金融機構辦理電子銀行業務安全控管作業基準

壹、前言

中華民國銀行商業同業公會全國聯合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。

貳、電子銀行業務之定義

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。

參、電子銀行業務之訊息傳輸途徑

係指客戶端利用電子設備及通訊設備與金融機構進行交易時所使用的網路型態。

一、金融機構專屬網路

金融機構專屬網路係直接以連線方式(撥接(Dial-Up)、專線(Lease-Line)或虛擬私有網路(Virtual Private Network，VPN)等方式)傳輸訊息。

二、加值網路(Value Added Network，VAN)

加值網路係指運用基礎通訊網路所建置之設施，提供正常傳輸外附加價值之服務，諸如自動錯誤偵測及修復(automatic error detection and correction)、通訊協定轉換(protocol conversion)及訊息儲存及後送(message storing and forwarding)等，以增加網路使用之附加價值。

三、網際網路(Internet)

客戶端利用電子設備及通訊設備，透過網際網路服務業者(Internet Service Provider，ISP)與金融機構間進行交易。網際網路(Internet)係一個提供全球資訊之高速網路環境，使用者需先行連結至特定網站，再運用該網站服務連結至個別網址，以便進一步使用 Internet 之各種資訊及資源； ISP 即指以提供前述網站服務為營利目的之公司。

四、行動網路

客戶端利用電子設備及通訊設備，透過電信服務業者(Telecom)與金融機構間進行交易。電信服務業者在各區域間佈建縝密之基地台(base station)，以負責訊息之傳送及接收。惟實際運用行動網路進行交易指示時，應依個別電信服務業者與金融機構間傳輸途徑之不同，分別納入前述金融機構專屬網路或網際網路傳輸途徑予以規範。

肆、電子銀行業務之交易類別及風險

係指由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。

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 服務項目舉例如下：

台外幣存提款、台外幣轉帳、匯兌、台外幣匯款、消費、投資、基金下單、債票券下單、款項繳納、授信等交易。

２、申請指示 服務項目舉例如下：

開發信用狀申請、修改信用狀申請等交易。

（二）高風險及低風險性之交易

依據其交易指示執行結果對客戶權益影響之不同，可再行區分為高風險性之交易及低風險性之交易。

交易風險類別	說明
高風險	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。
低風險	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。 １、事先約定轉入帳戶。 ２、概括約定及限定性繳費繳稅之稅費轉帳。 ３、客戶非直接獲取金融機構之服務且需其人工後續認定客戶身分者之申請指示類。 ４、非約定轉入帳戶 ４．１、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。 ４・２、網際網路之低風險性交易，以每戶每筆不超過五萬元、每天累積不超過十萬元、每月累積不超過二十萬元為限。 ４・３、配合採用各種嚴密的技術防護措施時，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。

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之服務項目。

其服務項目舉例如下：

非電子轉帳及交易指示類	服務項目
查詢	１、帳務類查詢： 存放款餘額查詢、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、信用狀查詢等交易。 ２、非帳務類查詢： 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、業務簡介查詢等交易。
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、消費通知等交易。

伍、本基準之構面

本基準構面包括交易面、管理面、環境面及支付工具面等四大構面之安全需求及安全設計，其基本標準如下：

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	金融機構專屬網路		加值網路		網際網路	
交易類別	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	電子轉帳及交易指示類	非電子轉帳及交易指示類

防護措施	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		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	*非必要*	*非必要*	非必要	必要	必要	非必要
訊息完整性	必要	必要	非必要	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	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	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	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	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。

(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。

（２）使用動態密碼（One Time Password，OTP）或採憑證驗證方式為簽入密碼者，得不使用簽入介面之安全設計。動態密碼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，隨機產生限定一次使用之密碼者，其安控層次已較採用固定密碼簽入者高，故得不再使用簽入介面之安全設計。

（３）透過網際網路傳輸途徑並採用戶代號及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。

（３・１）用戶代號之安全設計：

（３・１・１）金融機構不得使用客戶之顯性資料(如統一編號、身分證號及帳號)作為唯一之識別，否則應另行增設使用者代號以資

識別。

（３・１・２）不應少於六位。

（３・１・３）不應訂為相同的英數字、連續英文字或連號數字。

（３・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。

（３・１・５）客戶同一時間內只能登入一次密碼。

（３・１・６）如增設使用者代號，至少應依下列方式辦理：

（３・１・６・１）不得為客戶之顯性資料。

（３・１・６・２）如輸入錯誤達五次，金融機構應做妥善處理。

（３・１・６・３）新建立時不得相同於用戶代號及密碼；變更時，亦同。

（３・２）密碼之安全設計：

（３・２・１）不應少於六位。若搭配交易密碼使用則不應少於四位。

（３・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。

（３・２・３）不應訂為相同的英數字、連續英文字或連號數字。

（３・２・４）密碼與代號不應相同。

（３・２・５）密碼連續錯誤達五次，不得再繼續執行交易。

（３・２・６）變更密碼不得與前一次相同。

（３・２・７）首次登入時，應強制變更預設密碼。

（４）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簽入介面之安全設計；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。

