

三、資訊作業

項 目 編 號	查 核 事 項	法 令 規 章
1	(一)資訊組織管理	
1.1	1.資訊安全政策是否經董事會、常董會決議或經其授權之經理部門核定，並對所有員工及相關外部各方公布傳達？	電子支付機構資訊系統標準及安全控管作業基準第 14 條
1.2	2.是否訂定資訊作業相關管理及操作規範，並每年檢討修訂？	
1.3	3.是否依據電子支付平臺之作業流程，識別人員、表單、設計、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？	
1.4	4.是否定義人員角色及責任並區隔相互衝突的角色？	
1.5	5.是否於每年四月底前由會計師檢視提出資訊系統及安全控管作業評估報告？	電子支付機構資訊系統標準及安全控管作業基準第 27 條
1.6	6.辦理電子支付機構業務之資訊系統及其備援系統是否置於我國境內？若否，是否符合主管機關可立刻、直接、完整、持續取得相關資訊之情形，並經主管機關核准？	電子支付機構業務管理規則第 44 條
2	(二)網路及資訊系統安全	電子支付機構資訊系統標準及安全控管作業基準第 20、21 條
2.1	1.機敏資料是否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？	

項 目 編 號	查 核 事 項	法 令 規 章
2.2	2. 電子支付作業環境與其他網路間之連線是否透過防火牆或路由器進行控管？	
2.3	3. 系統是否僅得開啟必要之服務及程式，使用者及特約機構僅能存取已被授權使用之網路及網路服務？	
2.4	4. 是否每年檢視防火牆及具存取控制（Access control list, ACL）網路設備之設定？每年檢視防火牆是否開啟具安全性風險或非必要之通訊埠，連線設定是否有安全性弱點？	
2.5	5. 經由網際網路連接至內部網路進行遠距之系統管理工作，是否至少每年審查一次申請使用及授權之適當性？若涉及變更作業，是否採用照會或二項(含)以上安全設計並經主管授權？是否定義可連結之遠端設備並建立監控機制？	
2.5.1	(1) 如使用虛擬私有網路（VPN），是否訂定作業規範，建立日誌檢視、攻擊偵測、事件應變及事件復原機制，並採用高強度密碼或多因子進行身分驗證？	
2.5.2	(2) 如使用異地辦公之虛擬桌面（VDI），是否訂定作業規範，避免連接本機印表機印出檔案、連接可卸除裝置存取檔案或透過剪貼簿於兩端剪貼資料，並採用高強度密碼或多因子進行身分驗證？	
2.6	6. 是否建立偵測網頁與程式異動及惡意網站連結，並通知相關人員處理？	

項 目 編 號	查 核 事 項	法 令 規 章
2.7	7.是否建立入侵偵測或病毒偵測機制並定期更新惡意程式行為特徵與病毒碼？	
2.8	8.是否建立上網管制措施，並至少每年辦理一次電子郵件社交工程演練？	
2.9	9.電子支付平臺上線前及每半年是否針對異動程式進行程式碼掃描或黑箱測試，並對其掃描或測試結果進行風險評估？	
2.10	10.是否每季進行資訊系統弱點掃描，並確認掃描工具為新版本？電子支付平臺是否每年執行滲透測試，並依風險等級進行處理及留存紀錄？	
2.11	11.對已停止弱點修補或更新之系統軟體與應用軟體，是否採取必要防護措施？	
2.12	12.是否對客戶加強資安觀念宣導，提醒客戶除應於個人電腦或行動裝置上設定密碼保護機制外，並應安裝防毒軟體，以提升網路交易安全性？	
2.13	13.對金融資安資訊分享與分析中心(F-ISAC)資安情資之接收與處理，是否建立妥善管理機制？	
2.13.1	(1)是否依金融資安資訊分享與分析中心(F-ISAC)所訂「情資分享管理辦法」，建立資安情資內部作業處理流程與規範，並妥善處置所接收之資安情資？	
2.13.2	(2)對所訂資安情資處理流程之相關控制措施，是否建立定期檢視機制，以確認其有效性？	

