

電子支付機構資訊系統標準及安全控管作業基準 辦法總說明

為確保電子支付機構之交易資訊安全及業務健全運作，避免因資訊系統運作、傳輸或處理錯誤，影響服務之穩定與安全，並衍生相關糾紛，電子支付機構管理條例(以下簡稱本條例)第二十九條第一項、第三項、第三十九條及第四十條準用第二十九條第一項、第三項規定，電子支付機構應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；電子支付機構就電子支付機構業務，利用行動電話或其他可攜式設備於實體通路提供服務，其作業應符合主管機關所定安全控管作業基準規定，並於開辦前經主管機關核准。

為明確規範電子支付機構之資訊系統標準及安全控管作業基準，以利相關業者遵循及主管機關執行法令，爰依第二十九條第二項、第三十九條及第四十條準用第二十九條第二項授權，並參酌 CNS 27001「資訊技術-安全技術-資訊安全管理系統—要求事項」國家標準、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及中華民國銀行商業同業公會全國聯合會「金融機構資訊系統安全基準」、「金融機構辦理電子銀行業務安全控管作業基準」等規範，訂定本辦法計二十四條，其要點如下：

- 一、本辦法之適用範圍及用詞定義。(第二條及第三條)
- 二、使用者註冊時身分確認、登入帳號與固定密碼、交易類型與限額及各網路型態之交易安全設計。(第四條至第九條)
- 三、電子支付平臺之設計原則。(第十條)
- 四、電子支付機構應訂定組織、人員及設備安全之相關管理措施；其提供之電子支付平臺應就機房、營運、網路、金鑰、系統生命週期、資安事故及營運持續管理等資訊系統標準，採取相關資訊安全維護措施。(第十一條至第二十二條)
- 五、電子支付機構除應盤點與資訊安全相關法令，定期檢核落實程度外，並應於業務申請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。(第二十三條)
- 六、本辦法之施行日期。(第二十四條)

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	說明
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。	本辦法訂定依據。
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。	本辦法之適用範圍。
<p>第三條 本辦法用詞定義如下：</p> <p>一、電子支付機構業務：指本條例第三條第一項各款業務。</p> <p>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。</p> <p>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。</p> <p>四、網路型態區分如下：</p> <p>（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。</p> <p>（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。</p> <p>（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。</p> <p>五、訊息防護措施區分如下：</p> <p>（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</p>	<p>一、定明本辦法之用詞定義。</p> <p>二、第二款說明電子支付平臺包含網路設備、防火牆、入侵偵測或入侵防禦、防毒伺服器、上網管制、異動偵測、軌跡紀錄等資訊安全設備，與提供給使用者使用之網際網路應用程式（網站）、實體通路支付服務程式、使用者端程式、行動裝置應用程式，及提供給客服、帳務、作業使用等內部作業所需之應用軟體、系統軟體、硬體設備。</p> <p>三、第三款說明電子支付作業環境亦包含與電子支付平臺同一網段未經過防火牆分隔之應用軟體、系統軟體及硬體設備。</p> <p>四、第四款說明電子支付平臺為提供使用者相關服務，所利用之三種網路型態。</p> <p>五、第五款說明電子支付平臺所具備之訊息防護措施。</p> <p>六、第六款列舉常用之密碼學演算法。</p> <p>七、第七款系統維運人員係指具權限得存取電子支付平臺，進行系統管理或操作之人員。上述人員可能進行網路管理、設備管理、資訊安全設備管理人員、電子支付平臺開發、維護與管理、或帳戶管理。</p> <p>八、第十款機敏資料係使用者於註冊或交</p>

