



PCI自我評估問卷

版本1.0

2004年12月

VISA PAYMENT SECURITY SERVICES
ASIA PACIFIC

免責聲明

這份支付卡產業（PCI）自我評估問卷是要用來當作一份「檢查項目表」，以確保儲存、處理，或傳送Visa持卡人資料的所有公司行號均遵守PCI資料安全標準，但是Visa Asia Pacific並不擔保，亦未聲稱填寫問卷或遵守問卷內容之規定即可避免安全違失或損失，另外並聲明，不論是否已實施自我評估問卷之建議，其所致之任何安全違失或損失，Visa Asia Pacific一概不負任何責任。

重要

支付卡產業（PCI）自我評估問卷是Visa Asia Pacific整套客戶資料安全（AIS）文件的一部份，所有會員及其代理商（特約商店及服務提供廠商）均必須確實按照PCI資料安全標準處理。儲存，以及傳送持卡人資料（本標準超越Visa 2000年3月之AIS標準v1.4）。

有關Visa Asia Pacific之AIS計畫詳情，歡迎上網 <http://www.visa-asia.com/secured> 查閱。

如何填寫問卷

本問卷分成六個部分，每一個部分都以一個特定的安全領域為中心，並以PCI資料安全標準中的要求為準。如有疑問而勾選「無資料」，即應附加簡短的說明。

問卷報告

自我評估問卷及系統週邊設備掃描結果中必須記載下列各項：

公司資料

公司名稱： DBA(S)：

聯絡人姓名： 職稱：

電話號碼： 電子郵件：

每年處理的大約交易量/客戶數量：

請對貴公司做概要的敘述。

貴公司在付款流程中扮演何種角色？貴公司如何儲存、處理及/或傳送持卡人資料，以及具備如何之能力？

列出所有的第三人服務提供廠商：

處理器： 閘道：

網路主機： 購物車：

其他地點： 其他：

列出使用的銷售點（POS）軟體/硬體：

評估結果評分

填寫評估表的各部分之後，填寫人應按下述填寫評分欄：

各部分如果...	則該部分之評分是 ...
所有問題均回答「是」或「無資料」	綠色 - 特約商店或服務提供廠商遵守PCI資料安全標準的自我評估部分。 註：如果勾選「無資料」，請附加簡短的說明。
有任何問題回答「否」	紅色 - 特約商店或服務提供廠商被視為未遵守要求，要達遵守要求之程度，風險必須加以解決，並必須再進行自我評估，以證實遵循規定。

第1部分：	綠色 紅色	第4部分：	綠色 紅色
第2部分：	綠色 紅色	第5部分：	綠色 紅色
第3部分：	綠色 紅色	第6部分：	綠色 紅色

整體評分： **綠色** **紅色**

建置及維持安全的網路

要求 1：安裝及維持一套防火牆配置以保護資料

問題	回答		
1.1 所有的路由器、交換機、無線存取點，以及防火牆組態是否均穩當，以及是否均符合明訂的安全標準？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.2 如果採用無線技術，則是否僅限於經過授權的裝置始能對網路進行存取？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 無資料
1.3 防火牆之變更是否需要經過授權，變更是否做成紀錄？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.4 為保護網路而使用防火牆，以及對於連線之限制，是否均為營運所必須？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.5 所有邊界路由器是否均安裝入口及出口過濾器，以防止用欺偽的IP位址偽裝？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.6 儲存支付卡帳號資料之資料庫是否位於內部網路（非DMZ），並由防火牆保護？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.7 如果使用無線技術，則無線網路及支付卡環境之間是否有周邊防火牆？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 無資料
1.8 和網際網路直接連結的各台移動式電腦是否有安裝個人的防火牆及防毒軟體？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 無資料
1.9 位於公眾得到達之網路區段的網路伺服器是否用防火牆（DMZ）和內部網路隔開？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.10 防火牆是否使用網路位址轉移（NAT）配置成會轉譯（隱藏）內部IP位址？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	

建置及維持安全的網路

要求 2：不可使用供應商提供的出廠預設值作為系統密碼及其他的安全參數

問題		回答		
2.1	生產系統在投入生產之前，是否先變更供應商在該系統上內建的安全設定？	<input type="checkbox"/>	<input type="checkbox"/>	
		是	否	
2.2	生產系統在投入生產之前，是否先使供應商內建的帳號和密碼失效，或是變更該生產系統？	<input type="checkbox"/>	<input type="checkbox"/>	
		是	否	
2.3	如果使用無線技術，是否變更供應商內建的設定（亦即WEP金鑰、SSID、密碼、SNMP共用字串、解除SSID廣播功能）？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> 無資料
		是	否	
2.4	如果使用無線技術，則是否在具備WPA功能時，採用Wi-Fi保護存取（WPA）技術加密及驗證？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> 無資料
		是	否	
2.5	是否所有的生產系統（伺服器及網路元件），藉由移除內建配置所安裝之所有非必要的服務及通訊協定後變得堅固？	<input type="checkbox"/>	<input type="checkbox"/>	
		是	否	
2.6	生產系統及應用程式之遠端管理是否使用安全、加密的傳輸？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> 無資料
		是	否	