項 目 編 號	查 核 事 項	法 令 規 章
2.13.3	(3)是否依內部控制三道防線機制，對資安警訊處理機制加強辦理自行查核及內部稽核？	電子支付機構資訊系統標準及安全控管作業基準第 11 條
2.14	14.針對其他網路區域所連接具 IP 網路連線功能並實際連線於 Internet 或 Intranet 之辦公設備，是否建立管理清冊並定期更新，每年至少盤點一次並留存紀錄？是否具備安全性更新機制，或限制其網際網路連線能力、加強存取控制或進行網路連線行為監控？	
3	(三)系統運作管理	
3.1	1.電子支付平臺之設計原則，是否符合下列規定：	
3.1.1	(1)網際網路應用系統：	
3.1.1.1	①載具密碼不應於網際網路上傳輸，機敏資料傳輸應全程加密。	
3.1.1.2	②使用者或特約機構超過十分鐘未使用應中斷其連線或採取其他保護措施。	
3.1.1.3	③應辨識合作第三方網站或應用系統傳送之訊息，並妥善保護使用者及特約機構資料。	
3.1.1.4	④應辨識使用者輸入與系統接收之支付指示一致性。	
3.1.1.5	⑤應設計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。	
3.1.1.6	⑥應避免存在網頁程式安全漏洞(如 Injection、	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.1.7	Cross-Site Scripting 等)。	
3.1.1.8	⑦應偵測網頁與程式異動時，進行紀錄與通知措施。	
3.1.1.9	⑧採用固定密碼進行身分確認應加強安全機制。	
3.1.1.10	⑨個人資料顯示之隱碼。	
3.1.2	⑩建置防偽冒與洗錢防制偵測機制。	
3.1.2.1	(2)實體通路支付服務程式：	
3.1.2.2	①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。	
3.1.3	②辦理代理收付實質交易、儲值卡款項移轉交易或辦 理國內外小額匯兌時，如將支付指示記錄於圖片、 條碼或檔案，應經使用者確認；如將前述媒體透過 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。	
3.1.3.1	(3)使用者及特約機構端電腦應用程式：	
3.1.3.2	①應採用被作業系統認可之數位憑證進程式碼簽 章。	
3.1.3.3	②執行時應先驗證網站正確性。	
3.1.3.4	③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)。	
	④採用晶片金融卡辦理國內外小額匯兌時，須於使用	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4	者端經由人工確認交易內容後才完成交易。	
3.1.4.1	(4)使用者及特約機構端行動裝置應用程式： ①應建立應用程式發布程序，由兩人以上或採用兩項(含)以上技術管控。	
3.1.4.2	②應於發布前檢視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、法遵及風控等主管同意，以利綜合評估是否符合「個人資料保護法」之告知義務。	
3.1.4.3	③偵測行動裝置疑似遭破解(如 root、jailbreak、USB debugging 等)，應提示使用者注意風險並限制辦理國內外小額匯兌。	
3.1.4.4	④應於顯著位置(如官網、應用程式下載頁面等)提示使用者及特約機構於行動裝置上安裝防護軟體。	
3.1.4.5	⑤應於官網上提供應用程式之名稱、版本與下載位置。	
3.1.4.6	⑥應建立偽冒應用程式偵測、下架或告警機制。	
3.1.4.7	⑦應每年由合格實驗室依據行動應用資安聯盟「行動應用 APP 基本資安檢測基準」辦理並通過檢測；針對應用程式及其應用伺服器之完整功能辦理程式碼掃描或黑箱測試，並修正中/高風險漏洞；辦理國內外小額匯兌者，應依據 OWASP 公布之 Mobile ApplicationSecurity Checklist L2 項目辦理檢測；應	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.8	建立檢測報告之檢視機制，並送資安專責主管監控及執行資訊安全管理作業。 ⑧應用程式及其應用伺服器新功能首次上線、系統架構異動或既有功能異動時，應針對新增或異動之程式辦理程式碼掃描或黑箱測試，並修正中/高風險漏洞；辦理國內外小額匯兌者，應依據 OWASP 公布之 Mobile Top 10 項目辦理檢測，並修正中/高風險漏洞。	
3.1.4.9	⑨採用行動裝置儲存金鑰之安全設計應於交易時增設存取控管或人工確認，限制由可信任行動應用程式存取金鑰，以防止遭受惡意程式發動阻斷服務攻擊或執行偽冒交易。	
3.1.4.10	⑩採用空中傳輸(OTA)方式下載敏感資料前，應確認使用者及特約機構身分、確認行動裝置及應用程式之正確性。	
3.1.4.11	⑪採用安全元件作為儲存裝置時，應確認使用者及特約機構指定之安全元件編號(如 SE ID)、並於 SE 內增設存取控管，限制由可信任應用程式存取。	
3.1.4.12	⑫辦理國內外小額匯兌並採用近距離無線通訊(NFC)技術進行付款交易資料傳輸者，應經由使用者人工確認其意思表示（如密碼、圖形驗證碼）。	
3.1.4.13	⑬採用 WebView、WebBrowser 存取具個人資料或認	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.14	證資訊(如固定密碼)之網頁時，應無留存記錄，或應依據使用者或特約機構授權範圍辦理。	
3.1.5	⑭行動應用程式有使用第三方函式庫或元件之需要時，應評估安全風險及妥善管控程序，並應留存評估記錄。	
3.1.5.1	(5)條碼掃描技術： ①條碼掃描支付過程中，所存取之資訊應遵循該業務所需最小化原則。	
3.1.5.2	②採用交易資訊類條碼者，應用程式應以彈出式視窗或其他方式提供接收方檢視條碼之資料內容，再由接收方處理後續事宜。	
3.1.5.3	③被掃模式採用交易指示類條碼者，應設定條碼合理使用時效，且在時效內以使用一次為限。	
3.1.5.4	④條碼受理終端所提交之條碼訊息請求應確保傳輸過程中的資訊完整性及隱密性，並確保在傳輸過程中不被篡改及洩露。	
3.1.5.5	⑤條碼受理終端相關應用程式，應能針對所解析之條碼進行格式檢查，確保資料格式合理性，預防程式碼注入。	
3.1.5.6	⑥條碼受理終端相關應用程式，應能針對所解析之交易指示類條碼進行來源辨識性及完整性檢查，對於未驗證通過之條碼應予明確提示並拒絕執行交易。	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.5.7	⑦條碼受理終端相關應用程式，對所解析之條碼產生網站連結，應採包括但不限於白名單或伺服器認證等機制進行網站合法性檢查，以預防連結惡意網站或執行惡意程式風險。	
3.1.5.8	⑧主掃模式及被掃模式等各類應用情境，所生成之交易指示類條碼收付不得共用，以確保專碼專用。	
3.1.6	(6)Application Programming Interface (API) 訊息交換：	
3.1.6.1	①應使用 HTTP 強制安全傳輸 (Http Strict Transport Security, HSTS) 協議，以防止 SSL 剝離 (Strip) 攻擊。	
3.1.6.2	②應正面表列並限制僅接受所需之 HTTP 請求方法 (如 GET、POST)。	
3.1.6.3	③應採用 HTTP 請求表頭 (header) content-type 欄位 (如 application/xml、application/json 等) 並確保回應內容與表頭所宣告內容類型 (content-type) 一致。	
3.1.6.4	④應進行欄位格式檢查以防止常見之網頁應用程式威脅 (如 Cross-Site Script、SQL Injection、Remote Code Execution 等)。	
3.1.6.5	⑤認證資訊 (如 credentials、password、tokens、API keys 等) 應採用標準之 HTTP 授權表頭 (Authorization header) 或本體 (Body) 傳送，不得以 URL 之參數形式傳送。	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.6.6	⑥應設定安全性表頭 (Security Headers)，限定代理存取端僅針對指定之內容類型進行處理 (X-Content-Type-Options: nosniff)，並防止辦理身分確認之網頁為其他網站嵌入 (X-Frame-Options: deny、sameorigin)。	電子支付機構資訊系統標準及安全控管作業基準第 17 條
3.1.7	(7) Software Development Kit (SDK) 軟體開發套件：應依據實際應用範圍，符合相關規範。	
3.1.8	(8)開放應用程式介面 (Open API)：如有使用第三方開放應用程式介面之需要時，應進行安全風險評估及妥善管控程序，並應留存評估記錄。	
3.2	2.電子支付平臺之機敏資料隱密及金鑰管理，是否符合下列要求：	
3.2.1	(1)如有機敏資料儲存於使用者或特約機構端操作環境、於網際網路上傳輸、使用者或特約機構身分識別資料 (如密碼、個人化資料) 儲存於系統內等情形，是否建立訊息隱密性機制？個人化資料如為生物特徵者，是否遵循銀行公會所訂自律規範辦理？	
3.2.2	(2)使用者或特約機構身分識別資料如為固定密碼者，是否於儲存時先進行不可逆運算 (如雜湊演算法)？	
3.2.3	(3)採用硬體安全模組保護金鑰者，該金鑰是否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？	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.4	(4)當金鑰使用期限將屆或有洩漏疑慮時，是否進行金鑰替換？	電子支付機構資訊系統標準及安全控管作業基準第 15 條
3.3	3.電子支付平臺之系統維運人員管理是否符合下列規定：	
3.3.1	(1)是否建立人員之註冊、異動及撤銷註冊程序，並依最小權限（least privilege）及僅知原則（need-to-know）配置適當之權限？	
3.3.2	(2)是否定期審查帳號與權限之合理性及異常存取紀錄？人員離職或調職時是否盡速移除權限？	
3.3.3	(3)最高權限帳號或具程式異動、參數變更權限之特權帳號，是否依使用人員職務範圍等予以限制？相關使用是否經核准並留存稽核軌跡？	
3.3.3.1	①應與日常維運帳號區隔，並列冊保管。	
3.3.3.2	②應使用特權帳號管理系統，採取適當之限制存取權限並評估設定之合理性，以降低帳號密碼洩露風險；無法由特權帳號管理系統納管之帳號，密碼應採兩人以上分持管理或其他管控措施，以符合作業牽制原則。	
3.3.3.3	③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，且定期覆核使用結果。	
3.3.3.4	④用於提供網際網路服務之伺服器及 AD（網域服務）主機者，應採雙因子認證。	

