電子支付機構資訊系統標準及安全控管作業基準辦法條文

第一條　本辦法依電子支付機構管理條例(以下簡稱本條例)第二十九條第二項、第三十九條及第四十條準用第二十九條第二項規定訂定之。

第二條　電子支付機構辦理電子支付機構業務之資訊系統及安全控管作業，應依本辦法規定辦理。

第三條　本辦法用詞定義如下：

一、電子支付機構業務：指本條例第三條第一項各款業務。

二、電子支付平臺：指辦理電子支付機構業務相關之應用軟體、系統軟體及硬體設備。

三、電子支付作業環境：指電子支付平臺、網路、作業人員及與該電子支付平臺網路直接連結之應用軟體、系統軟體及硬體設備。

四、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，透過電信服務業者進行訊息傳輸。

五、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。

六、常用密碼學演算法如下：

(一)對稱性加解密演算法：指資料加密標準(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)。

(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)。

七、系統維運人員：指電子支付平臺之作業人員，其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、使用者服務、業務推廣、帳務管理或會計管理等作業。

八、一次性密碼(One Time Password；以下簡稱 OTP)：指運用動態密碼產生器、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。

九、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。

十、機敏資料：指包含但不限於密碼、個人資料、身分認證資料、信用卡卡號、信用卡驗證碼或個人化資料等。

十一、近距離無線通訊(Near Field Communication；以下簡稱NFC)：指利用點對點功能，使行動裝置在近距離內與其他設備進行資料傳輸。

十二、實體通路支付服務(Online To Offline，O2O)：指電子支付機構就電子支付機構業務，利用行動裝置或其他可攜式設備於實體通路提供服務。

十三、約定連結存款帳戶付款：指電子支付機構辦理代理收付實質交易款項業務，依使用者與金融機構間之約定，向金融機構提出指示，連結該使用者存款帳戶進行轉帳，由電子支付機構收取代理收付款項，並於該使用者電

子支付帳戶記錄代理收付款項金額及移轉情形之服務。

第四條　電子支付機構於受理使用者註冊時，所採用之身分確認程序之安全設計如下：

一、確認行動電話號碼：應確認使用者可操作並接收訊息通知。

二、確認電子郵件信箱：應確認使用者可接收郵件並讀取郵件內容。

三、確認社群媒體帳號：應經使用者授權取得社群媒體之個人資料。

四、確認金融支付工具之持有人與電子支付帳戶使用者相符，方式如下：

(一)確認存款帳戶持有人：應向金融機構查詢或確認存款帳戶持有人身分證統一編號或商業統一編號。個人使用者無身分證統一編號者，應提供其他身分證明文件及其號碼等資料供金融機構確認。

(二)確認信用卡持有人：應向信用卡發卡機構查詢或確認持有人身分證統一編號。

五、確認證明文件影本：得採上傳或拍照方式取得完整清晰可辨識之影像檔。

六、臨櫃確認身分：臨櫃受理使用者註冊，應了解使用者動機、查證電話與住址、辨識具照片之身分證明文件、留存影像、留存印鑑或簽名、約定收付款限額及注意周邊環境。

七、以電子簽章確認身分：應透過憑證進行簽章、驗證憑證有效性,並確認該憑證之身分與電子支付帳戶使用者相符。

第五條　　電子支付帳戶使用者登入電子支付平臺時應進行身分確認，得以帳號及固定密碼登入。

前項帳號及固定密碼之安全設計如下：

一、帳號如使用顯性資料(如商業統一編號、身分證統一編號、行動電話號碼、電子郵件帳號、信用卡卡號等)作為唯一之識別，應另行增設使用者代號以資識別。使用者代號亦不得為上述顯性資料。