<p>損害其秘密性。</p> <p>(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。</p> <p>(三)訊息來源辨識性(Authentication):指傳送方無法冒名傳送資料。</p> <p>(四)訊息不可重複性(Non-duplication):指訊息內容不得重複。</p> <p>(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。</p> <p>六、常用密碼學演算法如下:</p> <p>(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)。</p> <p>(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)。</p> <p>(三)雜湊函數:指安全雜湊演算法(Secure Hash Algorithm;以下簡稱 SHA)。</p> <p>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。</p> <p>八、一次性密碼(One Time Password;以下簡稱 OTP):指運用動態密碼產</p>	<p>易時,提供給電子支付機構之資料。</p> <p>九、第十一款說明近距離無線通訊方式,係透過具有 NFC 功能之設備將訊息以 NFC 方式傳送至另一具有 NFC 功能之設備上。</p> <p>十、第十二款說明實體通路支付服務運作方式,透過行動裝置將支付指示或訊息傳送至實體商家之電腦、行動裝置上。</p> <p>十一、第十三款說明使用者之電子支付帳戶及其在金融機構之存款帳號之連結,須使用者事先與金融機構約定後,方能由電子支付機構發動扣款交易。</p>
---	--

<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	
<p>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：</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>一、定明受理使用者註冊之身分確認程序之安全設計。</p> <p>二、第一款得採簡訊或推播等方式辦理。推播係指行動裝置作業系統提供之訊息通知機制，採用該機制之電子支付機構應隨時確認該機制之有效性與隱密性，如該機制無法確認使用者行動裝置電話或有致訊息有洩漏之虞時，應立即採用其他加強機制。</p>

<p>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：</p> <p>(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。</p> <p>(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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>三、第二款規定電子支付機構須能確認使用者可讀取該機構所傳送之電子郵件，以利必要時聯繫。</p> <p>四、第三款規定電子支付機構須能確認使用者可讀取該機構所傳送之社群媒體訊息，以利必要時聯繫。</p> <p>五、第四款規定電子支付機構須能確認使用者提供之存款帳戶或信用卡之持有人身分證統一編號與註冊資料相符。電子支付機構得透過相關交易入帳方式確認存款帳戶與註冊資料相符。</p> <p>六、第六款規定電子支付機構就使用者臨櫃註冊時應確認及注意之事項。</p> <p>七、第七款規定電子支付機構應使用符合電子簽章法之憑證確認使用者身分。憑證使用時，電子支付機構應驗證憑證是否過期、是否註銷、上層各憑證是否有效、最上層憑證(根憑證)是否符合電子簽章法相關要求。</p>
<p>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。</p> <p>前項帳號及固定密碼之安全設計如下：</p> <p>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。</p> <p>二、密碼不應少於六位。</p> <p>三、密碼不應與帳號相同，亦不得與使用者代號相同。</p>	<p>一、第一項定明使用者登入電子支付平臺，可採用帳號及固定密碼方式進行身分確認。其他方式，包括一次性密碼、二項(含)以上技術、憑證簽章等機制，亦可採用。如採用帳號及固定密碼登入者，應符合第二項規定。</p> <p>二、第二項第四款所稱連續英文字與連號數字係指輸入之所有內容具有字元連續性，如：ABCDE 或 12345678，惟下列案例不視為連續英文字或連號數字：ABC123。預設密碼係指系統隨機產生之密碼，該預設密碼得為相同英數字、連續英文字或連號數字。</p> <p>三、第二項第八款規定電子支付機構於使</p>

<p>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。</p> <p>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。</p> <p>六、密碼連續錯誤達五次時應限制使用，須重新申請密碼。</p> <p>七、變更後之密碼不得與變更前二次密碼相同。</p> <p>八、密碼超過一年未變更，電子支付機構應做妥善處理。</p> <p>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。</p>	<p>用者密碼超過一年未變更時，應作妥善處理，如可為主動通知、於下次使用者登入時通知或強迫變更密碼。</p>
<p>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：</p> <p>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：</p> <p>(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。</p> <p>(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。</p> <p>(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</p>	<p>一、定明電子支付機構業務之交易類型及其交易安全設計。</p> <p>二、如使用者以信用卡線上支付、超商付款或其他實體通路付款等方式，因未採用本條之安全設計，無須列入交易額度計算，惟其款項仍經過電子支付帳戶進行代理收付。</p> <p>三、如使用者與電子支付機構以契約約定使用者於實質交易提出支付指示時，電子支付機構得於一定期間後才執行移轉者，該執行動作無須列入交易額度計算。</p> <p>四、如單筆實質交易付款金額為新臺幣三千元，因屬每筆付款金額未達等值新臺幣五千元者，電子支付機構可設計一律採用 A 類交易安全設計或由使用者自行決定以 A、B、C 或 D 任一類交易安全設計進行支付。</p>