項 目 編 號	查 核 事 項	法 令 規 章
3.3.4	(4)帳號是否採一人一號管理？是否確認人員之身分與存取權限？必要時是否限定使用之機器與網路位置(IP)？	
3.3.5	(5)於登入作業系統進行系統異動或資料庫存取時，是否留存人為操作紀錄，並於使用後儘速變更密碼？若無法變更密碼者，是否建立監控機制，並於使用後覆核其操作紀錄？	
3.3.6	(6)加解密程式或具變更權限之公用程式(如資料庫存取程式)是否列冊管理並限制使用？是否設定存取權限，防止未授權存取，並保留稽核軌跡？	
3.4	4.電子支付機構對於使用者及特約機構，所採用之身分確認程序(包括確認行動電話號碼、確認金融支付工具、以臨櫃審查、符合電子簽章法之憑證簽章或透過視訊櫃員機，確認使用者身分)之安全設計是否符合規定？使用者及特約機構登入電子支付平臺時，是否進行身分確認，並依法規規定之安全設計登入？	電子支付機構資訊系統標準及安全控管作業基準第 7、8 條
3.5	5.電子支付機構對於代理收付實質交易(包括儲值卡進行線上即時交易、電子支付帳戶進行線上即時交易、儲值卡進行非線上即時交易)、收受儲值款項(包括儲值卡進行線上即時儲值交易、儲值卡進行非線上即時儲值交易)、辦理國內外小額匯兌、進行事先約定支付交易、帳務清算及結算交易，是否依不同應用範圍，採	電子支付機構資訊系統標準及安全控管作業基準第 9 條