二、密碼不應少於六位。

三、密碼不應與帳號相同，亦不得與使用者代號相

同。

四、密碼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。

五、密碼應採英數字混合使用，且宜包含大小寫英文字母或符號。

六、密碼連續錯誤達五次時應限制使用，須重新申請密碼。

七、變更後之密碼不得與變更前二次密碼相同。

八、密碼超過一年未變更，電子支付機構應做妥善處理。

九、使用者註冊時係由電子支付機構發予預設密碼者，於使用者首次登入時，應強制變更預設密碼。

第六條　電子支付機構對於不同交易類型，應依其不同交易限額，採用下列交易安全設計：

一、辦理代理收付實質交易款項(含實體通路支付服務交易)，於使用者以電子支付帳戶款項支付、以約定連結存款帳戶付款支付、提出提前付款請求，或提出取消暫停支付請求時，應依其不同交易限額，採用下列交易安全設計：

(一)每筆付款金額未達等值新臺幣五千元，或每日付款金額未達等值新臺幣二萬元，或每月付款金額未達等值新臺幣五萬元者，應採用 A 類交易安全設計。

(二)每筆付款金額達等值新臺幣五千元且未達等值新臺幣五萬元，或每日付款金額達等值新臺幣二萬元且未達等值新臺幣十萬元，或每月付款金額達等值新臺幣五萬元且未達等值新臺幣二十萬元者，應採用 B 類交易安全設計。

(三)每筆付款金額達等值新臺幣五萬元以上，或每日付款金額達等值新臺幣十萬元以上，或每月付款金額達等值新臺幣二十萬元以上者，應採用 C 類交易安全設計。

二、於使用者進行電子支付帳戶間款項移轉時，應依其不同交易限額，採用下列交易安全設計：

(一)每筆付款金額未達等值新臺幣五萬元，或每日付款金額未達等值新臺幣十萬元，或每月付款金額未達等值新臺幣二十萬元者，應採

用C類交易安全設計。

(二)每筆付款金額達等值新臺幣五萬元，或每日付款金額達等值新臺幣十萬元以上，或每月付款金額達等值新臺幣二十萬元以上者，應採用D類交易安全設計。

前項D類交易安全設計得替代C類交易安全設計，C類交易安全設計得替代B類交易安全設計，B類交易安全設計得替代A類交易安全設計。

第七條　電子支付機構執行前條所列交易應進行身分確認，各類交易安全設計並應符合下列要求：

一、A 類交易安全設計：指採用固定密碼之安全設計，其安全設計應符合第五條第二項之規定。

二、B類交易安全設計：指採用簡訊傳送一次性密碼至使用者行動裝置之安全設計，應設定密碼有效時間，並應避免簡訊遭竊取或轉發。

三、C類交易安全設計：指採用下列任一款之安全設計：

(一)採用晶片金融卡之安全設計，應依每筆交易動態產製不可預知之端末設備查核碼，每次

需輸入卡片密碼產生交易驗證碼，並由原發卡銀行驗證交易驗證碼；應設計防止第三者存取。

(二)採用一次性密碼之安全設計，應採用實體設備且非同一執行交易之設備；設定密碼有效時間；設計密碼連續錯誤達三次時予以鎖定使用，經適當身分認證後才能解除。如實體設備與執行交易之設備為同一設備，則應於使用者端經由人工確認交易內容後才能完成交易。

(三)採用二項(含)以上技術(Two Factors Authentication)，其安全設計應具有下列任二項以上技術：

1、使用者與電子支付機構所約定之資訊，且無第三人知悉(如登入密碼)。

2、使用者所持有的設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等)：電子支付機構應確認該設備為使用者與電子支付機構所約定持有之實體設備。

3、使用者所擁有的生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)：電子支付機構應依據其風險承擔能力調整生物特徵之錯誤接受度，以有效識別使用者身分，必要時應增加多項不同種類生物特徵。

