金融機構辦理快速身分識別機制安全控管作業指引

指引內容	說明
第一點 為強化金融機構或其所屬公會(以下合稱金融機構)辦理跨機構間之客戶快速身分識別機制(以下簡稱金融FIDO)之安全控管，並有一致性之作業準則，特訂定本指引。 金融機構辦理金融FIDO，應依各金融業業務試辦作業要點向金融監督管理委員會(下稱金管會)申請業務試辦，除應符合金管會、金融機構所屬公會及周邊單位相關規定外，應依本指引辦理。 金融機構辦理同業別跨機構間之客戶快速身分識別機制，已依各業別業務試辦作業要點經金管會核准試辦並另為規範者，得不適用本指引。 第二項所稱金融機構所屬公會及周邊單位，詳附表一。	一、本指引訂定目的。 二、金融機構或其所屬公會於辦理跨機構快速身分識別機制時，應依各金融業業務試辦作業要點向金管會申請業務試辦，除應符合金管會、金融機構所屬公會及周邊單位相關規定外，應依本指引辦理。 三、現行銀行業、證券期貨業及保險業已分別訂有各業申請業務試辦作業要點，爰對於同業別間僅為跨機構之試辦案件，已依前開各業務試辦作業要點經金管會核准試辦並另為規範者，得不適用本指引。
第二點 本指引用詞定義如下： 一、快速身分識別機制：指金融機構依據國際Fast IDentity Online標準(以下簡稱FIDO標準)提供客戶身分識別服務，並由身分識別服務提供者、身分識別服務信賴者、身分核驗者等角色共同運作。各角色應由金融機構擔任，其任務如下： (一)身分識別服務提供者(Identity Provider(IDP)；以下簡稱服務提供者)：依據FIDO標準及本指引提供跨機構間之客戶快速身分識別服務。 (二)身分識別服務信賴者(Relying Party(RP)；以下簡稱服務信賴者)：應用金融FIDO進行身分識別以提供客戶線上服務。 (三)身分核驗者：負責核驗客戶身分，並得透過金融資訊服務事業、票據交換所平台進行跨行核驗。 二、金融FIDO平臺：指辦理快速身分識別機制相關作業之應用軟體、	一、明定本指引之用詞定義。 二、第一款說明身分識別服務機制之定義及運作身分識別服務機制之角色任務，並明定各角色應由金融機構或其所屬公會擔任。 三、第一款第一目服務提供者係指FIDO Server，第二目服務信賴者係指提供客戶透過FIDO驗證進行金融服務之金融機構；第三目明定身分核驗者得透過金融資訊服務事業、票據交換所平台進行客戶身分跨行核驗。 四、第八款明定網路型態區分。 五、第十一款及第十二款明定各業可適用業務項目/服務請詳附表二，其中附表二係由金管會創新中心彙整各業務局意見提供；另因「保險業辦理電子商務應注意事項」刻研議將金融FIDO納入現行身分驗證作業範圍，保險業電子商務業務使用金融FIDO進行身分核驗者，可逕行參照該注意事項辦理。

系統軟體及其硬體設備。 三、金融FIDO作業環境：指金融FIDO平臺及用於管理或防護金融FIDO平臺及其系統維運人員之應用軟體、系統軟體及其硬體設備。 四、系統維運人員：指金融FIDO平臺之作業人員，負責管理或操作營運環境之應用軟體、系統軟體、硬體、網路、資料庫、客戶服務、業務推廣、帳務管理或會計管理等作業。 五、接觸式介面：指使用裝置內的探針以物理方式接觸另一設備(如卡片)，進行資料交換。 六、非接觸式介面：指使用裝置內的感應設備(如NFC近場通訊、藍芽等)以非接觸方式靠近另一設備(如卡片)，進行資料交換。 七、行動裝置：指包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。 八、網路型態區分如下： （一）專屬網路：指利用電子設備或通訊設備直接以連線方式（撥接（Dial-Up）、專線（Leased-Line）或虛擬私有網路（Virtual Private Network；VPN）等）進行訊息傳輸。 （二）網際網路（Internet）：指利用電子設備或通訊設備，透過網際網路服務業者進行訊息傳輸。 （三）行動網路：指利用電子設備或通訊設備，透過電信服務業者行動通信服務進行訊息傳輸。 九、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、常用密碼學演算法如下: (一)對稱性加解密演算法:指三重資料加密標準(Triple DES;以下簡稱 3DES)、進階資料加密標準(Advanced Encryption Standard;以下簡稱 AES)。 (二)非對稱性加解密演算法:指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)。 (三)雜湊函數:指安全雜湊演算法(Secure Hash Algorithm;以下簡稱 SHA)。 十一、申請指示類業務:係指線上開戶、銷戶;查詢帳務及個人資料;申辦、授權同意;線上變更資料;交易額度調整等業務,各業可適用業務項目/服務等請詳附表二。 十二、交易指示類業務:係指客戶交易指示(如轉帳交易等);證券、期貨下單登入;交割專戶分戶帳戶款項、保證金專戶出金;行動投	