<p>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。</p> <p>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：</p> <p>(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。</p> <p>(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。</p> <p>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。</p>	
<p>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：</p> <p>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。</p> <p>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。</p> <p>三、C 類交易安全設計：指採用下列任一款之安全設計：</p> <p>(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。</p>	<p>一、第一項依據前條各類交易安全設計之具體要求。</p> <p>(一)如採用 A 類交易安全設計，應進行使用者風險分析，依據使用者操作環境、連網地點、購物習慣等資訊，評估該筆交易是否必須再次輸入密碼，以維交易安全。</p> <p>(二)簡訊被竊資安事故時有所聞，考量使用者操作便利，採用 B 類交易安全設計前，應進行組織風險評估，並針對使用者操作環境、連網地點、購物習慣等進行風險分析，如有必要應增加其他防護機制(如設備指定、推播確認、郵件回覆等)。</p> <p>(三)採用一次性密碼之安全設計須採經使用者與電子支付機構所約定持有之實體設備；該實體設備應妥善保護產製一次性密碼所需要的個人化資料。如</p>

<p>(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。</p> <p>(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：</p> <ol style="list-style-type: none"> 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。 <p>四、D 類交易安全設計：指採用下列任一款之安全設計：</p> <p>(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。</p> <p>(二)採用符合電子簽章法之安全設計。</p> <p>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</p>	<p>實體設備與交易設備為同一台設備(如使用行動裝置產生 OTP 並透過 APP 提出支付指示)，則應於使用者端經由人工確認(如抽拔卡、特殊按鍵等)交易內容後才完成交易。</p> <p>(四)電子支付機構如採用二項(含)以上技術：</p> <ol style="list-style-type: none"> 1. 所採用之約定資訊(如密碼)須於契約內要求使用者妥善保管。 2. 所採用之實體設備須可由電子支付機構於註冊與交易時進行設備確認；上述機制應先進行評估，如無法適用所有設備或無法透過契約取得技術提供者之承諾時，應改用其他機制。 3. 採用生物特徵時，須隨時調整錯誤接受度，必要時應增加多項不同種類生物特徵或其他輔助機制。 <p>二、第二項規定前項第四款第二目採用符合電子簽章法之安全設計如使用憑證機制之相關要求。</p> <p>(一)第一款規定憑證作業辦法應描述其適用範圍包含電子商務或其他相關業務。</p> <p>(二)第二款規定憑證機構應簽發符合電子簽章法之憑證，電子支付機構依據本辦法及憑證機構之憑證作業辦法辦理，以符合訊息不可否認。</p> <p>(三)第三款規定電子支付機構得擔任憑證註冊中心，簽發憑證給使用者使用。</p> <p>(四)第四款規定須以有效憑證申請新憑證，一旦憑證失效應重新申請。</p> <p>(五)第五款規定電子支付機構選擇合作憑證機構時，應考量憑證機構之賠償責任，以分散交易風險。</p> <p>(六)第六款規定電子支付機構得選用政府憑證作為註冊時之身分確認。</p> <p>(七)第七款規定驗證憑證有效性可下載最新憑證註銷清單比對，或向憑證機構</p>
---	---