項 目 編 號	查 核 事 項	法 令 規 章
	行對應之交易安全設計？	
3.6	6.約定連結存款帳戶付款之設計原則，是否符合下列要求：	電子支付機構資訊系統標準及安全控管作業基準第 10 條
3.6.1	(1)憑證私鑰是否儲存於符合法規或其他相同安全強度之硬體安全模組內並限制金鑰明文匯出？	
3.6.2	(2)是否建立控管機制，限制非授權人員或程式存取約定連結存款帳戶付款作業之相關程式？	
3.6.3	(3)是否要求專用存款帳戶銀行或開戶金融機構建立合理交易流量管控機制？	
3.7	7.電子支付平臺之系統生命週期管理，是否訂定資訊安全開發設計規範？系統軟體及應用軟體是否安裝最新安全修補程式？測試用的機敏資料是否進行遮蔽處理或管制保護？程式自行開發及變更是否遵循職能分工與牽制原則？是否留存完整紀錄？委外廠商交付之系統或程式是否確保無惡意程式及後門程式？放置於網際網路之程式是否通過程式碼掃描或黑箱測試？	電子支付機構資訊系統標準及安全控管作業基準第 22 條
3.8	8.環境及儲值卡端末設備面之安全需求及安全設計，是否符合下列要求：	電子支付機構資訊系統標準及安全控管作業基準第 12 條
3.8.1	(1)保持儲值卡端末設備與環境之實體完整性，是否採用下列安全設計：	
3.8.1.1	①定期檢視是否有增減相關裝置。	
3.8.1.2	②應確定與儲值卡端末設備合作廠商簽訂資料保密	

