用低風險交易之第一類數位存款帳戶、第二類數位存款帳戶，須採用中信賴等級以上之安全機制。

（4）第三類數位存款帳戶採用低信賴等級以上之安全機制，惟排除第七條第三款軟體 OTP 或透過簡訊傳送 OTP 之安全設計。

3、受理已開戶之客戶辦理申請網路銀行或晶片金融卡之非約定轉帳功能應採用第七條第一款第一目、第二款至第五款任一安全設計進行身分確認，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計。

4、辦理申請約定非同一統一編號之約定轉入帳戶，須透過線上逐筆採用第七條第一款第一目、第二款至第五款任一安全設計進行身分確認，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計，並應遵循下列要求：

（1）首次設定非同一統一編號帳戶者須先經臨櫃或採用第七條第五款視訊會議確認身分後方可為之。

（2）電話語音或網路銀行之新約定帳戶應於申辦日後次一日始生效，惟同一統一編號帳戶經評估並無遭詐騙損失之虞者除外。

（3）約定轉入帳戶之設定，其交易限額同第八條第二款第四目之2要求，若配合採用各種嚴密之技術防護措施，提供客戶確認設定內容並能防止或偵測設定內容被竄改，其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。

5、依據第七條第十款電信認證辦理開立第三類數位存款帳戶時需搭配第七條第五款視訊會議安全設計查驗本人並核對證件照片，另應確認門號使用電信業者服務已超過半年且近 6 個月內繳款正常並沒有停話紀錄。

6、透過 VTM 辦理開立新臺幣活期及定期存款帳戶業務應採用第七條第五款視訊會議安全設計並遵循下列要求：

（1）依臨櫃存款開戶相關規定辦理。

（2）限具本國國籍成年自然人親自辦理。

（3）開立之存款帳號，應有相關區別機制。

（4）相關開戶及印鑑卡等業務書件親自簽名。

（5）開戶視訊過程進行錄音及錄影，並至少留存六個月，其他交易文件保存期限則依各業務相關規範辦理。

（6）開戶初期設計有別於一般臨櫃開立帳戶之管控方式(如交易功能、金額)。

（7）客戶輸入基本資料時，即時檢核客戶是否為高風險客戶，俾引導至臨櫃辦理。

(８)VTM 提供蒐集、處理及利用個人資料告知事項內容，供客戶審閱及確認等功能，並具備檢核機制。

(９)帳戶交易持續加強各項疑似洗錢或資恐交易表徵之監控。

７、辦理晶片金融卡密碼解鎖作業，應採用第七條第一款第一目、第二款至第三款任一款安全設計，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計及下列情境，且應於發卡行之端末設備(如 ATM、POS、VTM 等)進行，並針對解鎖用之機敏資訊應依據第五條訊息處理方式進行端點對端點加密防護。

(１)以數位存款帳戶之安全設計解鎖臨櫃帳戶之晶片金融卡。

(２)以第三類數位存款帳戶之安全設計解鎖第一類或第二類數位存款帳戶之晶片金融卡。

(３)以適用第六條低風險交易之第一類數位存款帳戶或第二類數位存款帳戶之安全設計解鎖第一類(不含限適用第六條低風險交易)數位存款帳戶之晶片金融卡。

(二)辦理個人授信業務應採用第七條第一款至第七款之任一安全設計，但辦理下列業務，應遵循下列要求：

１、辦理本行個人新戶(含借款人及保證人)同意金融機構查詢聯徵中心信用資料(申請階段)，應採用第七條第一款憑證簽章之安全設計，但如為他行既有非數位存款客戶，得採用下列任一方式之安全設計：

(１)採用第七條第一款憑證簽章之安全設計。

(２)採用第七條第五款視訊會議之安全設計，上傳身分證影像檔或透過 MyData 平台取得身分證電子檔，並搭配第七條第二款非數位存款帳戶晶片金融卡進行身分確認。

(３)採用第七條第八款存款帳戶之安全設計並上傳身分證影像檔或透過 MyData 平台取得身分證電子檔，其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送。

(４)採用第七條第十款電信認證之安全設計，上傳身分證影像檔或透過 MyData 平台取得身分證電子檔，並搭配第七條第五款視訊會議或第八款存款帳戶之財金公司之「跨行金融帳戶資訊核驗」進行身分確認，並視風險評估決定是否強化控管措施(如：確認門號使用電信

業者服務已超過半年且近 6 個月內繳款正常並沒有停話紀錄等)。

2、辦理本行個人既有數位存款帳戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：

(1)本行既有第一類(不含限適用第六條低風險交易)數位存款帳戶或第二類數位存款帳戶者，應採用第七條第一款至第七款之任一安全設計方式辦理簽約對保。

(2)本行既有適用第六條低風險交易之第一類數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計：

甲、採用第七條第一款第一目或第二目憑證簽章辦理簽約對保。

乙、採用第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配第七條第六款知識詢問或上傳身分證影像檔或透過 MyData 平台取得身分證電子檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位帳戶。

丙、採用第七條第四款包含生物特徵之「兩項以上技術」搭配第七條第一款第四目 C3 憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。