<p>要求如下：</p> <ol style="list-style-type: none"> 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。 	<p>線上查詢最新憑證狀態。</p> <p>(八)第八款規定為確保憑證私鑰安全，目前不接受將私鑰儲存於電腦或行動裝置內，應儲存於安全晶片硬體。如憑證私鑰放置於行動裝置安全晶片內，使用者亦透過行動裝置進行支付指示，則應增加人工確認機制，以防止惡意程式逕行發送支付指示。</p>
<p>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：</p> <ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 一、定明不同連線類型之安全規定，其中支付指示符合訊息不可否認性之安全設定，須採用前條第一項第四款第二目之交易安全設計。 二、訊息來源辨識性係指電子支付機構應辨識外部網站及其所傳送交易資料之正確性。

<p>防護措施。</p> <p>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。</p>	
<p>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：</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>四、訊息不可重複性：應採用序號、時間戳記等機制產生。</p> <p>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。</p>	<p>一、定明密碼學之訊息隱密性、完整性、來源辨識性、不可重複性及不可否認性之安全設計要求。</p> <p>二、SHA1 演算法已不建議擴大使用，電子支付機構於長期應考量改用較高安全強度之演算法。</p> <p>三、訊息不可否認性之安全設計不得採用 SHA1 演算法。</p>
<p>第十條 電子支付平臺之設計原則應符合下列要求：</p> <p>一、網際網路應用系統設計要求：</p> <p>(一)載具密碼不應於網際網路上傳</p>	<p>一、定明電子支付平臺之設計原則。</p> <p>二、第一款規定網際網路應用系統設計要求。</p> <p>(一)第三目規定電子支付機構與金融機</p>

<p>輸，機敏資料於網際網路傳輸時應全程加密。</p> <p>(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。</p> <p>(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。</p> <p>(四)應辨識使用者輸入與系統接收之支付指示一致性。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(八)應設計個人資料顯示之隱碼機制。</p> <p>(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。</p> <p>(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。</p> <p>二、實體通路支付服務程式設計要求：</p> <p>(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。</p> <p>(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</p>	<p>構、電子商務公司或跨境公司等機構進行訊息交換時，須確認訊息來源及交易資料正確性。</p> <p>(二)第四目規定為避免中間人竄改支付指示，電子支付平臺應確認所接收之指示與使用者輸入一致。</p> <p>(三)第七目因變更個人資料(含電話、電子郵件信箱與住址等)可能發生偽冒支付，故須加強身分確認。</p> <p>(四)第八目規定隱碼機制，使個人資料去識別化。</p> <p>(五)第十目規定電子支付平臺應建置使用者交易行為分析功能(得依據使用者購貨類別、往來商家、消費時間、消費金額、累計金額、連網地點、常用往來電子支付帳戶等進行分析)。</p> <p>三、第二款第二目規定圖片、條碼或檔案可為交易內容、支付指示或儲值款項。若為未指定交付對象者，應考量存取限制、次數限制及有效期限。</p> <p>四、第三款規定使用者端程式應能避免使用者下載非電子支付機構程式及連結非電子支付機構應用系統，另應避免將機敏資料儲存於使用者端，如有必要應加強保護。</p> <p>五、第四款規定行動裝置應用程式要求。</p> <p>(一)第二目應避免使用者下載非電子支付機構行動裝置應用程式。</p> <p>(二)第三目應提醒使用者使用遭破解行動裝置之風險。</p> <p>(三)第五目規定行動裝置應用程式非瀏覽器，採用憑證進行傳輸加密，應確認上層憑證之有效性，避免中間人竊取機敏資料。</p> <p>六、第五款說明約定連結存款帳戶付款係為提供使用者於電子支付平臺委由電子支付機構代為辦理金融機構存款帳</p>
--	--