項 目 編 號	查 核 事 項	法 令 規 章
3.8.1.3	契約，並應將參與儲值卡端末設備安裝、維護作業之人員名單交付造冊列管。	
3.8.1.4	③儲值卡端末設備安裝、維護作業人員至現場作業時，均應出示經認可之識別證件。除安裝、維護作業外，並應配合隨時檢視儲值卡端末設備硬體是否遭到不當外力入侵或遭裝置側錄設備。	
3.8.2	④應不定時派員抽檢安裝於特約機構或電子支付機構之儲值卡端末設備，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。	
3.8.2.1	(2)確保儲值卡端末設備交易之安全性，是否符合下列規範：	
3.8.2.2	①儲值卡內含錄碼及資料，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儲值卡端末設備。	
3.8.2.3	②應確保儲值卡端末設備之合法性，另儲值卡端末設備應有唯一之儲值卡端末設備代號。	
3.8.3	③應用於單筆交易金額超過等值新臺幣一千元之交易，儲值卡端末設備之安全模組應個別化（即每一儲值卡端末設備之認證金鑰皆不相同）。	
	(3)是否建置管控名單管理機制？對於線上即時交易是否即時驗證？非線上即時交易是否每日更新管控名單？使用於網際網路交易功能者，是否即時驗證？	

項 目 編 號	查 核 事 項	法 令 規 章
3.8.4	(4)儲值卡端末設備於非接觸式讀卡機交易時，若詢卡發現一張以上的卡片回應，是否主動拒絕交易，並顯示交易失敗？是否配合採用其他技術防護措施，如消費行為分析或讀卡機 SAM 卡 sign on 檢查（軟體式 SAM 讀卡機除外）？交易過程是否有聲音、燈號或圖像等提示，以防止特約機構不當扣款？	電子支付機構資訊系統標準及安全控管作業基準第 13 條
3.8.5	(5)非線上即時儲值交易之儲值卡端末設備是否具有安全模組之設計，並進行妥善之管理(如製發卡與交貨控管流程、管制製卡作業、落實安全模組之安全控管等)？是否逐筆授權儲值交易、限制單筆儲值金額及總額？	
3.8.6	(6)採用具加解密運算能力晶片卡、記憶型晶片卡或磁條卡，且應用於提供單筆交易金額超過等值新臺幣一千元交易之特約機構，如管控名單之驗證未送回進行即時驗證者，是否採取降低偽卡交易之必要措施？	
3.8.7	(7)是否制定儲值卡端末設備管理規章？	
3.9	9.儲值卡之安全需求及安全設計，是否符合下列要求：	
3.9.1	(1)儲值卡是否具有獨立且唯一之識別碼或具有認證之功能，以確保其合法性？	
3.9.2	(2)採用密碼者，密碼是否不少於 4 位？錯誤五次是否限制使用，並須重新申請密碼？密碼變更是否不得於前次相同？首次登入是否強制變更密碼？	