保等業務，各業可適用業務項目/服務等請詳附表二。 十三、個人資料：指個人資料保護法第二條第一款規定之資料。 十四、機敏資料：指包含但不限於個人資料、身分驗證資料(如密碼)或個人化資料(如註冊檔)等。 十五、評估單位：指具備資訊安全管理知識(如CISM、ISO 27001LA等)、資訊安全技術能力(如CISSP)、模擬駭客攻擊能力(如CEH、CIH等)及熟悉金融領域載具應用、系統開發或稽核經驗(如CISA)之外部專業機構或金融機構內部之個人或團隊。	
第三點 金融機構於客戶首次申請金融FIDO前，應先進行身分核驗。 金融機構辦理客戶身分核驗，應採用下列任一款安全設計： 一、客戶臨櫃核驗身分，其安全設計應符合下列要求： (一)辨識客戶與其所持之身分證明文件相符。 (二)留存影像。 (三)留存客戶意思表示之確認(如印鑑、簽名、電子簽名或生物辨識等)。 二、客戶使用晶片自然人憑證核驗身分，其安全設計應符合下列要求： (一)應確認憑證之正確性、有效性。 (二)應採用接觸式介面存取，以避免資料外洩，如具有存取控制(如密碼)者，得採用非接觸式介面存取。 三、客戶使用晶片金融卡核驗身分，該卡限經臨櫃申請開戶或經線上申請第一類高風險數位存款帳戶後取得者，其安全設計應符合下列要求： (一)應先由原發卡行驗證交易驗證碼。	一、明定身分核驗之安全設計原則。 二、第二項第一款明定臨櫃作業要求。 三、第二項第二款明定自然人憑證安全設計要求且限使用晶片載具之自然人憑證。 四、第二項第三款明定晶片金融卡安全設計要求，其中第一類高風險數位存款帳戶係指以晶片自然人憑證加視訊開戶者。

（二）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及有效性。 （三）系統應每次輸入卡片密碼產生交易驗證碼。 （四）元件於存取卡片時應設計防止第三者存取。 （五）應提示客戶收回卡片妥善保管。 （六）應採用接觸式介面存取，以避免資料外洩，如具有存取控制(如密碼)者，得採用非接觸式介面存取。	
第四點 金融機構辦理客戶註冊、註銷、異動等作業，應依據FIDO標準符合下列安全規定： 一、註冊作業：客戶於同一設備且同一連線階段(session)下完成身分核驗後，並在該設備內進行生物特徵設定或綁定、產生FIDO金鑰對、私鑰妥善儲存於該設備內及公鑰儲存於FIDO伺服器，完成註冊作業。客戶如未能於同一設備且同一連線階段(session)下完成者，得將身分核驗結果產製一啟用碼，供客戶接續完成註冊作業。啟用碼應搭配如簡訊OTP或軟體OTP等機制再次核驗客戶身分，並訂定三天內之有效期限，且在期限內以使用一次為限。 二、註銷作業：應採用適當身分核驗方式後辦理註銷(如密碼、知識詢問)。 三、異動作業：應驗證有效之原金鑰或依第三點規定重新辦理身分核驗後異動。	一、明定註冊、註銷、異動等作業應採用之安全規定。 二、第一款明定註冊作業之安全規範。 三、第二款明定註銷FIDO服務之要求。 四、第三款明定更新FIDO金鑰對之安全要求。
第五點 金融機構進行FIDO驗證，對於不同交易類型，應依其不同應用範圍，採用下列安全設計：	一、明定FIDO應用於申請指示類業務、交易指示類業務時應採用之安全設計。