四、D類交易安全設計：指採用下列任一款之安全設計：

(一)臨櫃受理使用者交易，應核對身分證明文件及印鑑或簽名。

(二)採用符合電子簽章法之安全設計。

前項第四款第二目採用符合電子簽章法之安全設計得使用憑證機制，相關要求如下：

一、應遵循憑證機構之憑證作業辦法。

二、應確認憑證之合法性、正確性、有效性、保證等級及用途限制，該憑證應由憑證主管機關核定之第三方憑證機構所核發。

三、擔任憑證註冊中心，受理使用者憑證註冊或資料異動時，其臨櫃作業應額外增加具二項(含)以上技術之安全設計或經由另一位人員審核。

四、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。

五、應用於交易不可否認之憑證，應選擇負賠償責任之憑證機構,且該憑證申請須由使用者自行產製私鑰。

六、政府機關核發之憑證限應用於註冊時之身分確認。

七、每筆交易須針對支付內容進行簽章並驗證該憑證之有效性。

八、應確認該憑證私鑰儲存於符合共同準則(Common Criteria) EAL 4+(至少包含增項 AVA_VLA.4 或 AVA_VAN.5)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。如晶片硬體與產生支付指示為同一設備,則應於使用者端經由人工確認交易內容後才完成交易;或於交易過程額外增加具二項(含)以上安全設計。

第八條　電子支付機構於不同網路型態應確保電子支付交易

符合下列安全規定：

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。如採用前條第一項第四款第二目之交易安全設計者，應同時符合訊息不可否認性之訊息防護措施。

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。如採用前條第一項第四款第二目之交易安全設計者，應同時符合訊息不可否認性之訊息防護措施。

第九條　前條所稱訊息隱密性、訊息完整性、訊息來源辨識性、訊息不可重複性及訊息不可否認性之安全設計應符合下列要求：

一、訊息隱密性：應採用 3DES 112bits、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。

二、訊息完整性：應採用 SHA1、3DES 112bits、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 3DES 112bits、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、時間戳記等機制產生。

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。

第十條　電子支付平臺之設計原則應符合下列要求：

一、網際網路應用系統設計要求：

(一)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。

(二)應設計連線控制及網頁逾時中斷機制。使用者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)應辨識使用者輸入與系統接收之支付指示一致性。

(五)應設計於使用者進行身分確認與交易機制時，須採用一次性亂數或時間戳記，以防止重送攻擊。

(六)應設計於使用者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。

(七)應設計於使用者修改個人資料、約定或變更提領電子支付帳戶款項之銀行存款帳戶時，須先經第七條第一項第二款至第四款任一類交易安全設計進行身分確認。

(八)應設計個人資料顯示之隱碼機制。

(九)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。

(十)應建置防偽冒與洗錢防制偵測系統，建立風險分析模組與指標，用以於異常交易行為發

生時即時告警並妥善處理。該風險分析模組與指標應定期檢討修訂。

二、實體通路支付服務程式設計要求：

(一)電子支付機構應確認實體通路之設備及其所傳送或接收之訊息隱密性及完整性。

(二)電子支付機構辦理款項間移轉或支付實質交易款項時，如將支付指示記錄於圖片、條碼或檔案，應經使用者確認；如將上述媒體透過近距離無線通訊、藍芽、掃描、上傳等機制交付他人者，應視必要增加存取限制(如密碼)，防止第三人竊取或竄改。

三、使用者端程式設計要求：

(一)應採用被作業系統認可之數位憑證進行程式碼簽章。

(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、行動裝置應用程式設計要求：

(一)應針對所需最小權限進行存取控制。

(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破解，應提示使用者注意風險。

(四)於安裝或首次啟動應用程式時，得提示使用者於行動裝置上安裝防毒軟體。

(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 技術進行付款交易資料傳輸前，應經由使用者人工確認。

五、約定連結存款帳戶付款設計要求：

(一)電子支付機構應向金融機構申請金融憑證，並向金融機構約定為執行本款作業之專屬憑證。應用時須以憑證簽章方式提出約定連結申請或扣款指示，雙方同意以憑證簽驗章機制作為交易不可否認。