項 目 編 號	查 核 事 項	法 令 規 章
3.9.3	(3)使用儲值卡儲存個人資料，是否設計存取控制或持卡人確認之機制，以限制其讀取？	電子支付機構資訊系統標準及安全控管作業基準第 26 條
3.9.4	(4)是否制定儲值卡交貨控管流程？	
3.10	10.電子支付核心系統轉換或架構重大調整且逾內部規範之最大可容忍中斷時間者，是否符合下列要求：	
3.10.1	(1)系統異動前之準備工作：是否建立架構審查機制？是否建立上線及復原計畫，並建立多個檢核點及啟動復原之決策條件？是否進行上線變更審查及風險評估，辨識複雜度及影響範圍？是否召開上線協調會議？是否請資安人員參與異動前關鍵準備工作，如：架構審查、上線變更審查及風險評估、上線協調會議等事項？	
3.10.2	(2)系統異動作業：是否執行系統及資料備份、驗證各項變更作業及資料內容？	
3.10.3	(3)系統異動後之事件管理：是否持續監控系統，確保資料正確、功能正常、系統穩定？是否成立應變小組，並落實事故應變？是否追蹤根因，提出短中長期改善方案並持續追蹤？	電子支付機構資訊系統標準及安全控管作業基準第 16 條
4	(四)個人資料安全保護	

項 目 編 號	查 核 事 項	法 令 規 章
4.1	1.為維護所保有個人資料之安全，是否採取下列資料安全管理措施：	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 9 條
4.1.1	(1)是否訂定各類設備或儲存媒體之使用規範？報廢或轉作他用時，是否採取防範資料洩漏之適當措施？	
4.1.2	(2)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，是否採取適當之加密措施？	
4.1.3	(3)作業過程有備份個人資料之需要時，對備份資料是否予以適當保護？	
4.2	2.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，是否實施適宜之存取管制？是否訂定妥善保管媒介物之方式？是否依媒介物之特性及其環境，建置適當之保護設備或技術？	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 11 條
4.3	3.為維護所保有個人資料之安全，是否依執行業務之必要，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？	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 12 條
4.4	4.是否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？是否編製個人資料清冊？是否進行風險評估與控管？	
4.5	5.是否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？	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 14 條

項 目 編 號	查 核 事 項	法 令 規 章
4.6	6.是否建立資料外洩防護機制？是否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？是否留存相關紀錄、軌跡與數位證據？	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 14 條
4.7	7.如刪除、停止處理或利用所保有之個人資料後，是否留存下列紀錄：	
4.7.1 4.7.2	(1)刪除、停止處理或利用之方法、時間。 (2)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。	
4.8	8.是否訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法，並落實執行各項安全維護措施(含定期辦理個人資料檔案清查及個人資料風險評估作業)？	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 3 條
4.9	9.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，是否定期辦理個人資料保護認知宣導及教育訓練？是否提出相關自我評估報告，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，自我評估報告是否訂定下列機制：	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 15 條
4.9.1	(1)檢視及修訂相關個人資料保護事項。	
4.9.2	(2)針對評估報告中有違反法令之虞者，規劃、執行改善	

項 目 編 號	查 核 事 項	法 令 規 章
	及預防措施。	
4.10	10.如自第三方機構(如電信業者)取得使用者或特約機構個人資料(如姓名、住址、電話、電子郵箱、繳款紀錄、電信評分等)者，是否要求第三方機構須事先取得使用者或特約機構同意？	
4.11	11.對依法具有調查權之機關(構)，要求提供使用者與特約機構之往來交易或其他相關資料：	
4.11.1	(1)是否要求該機關(構)正式備文，並表明為調查需要，註明案由，載明所需資料之內容及範圍？	電子支付機構提供使用者與特約機構往來交易資料及其他相關資料要點第 2 點
4.11.2	(2)提供使用者與特約機構之往來交易或其他相關資料予前開機關(構)，是否以密件處理，並提示該機關(構)及查詢者應予保密？	電子支付機構提供使用者與特約機構往來交易資料及其他相關資料要點第 6 點
5	(五)營運持續計畫及資安事件管理	
5.1	1.電子支付作業環境之營運持續管理，包括：	電子支付機構資訊系統標準及安全控管作業基準第 19、25 條
5.1.1	(1)備份媒體或檔案是否妥善保護？是否建立回存測試機制，以驗證備份之完整性及儲存環境之適當性？	
5.1.2	(2)是否進行營運衝擊分析，及是否建立重大資訊系統事件或天然災害之應變程序？應變程序內容是否包括相關資訊系統、設備、網路頻寬、人員等？	
5.1.3	(3)是否每年驗證及演練營運持續性控制措施，以確保其有效性，並保留相關演練紀錄及檢討演練結果？	