一、辦理申請指示類業務，應採用客戶所指定之設備及其生物特徵進行FIDO驗證，惟辦理非首次申請約定非同一統一編號之約定轉入帳戶時，應逐筆進行FIDO驗證。 二、辦理交易指示類業務，應採用客戶所指定之設備及其生物特徵進行FIDO驗證，惟辦理非約定轉帳交易時，應逐筆進行FIDO驗證。 各業別適用金融FIDO機制之相關業務及應採用之強化機制，詳附表二。	二、依金融機構辦理電子銀行業務安全控管作業基準規定，辦理申請約定非同一統一編號之約定轉入帳戶，須透過線上逐筆進行設定，惟首次設定時須先經臨櫃或視訊會議確認身分後方可為之，爰於本點第一項第一款及第二款明定非首次申請約定非同一統一編號之約定轉入帳戶，及辦理非約定轉帳交易時，應逐筆進行FIDO驗證。 三、現行各金融業辦理電子業務或服務所採用之安全設計，係分散規範於多項法規或自律規範，且現階段尚非所有電子業務均可適用金融FIDO，爰由金管會創新中心彙整各業務局意見提供附表二，明列各業別適用金融FIDO機制之業務範圍、適用金融FIDO時應採行之強化機制、現行法規採用之安全設計及其法規依據，俾利金融機構參照運用。
第六點 金融FIDO平臺之軟硬體設備間於不同網路型態進行訊息傳輸，應具備下列訊息安全設計： 一、專屬網路：應符合訊息完整性、訊息來源辨識性及訊息不可重複性之訊息防護措施。 二、網際網路或行動網路：應符合訊息隱密性、訊息完整性、訊息來源辨識性及訊息不可重複性之訊息防護措施。	一、明定不同網路型態下應具備之訊息安全設計。 二、鑒於專屬網路機制已具隱密性，爰未另列相關要求。
第七點 前點所稱訊息隱密性、訊息完整性、訊息來源辨識性及訊息不可重複性之安全設計，應符合下列要求： 一、訊息隱密性：應採用AES 128bits、RSA 2048bits、ECC 256bits以上或其他安全強度相同(含)以上之演算法進行加密運算，應採用TLS 1.2（含）以上之通訊協定並使用Elliptic Curve Diffie-Hellman Exchange方式進行金鑰交換。 二、訊息完整性：應採用SHA	一、明定前點所定各訊息安全設計之安全要求。 二、第一款明定訊息隱密性，應採用如AES 128bits等演算法進行加密運算。 三、第二款明定訊息完整性，應採用如SHA 256bits等演算法進行押碼或加密運算。 四、第三款明定訊息來源辨識性，應採用如RSA 2048bits等演算法進行押碼、加密運算或數位簽章。

256bits、AES 128bits、RSA 2048bits、ECC 256bits以上或其他安全強度相同(含)以上之演算法進行押碼或加密運算。 三、訊息來源辨識性：應採用SHA 256bits、AES 128bits、RSA 2048bits、ECC 256bits以上或其他安全強度相同(含)以上之演算法進行押碼、加密運算或數位簽章。 四、訊息不可重複性：應採用序號、一次性亂數、時間戳記等機制。 五、訊息不可否認性：應採用SHA256以上或其他安全強度相同（含）以上之演算法進行押碼，及採用RSA 2048bits、ECC 256bits以上或其他安全強度相同(含)以上之演算法進行數位簽章。	五、第四款明定訊息不可重複性，應採用如序號等方式進行運算。 六、第五款明定訊息不可否認性，應採用如SHA256及RSA 2048bits等演算法進行數位簽章。
第八點 金融FIDO平臺提供或使用下列應用系統或技術時，應符合下列設計要求： 一、網際網路應用系統： （一）機敏資料於網際網路傳輸時應全程加密。 （二）應設計連線控制及網頁逾時中斷機制，客戶超過十分鐘未使用應中斷其連線；使用同一連線並應用於交易指示類業務時，無須再次核驗身分，惟非約定轉帳除外。 （三）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。 （四）應設計個人資料顯示之隱碼機制。 （五）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。 二、客戶端電腦應用程式： （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	明定應用系統設計原則及相關安全要求。

出現憑證相關安全警告。 （二）執行時應先驗證連結的網站正確性。 （三）應避免儲存機敏資料，如有必要應採取加密或代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。 三、行動裝置應用程式： （一）於發布前檢視行動裝置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，應經資安、法遵及風控等單位同意，以利評估是否符合個人資料保護法之告知義務。 （二）應於官網上提供行動裝置應用程式之名稱、版本與下載位置。 （三）啟動行動裝置應用程式時，如偵測行動裝置疑似遭提權、越獄及破解，應提示客戶注意風險。 （四）應於顯著位置（如行動裝置應用程式下載頁面等）提示客戶於行動裝置上安裝防護軟體。 （五）採用憑證技術進行傳輸加密時，行動裝置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。 （六）採用 NFC、藍牙或QR Code技術進行傳輸資料時，應經由客戶人工確認(如密碼、圖形驗證碼)。 （七）應偵測客戶所指定設備之生物特徵，如發現有設定異動應及時通知客戶。 （八）每年應依據經濟部工業局制定之「行動應用 APP 基本資安檢測基準」辦理檢測並取得證書。 四、透過QR Code進行資料傳輸：	