<p>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。</p> <p>三、使用者端程式設計要求：</p> <p>(一)應採用被作業系統認可之數位憑證進程式碼簽章。</p> <p>(二)執行時應先驗證網站正確性。</p> <p>(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。</p> <p>四、行動裝置應用程式設計要求：</p> <p>(一)應針對所需最小權限進行存取控制。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>五、約定連結存款帳戶付款設計要求：</p> <p>(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</p>	<p>戶資金移轉至該使用者本人之電子支付帳戶。</p> <p>(一)第二目規定金融機構得受理電子支付機構使用者辦理代扣作業，註冊時金融機構應以其既有機制驗證使用者；不同驗證機制得進行不同交易額度。</p> <p>(二)第三目規定電子支付機構以其憑證簽章向金融機構提出代理使用者辦理帳戶扣款作業，金融機構驗證無誤後，依據使用者註冊時授權之交易金額與指定帳戶，進行轉帳。</p> <p>(三)第四目規定電子支付機構可憑藉專屬憑證向金融機構提出代理各使用者辦理帳戶扣款作業，該憑證私鑰須妥善保管並增加存取控管。</p> <p>(四)第六目金融機構得以轉帳、匯款、FXML、ACH 等方式辦理資金移轉。</p> <p>七、第六款依據本條例第十七條規定，定明再確認之安全設計。得以交易確認頁面、郵件及簡訊等方式通知，經付款方再確認後，才能進行交易；如透過其他方式(如超商代收或其他實體通路付款等)進行付款者，於其付款時可視為再確認。</p>
---	---

<p>認。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>六、再確認之設計要求：</p> <p>(一)收到支付指示後，以信用卡線上</p>	
--	--

<p>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。</p> <p>（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。</p>	
<p>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：</p> <p>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。</p> <p>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。</p> <p>三、應訂定資訊作業相關管理及操作規範。</p> <p>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。</p> <p>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。</p> <p>六、應定義人員角色與責任並區隔相互衝突的角色。</p> <p>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。</p>	<p>一、定明電子支付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。</p> <p>二、第四款規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。</p> <p>三、第五款規定應依據流程建立資產清冊、內容包括軟硬體、表單、作業流程及架構圖。</p> <p>四、第六款規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。</p> <p>五、第七款規定應定期提供適當教育訓練（如個人資料保護、消費者保護、防制洗錢及打擊資助恐怖主義、資訊安全等）。</p>
<p>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：</p> <p>一、應建立人員之註冊、異動及撤銷註</p>	<p>一、定明電子支付平臺之人員管理。</p> <p>二、第一款規定應建立人員清冊並配置適當權限，針對重要作業（如撥款、程式</p>

<p>冊程序，用以配置適當之存取權限。</p> <p>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。</p> <p>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。</p> <p>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)。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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)。</p> <p>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。</p>	<p>異動)得由另一位人員進行審核與放行。</p> <p>三、第三款規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操作稽核軌跡。</p> <p>四、第四款規定應定義那些作業：如最高權限帳號使用、程式異動、參數變更、帳款撥款、帳款調整、資料異動等作業。</p> <p>五、第五款規定為防止使用者個人資料外洩，如人員離開時應限制畫面呈現。</p> <p>六、第六款規定系統維運人員未直接登入電子支付平臺，而是登入電子支付平臺之作業系統(如 Windows、UNIX 等)進行系統異動或資料庫存取，仍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)。此人為操作紀錄應於使用後由另一人員進行覆核。</p> <p>七、第七款規定覆核共用帳號之操作紀錄時應能區分人員身分。</p> <p>八、第八款規定人員使用之密碼至少三個月變更一次；系統使用之密碼如無法三個月變更一次，可採用其他補強管控方式(如 FTP 密碼檔限制人員存取或該伺服器限制人員登入)。</p> <p>九、第九款規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。</p>
<p>第十三條 電子支付作業環境之個人資料</p>	<p>一、定明電子支付作業環境之個人資料保</p>