(3)本行既有第三類數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計：

甲、採用第七條第一款第一目或第二目之憑證簽章安全設計。

乙、採用第七條第五款視訊會議辦理簽約對保者，限將款項撥入本人非數位帳戶。

丙、採用第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配第七條第六款知識詢問或上傳身分證影像檔或透過 MyData 平台取得身分證電子檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位帳戶。

丁、採用第七條第四款包含生物特徵之「兩項以上技術」搭配第七條第一款第四目 C3 憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人帳戶，並視貸款金額大小、貸款撥入帳戶為

實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。

（４）本行既有第三類數位存款帳戶，經確認資金使用於特定目的用途且借款人同意貸款款項直接撥入第三方公司之實體帳戶者，如採第七條第四款包含生物特徵之「兩項以上技術」及第七條第一款第一目或第二目憑證簽章辦理簽約對保者，得將款項撥入他行第三方公司之實體帳戶。

３、辦理本行個人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：

（１）採用第七條第一款憑證簽章及第七條第五款視訊會議。

（２）採用第七條第三款一次性密碼，得將款項撥入本人非數位帳戶、第一類(不含限適用第六條低風險交易)數位存款帳戶或第二類數位存款帳戶。

（３）採用第七條第三款一次性密碼及第七條第五款視訊會議，得將款項撥入本人適用第六條低風險交易之第一類數位存款帳戶及第三類數位存款帳戶。

（４）採用第七條第四款包含生物特徵之「兩項以上技術」，得將款項撥入本人非數位帳戶、第一類(不含限適用第六條低風險交易)數位存款帳戶或第二類數位存款帳戶。

（５）採用第七條第四款包含生物特徵之「兩項以上技術」搭配第七條第一款第四目 C3 憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。

（６）依「長期使用循環信用持卡人轉換機制」申辦信用貸款方案者，採用第七條第一款至第七款之任一款安全設計。

４、辦理本行個人新戶之貸款契約或保證人保證契約成立，簽約對保方式應採用下列任一方式之安全設計：

（１）採用第七條第一款第一目或第二目憑證簽章之安全設計，得將款項撥入本人帳戶。

（２）採用第七條第八款存款帳戶之安全設計並上傳身分證影像檔、透過 MyData 平台取得身分證電子檔或查詢身分證領/補/換資料(限於申請階段已上傳身分證影像檔

或透過 MyData 平台取得身分證電子檔者)，且其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送，得將款項撥入本人帳戶。

(３)採用第七條第十款電信認證之安全設計者，上傳身分證影像檔、透過 MyData 平台取得身分證電子檔或查詢身分證領/補/換資料(限於申請階段已上傳身分證影像檔或透過 MyData 平台取得身分證電子檔者)，且限將款項撥入本人非數位帳戶，並視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近 6 個月內繳款正常並沒有停話紀錄、人工照會)。

５、辦理個人購屋貸款依「個人購屋貸款定型化契約應記載事項」第十三條及個人購車貸款依「個人購車貸款定型化契約應記載事項」第十二條（擔保物權連結條款）借款人或第三人提供擔保物設定抵押權予金融機構時，該抵押權擔保範圍僅限本貸款契約之債務，借款人因未來需求，需經擔保物提供人另以書面同意時，應採用第七條第一款第一目或第二目憑證簽章之安全設計。

(三)辦理法人授信業務應遵循下列要求：

１、辦理本行既有法人客戶及法人新戶同意金融機構查詢聯徵中心信用資料，應採用下列安全設計機制：

(１)採用第七條第一款第一目或第二目憑證簽章之安全設計。

(２)法人戶之負責人或保證人或依信保基金規定應查詢之關係人(如配偶)同意金融機構查詢聯徵中心信用資料之安全設計，應比照個人授信案件有關本行新戶同意金融機構查詢聯徵中心信用資料之安全設計。

２、辦理本行既有法人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：

(１)採用第七條第一款第一目或第二目憑證簽章之安全設計。

(２)透過本行法人戶申請平台驗證檢核既有客戶事先以授權書方式授權原留存印鑑之安全設計。上述檢核流程應透過公司負責人進行線上身分驗證後傳送印鑑，公司負責人身分驗證須依第八條第三款第二目第一子目個人貸款身分確認機制，相關檢核及驗證軌跡、紀錄等應比照第八條第六款規定辦理。

3、辦理3位以下本國籍自然人股東之法人新戶(不包括有法人股東之公司)之貸款契約成立，簽約對保方式應採用第七條第一款第一目或第二目憑證簽章之安全設計。

4、辦理法人戶之負責人或保證人契約成立之簽約對保方式，應採用下列任一方式之安全設計：

(1)採用第七條第一款第一目或第二目憑證簽章之安全設計。

(2)採用第七條第五款視訊會議，並搭配第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」。

(3)採用第七條第二款晶片金融卡之高信賴等級以上，或採用第七條第二款晶片金融卡之中、低信賴等級並搭配「第七條第五款視訊會議」之安全設計。

(4)採用第七條第四款兩項以上技術之高信賴等級以上，或採用第七條第四款兩項以上技術之中、低信賴等級並搭配「第七條第五款視訊會議」之安全設計。

5、法人戶徵授信相關文件之上傳，應採用法人戶及其負責人貸款契約成立之安全設計機制。

(四)信用卡業務除辦理新戶申辦信用卡業務應採用第七條第一款第一目、第一款第二目、第一款第四目、第八款、第九款或第十款之任一安全設計，其中採用第十款電信認證者，應視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內繳款正常並沒有停話紀錄、人工照會)；辦理其他信用卡業務應採用第七條第一款至第七款之任一款安全設計。