項 目 編 號	查 核 事 項	法 令 規 章
5.2	2.資訊安全事故管理，包括：	電子支付機構資訊系統標準及安全控管作業基準第 19、20、24 條
5.2.1	(1)是否將各作業系統、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，並設定合適告警指標並定期檢討修訂？原始日誌及稽核軌跡是否至少保存二年？	
5.2.2	(2)對監控及偵測之異常事件是否明確定義須通報之事件等級，並建置通報程序？	
5.2.3	(3)是否建置數位證據之收集、保護與適當管理程序，並至少留存二年？	
5.2.4	(4)是否隨時掌握資安事件，針對高風險或重要項目立即進行清查應變？	
5.2.5	(5)是否建立資訊安全事故評估、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？	電子支付機構業務管理規則第 29 條
5.3	3.提供收款使用者收付訊息整合傳遞或使用者間訊息傳遞服務，對所提供之端末設備及應用程式，是否採取適當防護及控管措施，以避免收付訊息遭洩漏或竄改？	
5.4	4.營運設備是否集中於機房內？機房是否建立門禁管制，以確保僅允許經授權人員進出？非授權人員進出是否填寫進出登記，並由內部人員陪同與監督？進出登記紀錄是否定期審查？	電子支付機構資訊系統標準及安全控管作業基準第 18 條
5.5	5.機房管理是否具備與機房相當之操作環境？	

項 目 編 號	查 核 事 項	法 令 規 章
6	(六)資訊作業委外管理	電子支付機構資訊系統標準及安全控管作業基準第 23 條
6.1	1.委外處理前是否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？	
6.2	2.委託契約或相關文件中，是否明確約定下列內容：	
6.2.1	(1)受託廠商應遵守規定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。	
6.2.2	(2)對受託廠商應依規定進行適當監督。	
6.2.3	(3)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。	
6.2.4	(4)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。	
6.3	3.是否定期要求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？	
6.4	4.支付核心系統之委外開發項目，專案成員是否有資安專責人員參與？是否妥善管理受託廠商之實體與邏輯存取權限；如涉個人資料交換，是否確認符合我國個人資料保護法相關規定？委外服務變更前，是否執行資訊安全風險評估並擬訂風險處理措施？	
6.5	5.委託作業涉及使用雲端服務管理，包括：	電子支付機構業務管理規則第 45-1 條

項 目 編 號	查 核 事 項	法 令 規 章
6.5.1	(1)是否訂定使用雲端服務之政策及原則，並採取適當風險管控措施？	電子支付機構資訊系統標準及安全控管作
6.5.2	(2)是否具專業技術及資源，監督雲端服務業者執行受託作業，或委託專業第三人輔助監督作業？	
6.5.3	(3)對於自行委託，或與委託同一雲端服務業者之金融機構聯合委託獨立第三人查核雲端服務業者，是否確認其查核範圍涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節？是否評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準？是否對所委託作業範圍進行查核並出具報告？	
6.5.4	(4)傳輸及儲存客戶資料至雲端服務業者，是否採行客戶資料加密或代碼化等有效保護措施？是否訂定妥適之加密金鑰管理機制？	
6.5.5	(5)對委託雲端服務業者處理之資料，是否保有完整所有權？除執行受託作業外，是否確保雲端服務業者不得有存取客戶資料之權限，並不得為委託範圍以外之利用？	
6.5.6	(6)委託雲端服務業者處理之客戶資料及其儲存地如位於境外，是否保有指定資料處理及儲存地之權利？境外當地資料保護法規是否低於我國要求？除經主管機關核准者外，客戶重要資料是否在我國留存備份？	
6.5.7		

項 目 編 號	查 核 事 項	法 令 規 章
	(7)是否訂定雲端服務緊急應變計畫及終止委託之移轉機制？緊急應變計畫是否包含如何確保順利移轉至另一雲端服務業者或移回自行處理，並確保原受託雲端服務業者留存資料全數刪除或銷毀？	業基準第 23 條