２、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)對稱性加解密系統如 NIST 之 DES (National Institute of Standards and Technology，Data Encryption Standard，以下簡稱 DES)等機制。 (１．１．１)應至少採用 DES(金鑰有效長度固定為 56 位元)或其他安全強度相同之演算法。

	(１．２)非對稱性加解密系統如 RSA (Rivest 、Shamir、Adleman Encryption Standard，以下簡稱 RSA)等機制，可對資料長度較小(如資料長度小於金鑰長度)之訊息做加密。 (１．２．１)如採用 RSA，金鑰長度不得小於 1024 位元，採用其他演算法則其安全強度至少須與前述規範之 RSA 強度相同。 (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、Diffie-Hellman Key Agreement)交換之。安全強度應符合上述(１・１・１)及(１・２・１)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。
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碼系統。 (１．１)對稱性系統如 DES(使用押碼(Message Authentication Code，MAC))等機制： (１．１．１)透過金融機構專屬網路或加值網路應至少採用 DES(金鑰(Secret Key)有效長度固定為 56 位元)或其他安全強度相同之演算法。 (１．１．２)透過網際網路應至少採用 Triple DES(金鑰有效長度為 112 位元) 或其他安全強度相同之演算法。 (１．２)非對稱性系統如 RSA(使用電子簽章(Digital Signature))等機制： (１．２．１)透過金融機構專屬網路或加值網路如採用 RSA 則其金鑰長度不得小於 512 位元。 (１．２．2)透過網際網路如採用 RSA 則其金鑰長度不得小於 1024 位元(若採用 RSA 且訊息格式屬金融電子資料交換(Electronic Data Interchange，EDI)文件者，則其金鑰長度不得小

	於 512 位元)。 (１．２．3)若採用其他演算法，則其安全強度至少須與前述規範之 RSA 強度相同。 (２)金鑰交換： (２．１)若訊息採對稱性加解密系統處理，則同前述『訊息隱密性』有關金鑰交換之規範。 (２．2)若訊息採非對稱性加解密系統處理，訊息簽章使用對應之公開金鑰可透過憑證交換或其他通道交換；惟透過非信賴之通道交換者，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。
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。 (１．１)對稱性系統如 DES(使用押碼(Message Authentication Code，MAC))等機制： (１．１．１)透過金融機構專屬網路或加值網路至少採用 DES(金鑰有效長度固定為 56 位元)或其他安全強度相同之演算法。 (１．１．2)透過網際網路應至少採用 Triple DES(金鑰有效長度為 112 位元) 或其他安全強度相同之演算法。 (１．２)非對稱性系統如 RSA(使用數位簽章(Digital Signature))等機制： (１．2．１)透過金融機構專屬網路或加值網路如採用 RSA 則其金

	鑰長度不得小於 512 位元。 (１．２．2)透過網際網路如採用 RSA 則其金鑰長度不得小於 1024 位元(若採用 RSA 且訊息格式屬金融電子資料交換(Electronic Data Interchange，EDI)文件者，則其金鑰長度不得小於 512 位元)。 (１．２．3)若採用其他演算法，則其安全強度至少須與前述規範之 RSA 強度相同。 (２) 金鑰交換： (２．１)若訊息採對稱性加解密系統處理，則同前述『訊息隱密性』有關金鑰交換之規範。 (２．２)若訊息採非對稱性加解密系統處理，訊息簽章使用對應之公開金鑰可透過憑證交換或其他通道交換；惟透過非信賴之通道交換者，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。
訊息不可重複性	如使用序號、時戳等機制。
無法否認傳送訊息	(１)訊息處理： 使用電子簽章(Digital Signature)或採用其他訊息簽章認證等機制。 (１．１)透過金融機構專屬網路或加值網路如採用 RSA 則其金鑰長度不得小於 512 位元。 (１．２)透過網際網路如採用 RSA 則其金鑰長度不得小於 1024 位元(若採用 RSA 且訊息格式屬金融電子資料交換(Electronic Data Interchange，EDI)

	文件者，則其金鑰長度不得小於 512 位元)。 (１．３)若採用其他演算法，則其安全強度至少須與前述規範之 RSA 強度相同。 (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： 金鑰應於使用一段期間後更換之，以確保其安全性。
無法否認接受訊息	(１)訊息處理： 使用電子簽章(Digital Signature)或採用其他訊息簽章認證等機制。 (１．１)透過金融機構專屬網路或加值網路如採用 RSA 則其金鑰長度不得小於 512 位元。 (１．２)透過網際網路如採用 RSA 則其金鑰長度不得小於 1024 位元(若採用 RSA 且訊息格式屬金融電子資料交換(Electronic Data Interchange，EDI)文件者，則其金鑰長度不得小於 512 位元)。 (１．３)若採用其他演算法，則其安全強度至少須與前述規範之 RSA 強度相同。 (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： 金鑰應於使用一段期間後更換之，以確保其安全性。