（一）QR Code表示的資料應為辦理該業務所需最小化為原則。 （二）應用於申請指示類業務或交易指示類業務時，應設計合理使用時效，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、如應用於申請指示類業務或交易指示類業務時，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安全性檢查。	
第九點 金融機構之資訊安全政策、內部組織及資產管理應符合下列要求： 一、資訊安全政策應經董事會、常務董事會決議或經其授權之經理部門核定。但外國金融機構在臺分支機構、獨資企業或未設董（理）事會者，應由其負責人簽署。 二、前款資訊安全政策應對所有員工及相關外部各方公布與傳達。 三、應訂定資訊作業相關管理及操作規範。 四、第一款資訊安全政策及前款管理及操作規範應每年檢討修訂，並於發生重大變更（如新頒布法令法規）時審查，以持續確保其合宜性、適切性及有效性。 五、應依據金融FIDO平臺之作業流程，識別人員、表單、設備、軟體、系統等資產，建立資產清冊、作業流程、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確性。 六、應定義人員角色與責任並區隔相互衝突的角色。 七、應依據作業風險與專業能力選擇適當人員擔任其角色並定期提供必要教育訓練。	一、明定金融機構應建立資訊安全政策、訂定資訊作業相關管理及操作規範、清點人員與設備資產、定義人員角色與責任並提供教育訓練。 二、第四款明定每年檢討修訂或發生重大變更時，應檢討修訂資訊安全政策、資訊作業相關管理及操作規範。 三、第五款明定應依據金融FIDO平臺作業流程建立資產清冊，並維持其正確性。 四、第六款明定應從組織架構依據作業流程，定義人員角色與責任，藉以適當授權，避免權限過大。 五、第七款明定應定期提供適當教育訓練。

第十點 金融FIDO平臺之系統維運人員管理應符合下列要求： 一、應建立人員之註冊、異動及撤銷註冊程序，用以配置適當之存取權限，針對重要作業(如程式異動)應由另一位人員進行審核與放行。 二、應至少每年定期審查帳號與權限之合理性，人員離職或調職時應盡速移除權限，以符合職務分工與牽制原則。 三、硬體設備、應用軟體、系統軟體之最高權限帳號或具程式異動、參數變更權限之帳號應列冊保管；最高權限帳號使用時須先取得權責主管同意，並保留稽核軌跡。 四、應確認人員之身分與存取權限，辦理特定作業(如程式異動)必要時得限定其使用之機器與網路位置（IP）。 五、人員超過十分鐘未操作電腦時，應設定密碼啟動螢幕保護程式或登出系統。 六、除代登系統外，於登入作業系統進行系統異動或資料庫存取時，應留存人為操作紀錄(如檔案之新增/刪除/修改/複製/貼上/下載/上傳、資料庫查詢、服務啟動/中止等動作)，並於使用後儘速變更密碼；但因故無法變更密碼者，應建立監控機制，避免未授權變更，並於使用後覆核其操作紀錄。此人為操作紀錄應於使用後由另一人員進行覆核。 七、帳號應採一人一號管理，避免多人共用同一個帳號為原則，如有共用需求，申請與使用須有其他補強管控方式，並留存操作紀錄且應能區分人員身分。 八、採用固定密碼者，應定期變更密碼：提供人員使用之帳號至少三個月一次；提供系統連線之帳	一、明定金融FIDO平臺之人員管理。 二、第一款明定應建立人員清冊並配置適當權限，針對重要作業應由另一位人員進行審核與放行。 三、第二款明定應定期審查帳戶與權限之合理性。 四、第三款明定應針對如網路設備、資安設備、作業系統、應用軟體、資料庫等之最高權限帳號或具程式異動、參數變更權限之帳號留存稽核軌跡。 五、第四款明定應確認人員之身分與存取權限。 六、第五款明定為防止客戶個人資料外洩，人員離開時應限制畫面呈現。 七、第六款明定系統維運人員未直接登入應用系統，而是登入金融FIDO平臺之作業系統(如Windows,UNIX)進行系統異動或資料庫存取，仍應留存人為操作紀錄。此人為操作紀錄應於使用後由另一人員進行覆核。 八、第七款明定覆核共用帳號之操作紀錄時應能區分人員身分。 九、第八款明定應定期變更密碼。 十、第九款明定重要程式應限制人員存取與執行，防止密碼、金鑰及個人資料外洩。

號，至少每三個月一次或其他補強管控方式（如限制人工登入）。 九、加解密程式或具變更權限之公用程式（如資料庫存取程式）應列冊管理並限制使用，該程式應設定存取權限，防止未授權存取，並保留稽核軌跡。	
第十一點　金融FIDO作業環境之個人資料保護應符合下列要求： 一、為維護所保有個人資料之安全，應採取下列資料安全管理措施： (一)訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。 (二)針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。 (三)作業過程有備份個人資料之需要時，對備份資料予以適當保護。 二、保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施： (一)實施適宜之存取管制。 (二)訂定妥善保管媒介物之方式。 (三)依媒介物之特性及其環境，建置適當之保護設備或技術。 三、為維護所保有個人資料之安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務 。 四、應針對金融FIDO作業環境，包含資料庫、資料檔案、報表、文件、傳檔伺服器及個人電腦等進行清查盤點是否含有個人資料並	一、明定金融FIDO作業環境之個人資料保護，相關規定係參考「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」(以下簡稱個資檔案維護辦法)。 二、第一款參考個資檔案維護辦法第九條，明定資料安全管理措施。 三、第二款參考個資檔案維護辦法第十一條，明定個人資料儲存設備安全管理措施。 四、第三款參考個資檔案維護辦法第十二條，明定接觸個人資料人員之權限及控管。 五、第四款明定應就個人資料建立清冊、進行風險評估與控管。 六、第五款參考個資檔案維護辦法第十四條，並具體說明至少需留存內容，包含人/事/時/地/物。設計辨識機制(如浮水印)，以利事後追蹤個人資料使用狀況。 七、第六款規定資料外洩防護機制須可以偵測透過系統操作(如複製/貼上)將個人資料複製至網頁(如WebMail、網站留言等)或上傳至網路儲存空間，並留存軌跡與數位證據。 八、第七款參考個資檔案維護辦法第十四條，明定處理所保有之個人資料應留存紀錄。 九、第八款參考個資檔案維護辦法第十五條，明定個人資料管理單位或人員，應定期提出相關自我評估報告。