(五)辦理財富管理業務應採用第七條第一款至第七款之任一款安全設計，但本基準另有限制者，從其規定。

(六)辦理信託業務應採用第七條第一款至第七款之任一款安全設計，但本基準另有限制者，從其規定。

四、首次辦理電子轉帳及交易指示類低風險交易之服務者應與資安、法遵及風控等單位(以下簡稱二道防線)建立各部門間之連繫機制、確認相關作業符合本基準及相關定型化契約等相關法令規定，留存驗證軌跡及建立各部門建議事項追蹤控管機制後，若合規即可開辦，並於開辦後六個月內重新檢視並作成報告交由二道防線確認。內部稽核單位應依據交易量與金額等評估新種業務之風險，排定內部稽核計畫辦理查核，並對評估風險偏高者適時辦理專案查核，以落實內部控制三道防線之運作；惟經主管機關核准採行風險導向內部稽核制度之金融機構，其內部稽核單位應將新種業務納入年度風險評估範圍，並就風險評估結果為高風險者列入次年度查核項目。

五、金融機構委由第三方辦理第七條第二款至第七款介面安全設計者僅限應用於「非電子轉帳及交易指示類」或「電子轉帳及交易指示類」之低風險交易，其驗證方式應符合上述安全規定並得與第三方以契約約定雙方權利義務關係及賠償責任。

六、應用於信用卡申辦或貸款申請時，系統應留存足以證明客戶意思表示同意金融機構查詢聯徵中心信用資料之紀錄(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)，且相關紀錄內容可完整呈現供日後查驗。

第九條　應用系統安全設計：

一、提供網際網路應用系統，應遵循下列要求：

(一)載具密碼不應於網際網路上傳輸。

(二)應設計連線(Session)控制及網頁逾時(TimeOut)中斷機制，客戶超過十分鐘未使用應中斷其連線或採取其他保護措施。

(三)應辨識合作第三方網站或應用系統傳送之訊息，確保訊息隱密、訊息完整、來源辨識及不可重複並要求妥善保護客戶資料。

(四)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，得不執行本措施。

(五)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。

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

(七)採用固定密碼進行網路銀行身分確認者，應加強下列安全機制：

1、採用適當保護機制，防止未經銀行同意以模擬瀏覽器(如 WebView、WebBrowser 等)方式竊取身分核驗資訊或機敏資訊(如不支援模擬瀏覽器、網頁程式動態變化或 App 外開指定瀏覽器等)。

2、確定為客戶行為(如於登入成功及失敗均及時通知客戶、採用圖形驗證碼經人工確認、搭配風險評估增加額外認證等)。

(八)應提供客戶安全教育宣導，強化風險認知與交易確認。

二、提供客戶端電腦應用程式，應遵循下列要求：

(一)可執行程式(如 EXE,COM 等)應採用被作業系統認可之數位憑證進行程式碼簽章(CodeSign) 且安裝過程不應出現憑證相關安全警告。

(二)執行時應先驗證網站正確性。

(三)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。

(四)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，得不執行本措施。

三、透過 QR Code 進行資料傳輸，應遵循下列要求：

（一）QR Code 表示的資料應為辦理該業務所需最小化為原則。

（二）應用於電子轉帳及交易指示類時，應依其業務屬性設計合理使用時效，且在時效內以使用一次為限。

（三）所產生之 QR Code，如具客戶個人資料應符合訊息隱密性、如應用於電子轉帳及交易指示類時，應符合訊息完整性、訊息來源辨識性與訊息不可重複性。

（四）應針對解析 QR Code 後進行格式檢查，如為網站連接應進行網站合法性檢查。

四、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」。

第十條　端末設備安全設計

一、自動櫃員機

（一）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。

（二）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。

（三）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

（四）自動櫃員機應具備 H/W DES 亂碼化裝置(Triple DES)。

（五）自動櫃員機應具備斷電卡片自動退出裝置。

（六）自動櫃員機應具備卡片沒收裝置。

（七）自動櫃員機應具備標準通訊介面。

（八）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。

(九)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。

二、實體卡片銷售端末設備

(一)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。

(二)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碼，並檢核資料之正確性與有效性。

(三)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。

(四)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。

(五)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。

(六)應與商家訂立檢核契約。

第十一條　其他

一、電子銀行業務倘與第三方(含金控及其子公司)進行資料傳輸或服務委外時，除應符合訊息來源辨識外，簽訂相關契約，明訂其須符合本基準之相關規定及雙方責任。

二、本基準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。