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。

(四)『電子轉帳及交易指示類』之限制

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，且必須採用用戶代號、密碼，以健全安全防護機制。

(五)『電子轉帳及交易指示類』無加密功能者之限制

電信網路(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。

(六)『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，若涉及他行居間代理者除以合約約定者外，其安全機制應具備『訊息來源辨識』之基本防護措施。

(七)除限定性繳費稅交易外之低風險非約定轉入帳戶之交易密碼規定

低風險非約定轉入帳戶之轉帳應增設交易密碼，並配合採用各種嚴密的技術防護措施，且能有效防範客戶端被植入木馬程式竊取密碼資料之攻擊手法。

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	得以下列方式處理及管控： １、 建置安全防護軟硬體如防火牆(Firewall)、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、 記錄使用者查詢電話。 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)。 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	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）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。 （３）放置網路伺服器於上鎖密室中。 ２、強制更換應用軟體及網路作業系統之預設密碼等。
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。 ２、編寫客戶端之操作手冊及制訂完整合約等。

三、環境及端末設備面之安全需求及安全設計

(一)環境面之安全需求

促使金融機構著重於環境及端末設備面之安全控管，強化其所提供之自動化設備之安全防護，以防範遭受外力破壞。

防護措施	基本需求
建立安全防護策略	1、為保持自動化服務區之環境實體完整性，定期檢視是否有增減相關裝置。 2、其安全防護依「銀行公會會員安全維護執行規範」第四條辦理。 3、自動化服務區環境之安全除應依「自動櫃員機之安全維護準則」辦理外，並應保持自動化服務區之環境實體完整性，定期檢視是否有增減相關裝置。 其檢視步驟至少應包括下述： （1）原始設施確實逐項編號。 （2）比對現場相關設施及裝置是否與原始狀態一致。 （3）建立檢視清單(Checklist)，並應定期陳核並追蹤考核。 （4）金融機構之個別自動櫃員機/自動化服務區應指定該金融機構鄰近之分支機構負責監管。
提高系統可靠性之措施	1、自動化設備之監視系統應依「銀行公會會員安全維護執行規範」第一條辦理。 2、自動化設備之警示通報系統應依「銀行公會會員安全維護執行規範」第六條辦理。
制定作業管理規範	於銀行內部環境管理部分應落實管理準則之規範。

(二)端末設備面之安全設計

防護措施	安全設計
建立安全防護策略	自動櫃員機之安全設計： 1、自動櫃員機金庫裝置應符合 UL291 LEVEL 1

	標準。 2、自動櫃員機鍵盤(KEY BORD/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）金融機構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）金融機構應與裝設地點之商家訂立檢核契約。 （6）金融機構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產製端末設備查核碼。 實體卡片銷售端末設備之安全設計： 運用銷售端末設備(Point Of Sale ：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、金融機構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產製端末設備查核碼。 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、金融機構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、金融機構應與商家訂立檢核契約。
提高系統可靠性之措施	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。
制定作業管理規範	１、制定自動櫃員機安全控管規章，含設備規格、安控機制說明、安控程序說明等。 ２、編寫自動櫃員機之操作手冊。 ３、制定銷售端末設備管理規章，含設備規格、安控機制說明、安控程序說明等。

四、支付工具面之安全需求及安全設計

(一)支付工具面之安全需求

防護措施	基本需求
建立安全防護策略	晶片金融卡之晶圓應至少符合「晶片金融卡規格安控等級」如 Common Criteria EAL 5 或 ITSEC level E4 等，並能防堵市面上常見之攻擊破解方法。
提高系統可靠性之措施	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。 ３、金融機構應確保卡片 END TO END 之交易安全。
制定作業管理規範	金融機構應揭示客戶使用卡片之注意事項，至少應包含下述： 1、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。 2、密碼資訊不應書寫於實體卡片上，並須定期變更密碼。 3、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。 4、金融機構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。

(二)支付工具面之安全設計

防護措施	安全設計
建立安全防護策略	實體卡片之安全設計： 交易驗證碼(TAC) 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碼作為驗證每筆交易之不可否認性，用以確保交易安全。 ２、金融機構發行多功能卡片（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，俾達到由發卡銀行端至客戶端安全。
提高系統可靠性之措施	得以下列方式處理及管控： １、應做卡片容量規劃。 ２、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」。
制定作業管理規範	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。

（94/2/22 本會全電字 0293 號函）
（94/1/11 行政院金融監督管理委員會金管銀(二)第 0948010020 號函備查 ）
（94/7/22 行政院金融監督管理委員會金管銀(二)第 0948010921 號函定調整時間備查）