編製個人資料清冊，並進行風險評估與控管。 五、應建置留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況，包括檔案、螢幕畫面、列表。 六、應建立資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或網路檔案、或列印等方式傳輸，並應留存相關紀錄、軌跡與數位證據。 七、如刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： (一)刪除、停止處理或利用之方法、時間。 (二)將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。 八、為持續改善個人資料安全維護，其所屬個人資料管理單位或人員，應定期提出相關自我評估報告，並訂定下列機制： (一)檢視及修訂相關個人資料保護事項。 (二)針對評估報告中有違反法令之虞者，規劃、執行改善及預防措施。 九、前款自我評估報告，應經董（理）事會、常務董（理）事會決議或經其授權之經理部門核定。但外國金融機構在臺分支機構、獨資企業或未設董（理）事會者，應由其負責人簽署。	十、個資檔案維護辦法第十條相關要求已明定於本指引相關條文，說明如下： (一)客戶身分確認及保護機制，本指引第四點。 (二)個人資料顯示之隱碼機制，本指引第八點第一項第一款第四目。 (三)網際網路傳輸之安全加密機制，本指引第六點及第七點。 (四)軟體驗證與確認程序，本指引第十七點。 (五)檔案及資料庫之存取控制與保護監控措施，本指引第八點第一項第一款第五目。 (六)外部網路入侵對策，本指引第十五點及第二十點。 (七)異常使用行為之監控，本指引第十點、第十三點及第十六點。
第十二點 金融FIDO平臺之機敏資料隱密及金鑰管理，應符合下列要求： 一、如有下列情形者，應建立訊息隱	一、明定金融FIDO平臺之機敏資料隱密及金鑰管理原則。

密性機制： (一)機敏資料儲存於客戶端操作環境。 (二)機敏資料於網際網路上傳輸。 (三)客戶身分識別資料（如密碼、個人化資料）儲存於系統內，不得儲存生物特徵資料於系統中（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），並應遵循金融機構所屬公會所訂定之生物特徵相關自律規範辦理。 二、客戶身分識別資料如為固定密碼者，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，應進行加密保護或加入不可得知之資料運算；採用加密演算法者，其金鑰應儲存於硬體安全模組內並限制匯出功能。 三、採用硬體安全模組保護金鑰者，該金鑰應由非系統開發與維護單位（如客服、會計、業管等）之二個單位（含）以上產製並分持管理其產製之基碼單，另金鑰得以加密方式分持匯出至安全載具（如晶片卡）或備份至具存取權限控管之位置，供維護單位緊急使用。 四、應減少金鑰儲存的地點，並僅允許必要之管理人員存取金鑰，以利管理並降低金鑰外洩之可能性。 五、當金鑰使用期限將屆或有洩漏疑慮時，應進行金鑰替換。	二、第一款明定三種情形需採用符合第七點訊息隱密性之安全防護措施(如AES、RSA、ECC)。 三、第二款明定客戶之固定密碼於傳輸時須設計不可逆並加密或加入不可得知之資料運算，以防止取得不可逆資料後，透過大數據找出可用密碼。採用加密機制者須保護加密金鑰，以防止上述保護機制失效。採用不可得知的資料運算者，須確保其運算邏輯應妥善保管，防止未授權存取。 四、第三款明定應妥善產製並保護硬體安全模組之主金鑰。 五、第四款明定集中管理金鑰，避免過度分散。 六、第五款明定金鑰使用期限或有洩漏疑時應立即更換。
第十三點 金融FIDO平臺之實體安全應符合下列要求： 一、主機房與異地機房應避免同時在地震斷層帶、海岸線、山坡地、海平面下、機場飛航下、土石流好發區域、百年洪水氾濫區域、核災警戒範圍區域、工安高風險	一、明定金融FIDO平臺之實體安全要求。 二、第一項第一款參考行政院委託財團法人國家實驗研究院國家高速網路與計算中心制定之「我國電腦機房異地備援機制參考指引」，明定主