<p>保護應符合下列要求：</p> <p>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：</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>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：</p> <p>(一)實施適宜之存取管制。</p> <p>(二)訂定妥善保管媒介物之方式。</p> <p>(三)依媒介物之特性及其環境，建置適當之保護設備或技術。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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</p>	<p>護，相關條文係參考「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」第九條、第十一條、第十二條、第十四條及第十五條等規定訂定。</p> <p>二、第四款規定應就個人資料建立清冊、進行風險評估與控管。</p> <p>三、第五款具體說明至少需留存內容，包含人/事/時/地/物，並設計辨識機制(如浮水印)，以利事後追蹤個人資料使用狀況。</p> <p>四、第六款規定資料外洩防護機制須可以偵測透過輸出入裝置(如 USB、CD/DVD、紅外線、藍芽、COM 或 LPT 等)、通訊軟體(如電子郵件、WebMail、Skype、檔案分享、Instant Message(IM)軟體或瀏覽器等)及系統操作(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等情形，並留存軌跡與數位證據。</p> <p>五、另該辦法第十條規定已訂於本辦法相關條文，說明如下：</p> <p>(一)使用者身分確認及保護機制：本辦法第四條及第五條。</p> <p>(二)個人資料顯示之隱碼機制：本辦法第十條第一款。</p> <p>(三)網際網路傳輸之安全加密機制：本辦法第八條及第九條。</p> <p>(四)軟體驗證與確認程序：本辦法第十九條。</p> <p>(五)檔案及資料庫之存取控制與保護監控措施：本辦法第十條第一款。</p> <p>(六)外部網路入侵對策：本辦法第十七條。</p> <p>(七)異常使用行為之監控：本辦法第十二條。</p>
---	---

<p>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。</p> <p>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：</p> <p>(一)刪除、停止處理或利用之方法、時間。</p> <p>(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。</p> <p>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：</p> <p>(一)檢視及修訂相關個人資料保護事項。</p> <p>(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。</p> <p>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。</p>	
<p>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：</p> <p>一、如有下列情形者應建立訊息隱密性機制：</p> <p>(一)機敏資料儲存於使用者端操作環境。</p> <p>(二)機敏資料於網際網路上傳輸。</p> <p>(三)使用者身分識別資料(如密碼、個人化資料)儲存於系統內。</p> <p>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</p>	<p>一、定明電子支付平臺之機敏資料隱密及金鑰管理。</p> <p>二、第一款規定三種情形須採用第九條訊息隱密性之安全防護措施。</p> <p>三、第二款規定使用者之固定密碼須進行不可逆運算，以防止系統維運人員知悉；須加密，以防止取得不可逆資料透過網路找出可用密碼；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。</p> <p>四、第三款規定應妥善產製並保護硬體安全模組之主金鑰。</p>

<p>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。</p> <p>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。</p> <p>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。</p> <p>五、當金鑰使用期限將屆或有洩漏疑慮時，應進行金鑰替換。</p>	<p>五、第四款規定應集中管理金鑰，避免過度分散。</p>
<p>第十五條 電子支付平臺之實體安全應符合下列要求：</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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</p>	<p>一、定明電子支付平臺之實體安全。</p> <p>二、第一款規定係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」。</p> <p>三、第二款規定機房應建立門禁管制，如採用單一身分確認機制(如密碼、鑰匙等)，應採相關措施防止遭冒用風險。建議可採用二項(含)以上身分確認。</p> <p>四、第三款規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。</p> <p>五、第五款規定油槽儲存及消防安全應符合相關法規規定，如公共危險物品及可燃性高壓氣體設置標準暨安全管理辦法及各類場所消防安全設備設置標準等規定。機房得採用可降低氧濃度、冷卻起火源、去除可燃物及抑制連鎖反應之全自動滅火系統並評估設置極早期火災預警系統。</p> <p>六、第六款規定應設置環境監控系統並自動告警與通知。人員應於接獲通知後，儘速到達現場並採取適當措施。</p>