(二)約定連結程序：使用者向電子支付機構提出

申請並同意委由電子支付機構代使用者辦理轉帳，使用者得以臨櫃、網路銀行或透過電子支付機構依前目所定方式等機制，向金融機構提出約定連結申請，並提供該使用者之金融機構存款帳號及其電子支付機構之電子支付帳戶帳號，經金融機構確認使用者身分後完成設定。不同身分確認機制，依據其適用之風險類別，應限制不同交易額度。

(三)交易程序：電子支付機構透過本款第一目所定方式向金融機構提出代使用者辦理扣款指示，經金融機構確認無誤後，撥付款項至電子支付帳戶。

(四)私鑰保護：該憑證私鑰應儲存於符合共同準則(Common Criteria) EAL 4+(至少包含增項 AVA_VLA.4 或 AVA_VAN.5)或 FIPS 140-1 Level 2 或其他相同安全強度之硬體安全模組內並限制匯出功能。

(五)存取控制：應建立管控機制，限制非授權人員或程式存取私鑰及本款作業之相關程式。

(六)資金移轉：金融機構將資金移轉至使用者之電子支付帳戶時，考量帳戶管理機構不同，視為跨行交易。

(七)即時通知機制：電子支付機構應要求金融機構建立即時通知機制，由金融機構於進行資金移轉後，立即向使用者通知。

六、再確認之設計要求：

(一)收到支付指示後，以信用卡線上刷卡、電子支付帳戶款項或約定連結存款帳戶付款進行支付者，應以事先與使用者同意之方式(如交易確認頁面、郵件、簡訊等)通知付款方再確認，經確認無誤後才進行交易。

(二)非以前目方式辦理者，如透過其他方式進行付款者，可視為付款方之再確認。

第十一條　電子支付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。但外國銀行在臺分行應由其負責人簽署。

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、應依據電子支付平臺之作業流程，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。

第十二條　電子支付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。

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，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，應限制使用者個人資料顯示於螢幕。

六、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，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。

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，應符合第五條第二項規定，並應定期變更密碼：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。

第十三條　電子支付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、應針對電子支付作業環境，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。但外國銀行在臺分行或未設董（理）事會者，應由其負責人簽署。

第十四條　電子支付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密性機制：

(一)機敏資料儲存於使用者端操作環境。

(二)機敏資料於網際網路上傳輸。

(三)使用者身分識別資料(如密碼、個人化資料)儲存於系統內。

二、使用者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的資料運算；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。

第十五條　電子支付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，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規規定。

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。

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電子支付作業環境之範圍，應符合本辦法相關規定。

第十六條　電子支付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收集、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，建立並落實電子支付作業環境安全設定辦法。

第十七條　　電子支付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、電子支付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、電子支付平臺每年應執行滲透測試，以加強資訊安全。

第十八條　電子支付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、電子支付作業環境與其他網路間之連線必須透

過防火牆或路由器進行控管。

三、系統僅得開啟必要之服務及程式，使用者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。

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、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。

六、應管控內部無線網路之使用人員申請，不得於內部無線網路連線至電子支付作業環境，並應使用必要防護措施進行隔離。

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認證，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。

第十九條　電子支付作業環境之系統生命週期管理應符合下列要求：

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辦法規定。

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，應先進行資料遮蔽處理或管制保護。

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。

第二十條　電子支付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)受託廠商應遵守本辦法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)對受託廠商應依本辦法內容進行適當監督。

(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或由委外廠商提出資訊安全稽核報告，至少每年一次。

第二十一條　電子支付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。

第二十二條　電子支付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。

第二十三條　電子支付機構應盤點與資訊安全相關法規規定，並將相關資訊安全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。

本辦法所訂之資訊系統及安全控管項目，電子支付機構應透過內部控制制度進行定期檢核，並應於依本條例第十條申請許可時及其後每年四月底前，由會計師進行檢視，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。

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，主管機關於必要時，得要求電子支付機構提高資訊系統標準及加強安全控管作業。

第二十四條　本辦法自中華民國一百零四年五月三日施行。