區域，並應有相關防護措施，以避免受到地震、海嘯、洪水、火災或其他天然或人為災難之損害。 二、營運設備應集中於機房內，機房應建立門禁管制，宜採用兩項以上身分確認，以確保僅允許經授權人員進出；非授權人員進出應填寫進出登記，並由內部人員陪同與監督；進出登記紀錄應定期審查，如有異常應適當處置。 三、應於主機房及異地機房內建立全天候監視設備並確保監視範圍無死角。 四、應有足夠營運使用之電力、供水、用油等供應措施，當發生供應措施中斷時，應至少維持七十二小時運作時間，並應介接二家以上或異地二線以上網際網路電信營運商互為備援。 五、油槽儲存及消防安全應符合相關法令法規，應設置全自動滅火系統，得設置極早期火災預警系統。 六、應設置環境監控機制，以管理電信、空調、電力、消防、門禁、監視及機房溫濕度等，並自動告警與通知；人員應於接獲通知後，盡速到達現場並採取適當措施。 七、機房管理應具備與機房相當之操作環境，或獨立可管制人員操作系統與設備之監控室。 前項第七款監控室應符合下列要求： 一、應具門禁與監視設備，且必須留存連線及使用軌跡，並定期稽核管理。 二、系統維運人員應經授權進入監控室使用監控室內專屬電腦設備；或應使用指定設備由內部網路以一次性密碼登入並經服務管控設備（如防火牆）使用監控室內專	機房與異地機房選址及相關防護措施。 三、第一項第二款明定應建立門禁管制，以確保僅允許經授權人員進出。 四、第一項第三款明定應確保主機房與異地機房各位置均包含於監視設備範圍內。 五、第一項第四款明定應能至少維持 72 小時運作；應有兩家或兩線以上網際網路服務。 六、第一項第五款明定應符合相關法令法規，以提供極早預警及自動滅火機制。 七、第一項第六款明定應設置環境監控系統並自動告警與通知。 八、第一項第七款及第二項明定機房管理及監控室之要求。

屬電腦設備。 三、連線過程須以內部網路、專線或虛擬私有網路進行。 四、監控室之網路設備與電腦設備如為金融FIDO作業環境之範圍，應符合本指引相關規定。	
第十四點 金融FIDO作業環境之營運管理應符合下列要求： 一、應避免於營運環境安裝程式原始碼。 二、應建立定期備份機制及備份清冊，備份媒體或檔案應妥善防護，確保資訊之可用性及防止未授權存取。 三、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。 四、相關留存紀錄應確保數位證據之蒐集、保護與適當管理程序，至少留存二年。 五、應訂定系統安全強化標準，建立並落實金融FIDO作業環境之系統安全設定。	一、明定金融FIDO作業環境之營運管理原則。 二、第一款明定應避免於營運環境安裝程式原始碼，除部分程式(如HTML, Script等)須提供程式原始碼外，其他程式應於營運環境上放置編譯後檔案。 三、第二款明定應建立備份機制。 四、第三款明定應建立回存測試機制，定期確認。 五、第四款明定留存本辦法之相關紀錄之要求，並確保數位證據之蒐集、保護與適當管理程序，至少留存二年。 六、第五款明定應建立並落實金融FIDO作業環境之系統安全設定，得參考我國GCB、PCI DSS、ISO 27001 機構等所提出之系統安全強化建議，訂定金融FIDO作業環境(含網路設備、資訊安全設備及系統維護人員電腦)之系統安全強化標準，並定期檢視。
第十五點 金融FIDO作業環境之脆弱性管理應符合下列要求： 一、應偵測網頁與程式異動，紀錄並通知相關人員處理。 二、應偵測惡意網站連結並定期更新惡意網站清單。 三、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。 四、應建立病毒偵測機制並定期更新病毒碼。 五、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。 六、應隨時掌握資安事件，針對高風險或重要項目立即進行清查與應	一、明定金融FIDO作業環境之脆弱性管理原則。 二、不論是系統維護人員或遭受外部攻擊，一旦發生FIDO平臺之網頁、參數、程式與服務異動，應能立即通知系統維護人員，爰於第一款明定應偵測網頁與程式異動，紀錄並通知相關人員處理；如為正常程序，應由另一位人員覆核其異動作業。 三、第二款至第四款明定應建立惡意網站、惡意程式、病毒偵測及防禦機制。 四、第五款明定應針對FIDO平臺與系統維護人員進行上網管制，以避免植入惡意程式。