<p>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。</p> <p>五、油槽儲存及消防安全應符合相關法規規定。</p> <p>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。</p> <p>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。</p> <p>前項第七款監控室應符合下列要求：</p> <p>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。</p> <p>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。</p> <p>三、連線過程須以內部網路、專線或虛擬私有網路進行。</p> <p>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。</p>	
<p>第十六條 電子支付作業環境之營運管理應符合下列要求：</p> <p>一、應避免於營運環境安裝程式原始碼。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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</p>	<p>一、定明電子支付作業環境之營運管理。</p> <p>二、第一款規定除部分程式(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。</p> <p>三、第三款規定應建立回存測試機制，定期確認。</p> <p>四、第四款規定應留存相關紀錄(如登入紀錄、操作紀錄、異常紀錄、作業紀錄、交易紀錄、軌跡紀錄、覆核紀錄、演練紀錄及掃描紀錄等)之要求，並確保數位證據之收集、保護與適當管理程序，至少留存二年。</p>

<p>法。</p>	<p>五、第五款規定得參考政府組態基準 (Government Configuration Baseline, GCB)、支付卡產業資料安全標準 (Payment Card Industry Data Security Standard, PCI DSS)、ISO 27001 機構等所提出之系統安全強化建議,訂定電子支付作業環境(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。</p>
<p>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：</p> <p>一、應偵測網頁與程式異動，紀錄並通知相關人員處理。</p> <p>二、應偵測惡意網站連結並定期更新惡意網站清單。</p> <p>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。</p> <p>四、應建立病毒偵測機制並定期更新病毒碼。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>一、定明電子支付作業環境之脆弱性管理。</p> <p>二、第一款規定，一旦電子支付平臺發生網頁、參數、程式與服務異動，應能立即通知系統維護人員；如為正常程序，應由另一位人員覆核其異動作業。</p> <p>三、第五款規定應針對電子支付平臺及系統維護人員進行上網管制，以避免植入惡意程式。</p> <p>四、第六款規定應隨時掌握資安事件，評估該事件對電子支付機構之影響並採取適當措施。</p> <p>五、第七款規定應定期對系統維護人員進行社交工程演練，並訂定衡量標準(如郵件開啟率、網站點擊率、附件下載率等)。</p> <p>六、第八款規定應針對電子支付作業環境進行弱點掃描，評估該弱點對電子支付機構之影響並採取適當措施。</p> <p>七、第九款規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(如可執行白名單)。</p> <p>八、第十款規定如程式長時間未異動，仍應配合掃描程式之更新進行掃描，以因應新型態之攻擊手法，電子支付機構可依據暴露風險(如放置於 DMZ 之系統)制定定期掃描時間。</p> <p>九、第十一款規定滲透測試得依據已知的</p>

<p>十、電子支付平臺上線前及每半年應針對異動程式進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。</p> <p>十一、電子支付平臺每年應執行滲透測試，以加強資訊安全。</p>	<p>程式碼弱點或黑箱測試報告進行驗證外，另應能考量電子支付平臺之架構與商業邏輯進行測試。</p>
<p>第十八條 電子支付作業環境之網路管理應符合下列要求：</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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</p>	<p>一、定明電子支付作業環境之網路管理。</p> <p>二、第一款規定透過防火牆管理電子支付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。</p> <p>三、第二款規定透過防火牆將電子支付作業環境與其他系統(如金融機構之網路銀行、電子票證業之電子票證)區隔。</p> <p>四、第四款規定應針對高風險設定(如 any IP、any port)及六個月內無流量之防火牆規則定期評估並儘速停用。</p> <p>五、第五款規定為能維持系統可用度，系統維運人員得透過遠端連線進行系統管理作業，惟不得將連線密碼紀錄於工具軟體(如 SSH、VPN、TLS 等)，防止惡意程式竊取連線密碼。得評估採用二項(含)以上或一次性密碼等安全設計登入電子支付平臺之作業系統。</p> <p>六、第六款規定不得以內部無線網路連線至電子支付作業環境。採用內部無線網路連線至其他內部環境時，應使用必要防護措施進行隔離。</p> <p>七、第七款規定為能維持系統可用度，系統維運人員得透過遠端連線進行系統管理作業，並應經審查及授權，每次使用須再次取得主管授權、留存操作紀錄及主管覆核。</p>

<p>子支付作業環境，並應使用必要防護措施進行隔離。</p> <p>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：</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(五)應建立監控機制，留存操作紀錄，並由主管定期覆核。</p>	
<p>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：</p> <p>一、應訂定資訊安全開發設計規範並落實執行。</p> <p>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。</p> <p>三、應確保系統軟體和應用軟體安裝最新安全修補程式。</p> <p>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。</p> <p>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。</p> <p>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，</p>	<p>一、定明電子支付作業環境之系統生命週期管理。</p> <p>二、第一款規定應將資訊安全要求訂定於開發設計規範。</p> <p>三、第二款規定系統委外開發應監督其依據本辦法規定辦理。</p> <p>四、第三款規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。</p> <p>五、第四款規定測試用之機敏資料(如金鑰)不應與營運環境相同，且應妥善保護。</p> <p>六、第五款規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；營運環境變更需要二人以上進行，針對變更內容進行檢視。</p> <p>七、第六款規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。</p>

<p>應建立程式原始碼管理機制，以符合職務分工與牽制原則。</p>	
<p>第二十條 電子支付作業環境之委外管理應符合下列要求：</p> <p>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。</p> <p>二、委託契約或相關文件中，應明確約定下列內容：</p> <p>(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。</p> <p>(二)對受託廠商應依本辦法內容進行適當監督。</p> <p>(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。</p> <p>(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。</p> <p>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。</p>	<p>一、定明電子支付作業環境之委外管理。</p> <p>二、第一款規定應制定廠商評估條件，遴選合適廠商，依據委外項目給予最小權限，安裝必要管控工具，以利其符合電子支付機構之資訊安全管控要求。</p> <p>三、第二款規定相關資訊安全要求應記載於委外契約內。</p> <p>四、第三款規定電子支付機構應對委外廠商進行資訊安全稽核；亦可接受由委外廠商提交經第三方出具之資訊安全稽核報告。</p>
<p>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：</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>一、定明電子支付作業環境之資訊安全事故管理。</p> <p>二、第一款規定應建立收納相關設備日誌機制，進行交叉比對，訂定監控項目與指標。</p> <p>三、第二款規定應建立通報程序與應變計畫，定期演練並留存作業紀錄。</p> <p>四、第三款規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。</p>
<p>第二十二條 電子支付作業環境之營運持</p>	<p>一、定明電子支付作業環境之營運持續管</p>

<p>續管理應符合下列要求：</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>理。</p> <p>二、第一款規定應對使用者承諾電子支付平臺服務時間與水準，定義最大可接受系統中斷時間，並評估異地備援機制之必要，以維持交易可用性。</p> <p>三、第二款規定應評估重大資訊系統事件(如大量電腦中毒、資料外洩、外部入侵等)或天然災害(如火災、颱風、地震等)之可接受範圍，投入相對應之資源，並建立各項應變程序。</p> <p>四、第三款規定應每年針對電子支付平臺各項服務進行演練，驗證營運持續性控制措施之有效性。</p>
<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>一、定明電子支付機構應遵循相關法令。</p> <p>二、第一項規定應盤點與資訊安全相關法規，如個人資料保護法、洗錢防制法、金融消費者保護法或其他主管機關規定、主管機關函令及公會自律規範等，定期辦理法令遵循自評，以確保電子支付機構符合相關規定。</p> <p>三、第二項規定應於申請電子支付機構業務時及其後每年委由會計師，針對本辦法各項要求進行資訊安全檢視並提出評估報告。</p> <p>四、第三項規定缺失單位應提出改善方案與預計時程，必要時應經高階主管審查同意；電子支付機構內部稽核單位應針對評估報告之缺失改善事項與預計時程進行追蹤覆查。針對評估報告、缺失改善紀錄、追蹤覆查紀錄應至少保存二年。</p>
<p>第二十四條 本辦法自中華民國一百零四</p>	<p>配合本條例之施行，定明本辦法之施行日</p>

年五月三日施行。

期。