變。 七、應針對系統維運人員定期執行電子郵件社交工程演練與教育訓練，至少每年一次。 八、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。 九、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。 十、金融FIDO平臺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。 十一、金融FIDO平臺每年應執行滲透測試，以加強資訊安全。	五、第六款明定應隨時掌握資安事件，評估該事件之影響並採取適當措施。 六、第七款明定應定期對系統維護人員進行社交工程演練。 七、第八款明定應針對金融FIDO作業環境進行弱點掃描，評估該弱點之影響並採取適當措施。 八、第九款明定避免採用已不再提供安全更新之作業系統與應用軟體，如需使用應導入必要防護措施(如白名單控管可執行程式)。 九、第十款明定金融FIDO平臺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，並進行後續風險評估。 十、第十一款明定金融FIDO平臺每年應執行滲透測試，該測試得依據已知的程式碼弱點或黑箱測試報告進行驗證外，另應能考量金融FIDO平臺之架構與商業邏輯進行測試。
第十六點 金融FIDO作業環境之網路管理應符合下列要求： 一、網路應區分網際網路、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。 二、金融FIDO作業環境與其他網段間之連線必須透過防火牆或路由器進行區隔與控管；同一網段與其他系統應有存取控管。 三、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	一、明定金融FIDO作業環境之網路管理原則。 二、第一款明定透過防火牆管理金融FIDO作業環境內各系統間之存取控管並與網際網路區隔，防止外部入侵。 三、第二款明定透過防火牆將金融FIDO作業環境與其他網段區隔及控管，並於同網段其他系統進行存取控管。 四、第三款明定系統開啟服務及程式之限制、客戶存取服務之規範原則，以及內部網址及網路架構等資訊之保密。 五、第四款明定應針對高風險設定及 6 個月內無流量之防火牆規則定期評估並盡速停用。 六、第五款明定系統維運人員得透過遠端連線進行系統管理作業，以維持系統可用度，並規範應遵循事項。

對外揭露。 四、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；針對已下線系統應立即停用防火牆規則。 五、為能維持系統可用度，系統維運人員得使用遠端連線進行系統管理作業，資料傳輸應使用足夠強度之加密通訊協定，並不得將密碼紀錄於工具軟體內，惟應避免將連線固定密碼紀錄於工具軟體內，防止惡意程式竊取；另得評估採用兩項以上技術或一次性密碼等安全設計，登入金融FIDO平臺之作業系統。 六、應管控內部無線網路之使用，不得以內部無線網路直接連線至金融 FIDO 平臺，並應加強必要防護措施進行隔離或限制。 七、經由網際網路連接至內部網路進行遠距之系統管理工作，應遵循下列措施： (一)應審查其申請目的、期間、時段、網段、使用設備、目的設備或服務，至少每年一次。 (二)應建立授權機制，依據其申請項目提供必要授權，至少每年檢視一次。 (三)變更作業應加強身分驗證，每次登入可採用照會或二項（含）以上安全設計並取得主管授權。 (四)應定義允許可連結之遠端設備，並確保已安裝必要資訊安全防護。 (五)應建立監控機制，留存操作紀錄，並由主管定期覆核。	七、第六款明定不得以內部無線網路直接連線至金融FIDO平臺。 八、第七款明定系統維運人員得經由網際網路連接至內部網路進行系統管理作業，惟應經審查、授權，每次使用須再次取得主管授權、留存操作紀錄、主管覆核。
第十七點 金融FIDO作業環境之系統生命週期管理應符合下列要求：	一、明定金融FIDO作業環境之系統生命週期管理原則。

一、應訂定資訊安全開發設計規範並落實執行。 二、對於委外開發的應用軟體，應執行監督並確保其有效遵循本指引規定。 三、應確保系統軟體和應用軟體安裝最新安全修補程式。 四、對於測試用之機敏資料(如SSL憑證金鑰)，應先進行資料遮蔽、加密或記號化，且不應與營運環境相同。 五、於開發階段起至營運階段，應遵循變更控制程序處理並留存相關紀錄；營運環境變更（如執行、覆核）應由二人以上進行，以相互牽制。 六、系統軟體變更應先進行技術審查並測試；套裝軟體不應自行異動，並應先進行風險評估。程式不應由開發人員自行換版或產製比對報表，應建立程式原始碼管理機制，以符合職務分工與牽制原則。	二、第一款明定應將資訊安全要求訂定於開發設計規範。 三、第二款明定系統委外開發應監督其依據資訊安全管控要求辦理。 四、第三款明定於開發階段起至營運階段使用之作業系統和軟體均須安裝最新安全修補程式。 五、第四款明定測試用之機敏資料不應與營運環境相同，其中記號化係指tokenization技術。 六、第五款明定應建立變更控制程序，於各階段管理參數、程式原始碼、執行碼及網頁等；營運環境變更需要兩人以上進行，針對變更內容進行檢視。 七、第六款明定應由非開發人員異動程式或產製比對報表，避免未授權異動，防止未經檢視程式或參數上線。
第十八點 金融FIDO作業環境之委外管理應符合下列要求： 一、委外處理前應先對受託廠商進行適當之安全評估，並依據最小權限及資訊最小揭露原則進行安全管控設計。 二、委託契約或相關文件中，應明確約定下列內容： (一)受託廠商應遵守本指引及其他適當資訊安全國際標準要求，確保委託人資料之安全。 (二)對受託廠商應依本指引內容進行適當監督。 (三)當委外業務安全遭到破壞時，受託廠商應主動、即時通知委託人。 (四)交付之系統或程式應確保無惡意程式及後門程式，其放置於網際網路之程式應通過	一、明定金融FIDO作業環境之委外管理原則。 二、第一款明定委外處理前應先對受託廠商進行評估，包含應制定廠商評估條件，遴選合適廠商，並依據委外項目給予最小權限，安裝必要管控工具，以利其符合資訊安全管控要求。 三、第二款明定相關資訊安全要求應記載於委外契約內。 四、第三款明定應對委外廠商進行資訊安全稽核。

程式碼掃描或黑箱測試。 三、應對委外廠商進行資訊安全稽核；亦可由委外廠商提交經第三方出具資訊安全稽核報告。	
第十九點 金融FIDO作業環境之資訊安全事故管理應符合下列要求： 一、應將各作業系統、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。 二、應建立資訊安全事故通報、處理、應變及事後追蹤改善作業機制，並應留存相關作業紀錄。 三、如有資訊安全事故發生時，其系統交易紀錄、系統日誌、安全事件日誌應妥善保管，並應注意處理過程中軌跡紀錄與證據留存之有效性。	一、明定金融FIDO作業環境之資訊安全事故管理原則。 二、第一款明定應建立集中管理相關設備日誌等之機制，進行交叉比對，訂定監控項目與指標。 三、第二款明定應建立通報程序與應變計畫，並留存作業紀錄。 四、第三款明定應留存資訊安全事故之相關紀錄、日誌，該紀錄應妥善保存、確保完整、及最小更動，該紀錄應可被驗證。
第二十點 金融FIDO作業環境之營運持續管理應符合下列要求： 一、應進行營運衝擊分析，定義最大可接受系統中斷時間，設定系統復原時間與資料復原時點，採取必要備援機制並應考量如有系統復原時間限制狀況下，建立安全距離外之異地備援機制，以維持交易可用性。 二、應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。 三、應每年驗證及演練其營運持續性控制措施，以確保其有效性，並應保留相關演練紀錄及召開檢討會議。	一、明定金融FIDO作業環境之營運持續管理原則。 二、第一款明定應進行營運衝擊分析。 三、第二款明定應評估重大資訊系統事件之可接受範圍，投入相對應之資源，並建立各項應變程序。 四、第三款明定應每年針對金融FIDO平臺各項服務進行演練，驗證營運持續性控制措施之有效。
第二十一點 金融機構應盤點前開資訊安全相關規定，並將相關要求與內部控制制度結合，定期進行法令遵循自評，以確保資訊安全之法令遵循性。 本指引所訂之資訊系統及安全控管項目，應透過內部控制制度進行定期檢核，並應依相關規範定期由評估	一、第一項明定金融機構應盤點與資訊安全相關規定，包含主管機關函令、周邊單位及所屬公會自律規範等，定期辦理法令遵循自評，以確保符合相關規定。 二、第二項明定各金融機構應依其所訂內部控制制度定期委由評估單位針

單位進行檢視，提出資訊系統及安全控管作業評估報告。 前項評估報告內容應至少包含評估人員資格、評估範圍、評估時所發現之缺失項目、缺失嚴重程度、缺失類別、風險說明、具體改善建議及社交演練結果，且應送稽核單位進行缺失改善事項之追蹤覆查。該報告應併同缺失改善等相關文件至少保存二年。 金融機構應確保其本身、主管機關，或其指定之人能取得辦理金融FIDO之相關資訊，包括相關系統之查核報告及實地查核權力。 為確保交易資料之隱密性及安全性，並維持資料傳輸、交換或處理之正確性，金融機構於必要時應提高金融FIDO作業環境相關資訊系統標準及加強安全控管作業。 金融機構應依金融機構作業委託他人處理相關規範，透過合作契約約定機構間共同運作金融FIDO之權責關係。	對本指引各項要求進行資訊安全檢視並提出評估報告。 三、第三項明定評估報告應包含之內容及最低保存年限，且應送稽核單位進行缺失改善事項之追蹤覆查。 四、第四項及第五項明定金融機構應確保其本身、主管機關及中央銀行，或其指定之人能取得辦理金融FIDO之相關資訊，必要時應提高資訊系統標準及加強安全控管作業。 五、第六項明定金融機構應參考「金融機構作業委託他人處理內部作業制度及程序辦法」第十條條文內容約定權責關係。
第二十二點 本指引函報金管會核備後實施，修正時亦同。	明定本指引之核定程序。