保護持卡人資料

要求 3：保護儲存的資料

問題	回答
3.1 不再需要時，是否安全的處置敏感的持卡人資料？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
3.2 是否禁止儲存資料庫、紀錄表檔案，或是銷售點產品中（位在卡片背面、晶片中等）磁條上任何磁軌的全部內容？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
3.3 是否禁止儲存資料庫、紀錄表檔案，或是銷售點產品中的卡片確認碼（卡片簽名欄上列印的三碼數值）？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
3.4 顯示持卡人資料時，是否隱藏全部的帳號，只顯示帳號的最後四碼？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
3.5 （資料庫、紀錄表、檔案、備份媒體等內的）帳號是否安全的儲存 — 例如以加密或切截的方式？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
3.6 帳號登入稽核紀錄表之前是否先經清除處理（sanitized）？	<input type="checkbox"/> 是 <input type="checkbox"/> 否

要求 4：將透過公共網路傳送之持卡人資料及敏感資料加密

問題	回答
4.1 透過公共網路傳送之敏感持卡人資料，是否使用SSL或業界可接受之其他方法加密？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
4.2 如果使用SSL傳送敏感的持卡人資料，是否使用128-位元加密的3.0版？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
4.3 如果使用無線技術，是否使用Wi-Fi保護存取（WPA）、VPN、128-位元之SSL或WEP將傳輸加密？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
4.4 如果使用無線技術，是否使用128-位元之WEP及其他的加密技術，共用的WEP 金鑰是否每季調換一次？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
4.5 透過電子郵件傳送帳號時，是否使用加密處理？	<input type="checkbox"/> 是 <input type="checkbox"/> 否

保護持卡人資料

要求 5：使用及經常更新防毒軟體

問題	回答
5.1 所有的伺服器及所有的工作站上是否均安裝病毒掃描軟體，以及病毒掃描軟體是否經常更新？	<input type="checkbox"/> 是 <input type="checkbox"/> 否

要求 6：開發及維護安全的系統和應用程式

問題	回答
6.1 開發系統、測試系統，以及生產系統是否用供應商發行的最新安全相關修補程式更新？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
6.2 軟體及應用程式開發程序是否根據業界的最佳實務作法，以及軟體開發生命週期（SDLC）程序是否全程將資訊安全納入？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資
6.3 如果用生產資料進行測試及開發，則是否在使用之前先將敏感的持卡人資料消毒？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資
6.4 生產環境及應用程式的所有改變是否均經過正式授權、規劃，並於執行之前先登錄？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
6.5 在研發網路應用程式時，是否有將安全實務界所共同接受之綱領（例如開放網路應用程式安全計劃（Open Web Application Security Project）群組（ www.owasp.org ））納入考量？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資
6.6 在網際網路上進行驗證時，是否將應用程式設計成可防止惡意使用者判斷出使用中的使用者帳號？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資
6.7 敏感的持卡人資料是否儲存在安全或加密的紀錄（cookies）內？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資
6.8 伺服器端實施的管制措施是否能防止SQL Injection，以及其他繞行通過客戶端輸入管制措施的行爲？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資

實施堅實的存取控管措施

要求 7：限制僅在業務相關之前提下，始得存取資料

問題	回答
7.1 支付卡帳號是否限制於必須知道的使用者始能進行存取？	<input type="checkbox"/> 是 <input type="checkbox"/> 否

要求 8：進行電腦存取的每一個人都賦予一個獨一無二的 ID

問題	回答
8.1 是否要求所有的使用者最起碼均必須以獨一無二的使用者名稱及密碼加以驗證？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.2 如果員工、管理者，或是第三人從遠端對網路進行存取，則遠端存取軟體（諸如PCAnywhere、撥入dial-in或VPN）是否配置獨一無二的使用者名稱及密碼，並啟用加密及其他的安全功能？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資
8.3 網路裝置及系統上的所有密碼是否均加密？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.4 員工離開公司時，員工的使用者帳號及密碼是否立即廢止？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.5 是否經常查察所有的使用者帳號，以確保惡意、過時或未知之帳號均不存在？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.6 長期未使用的非消費者帳號（閒置的帳號）是否經過一段預定的期間後，即自動的在系統中失效？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.7 是否只有在必要的時間內，才啟用供應商進行遠端維護所使用的帳號？	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 無資
8.8 非消費者之使用者是否禁止使用群組、共用或常用易猜的帳號密碼？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.9 是否要求非消費者之使用者定期變更其密碼？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.10 非消費者之使用者是否有適用的密碼政策，以規定採用加強型密碼，防止使用先前曾經使用過的密碼？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
8.11 是否有帳號停用機制，以阻隔惡意的使用者以多次輸入密碼的方式，或使用卑鄙的手段得以進行存取？	<input type="checkbox"/> 是 <input type="checkbox"/> 否

實施堅實的存取控管措施

要求 9：限制對持卡人資料進行實體存取

	問題	回答		
9.1	是否有實施多重的實體安全管制措施（諸如識別證、陪同或陷阱），以防止未經授權者擅入場所之內？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.2	如果使用無線技術，則是否限制對無線網路基地台、無線網路閘道，以及無線手持式裝置進行存取？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 無資
9.3	（伺服器、工作站、筆記型電腦及硬碟等）內含持卡人資料的設備及媒體是否有實體保護，以防止未經授權的存取？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.4	列印於紙張上或經傳真接收的所有持卡人資料是否均加以保護，以防止未經授權的存取？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.5	是否實施程序，以安全可靠的發送及處置內含敏感持卡人資料之備份媒體及其他媒體？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.6	儲存持卡人資料的所有媒體裝置是否均正確的紀錄並安全可靠的存放？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.7	在進行實質處置之前，是否先將持卡人資料刪除或毀壞（例如將紙本文件絞碎或將備份媒體消磁）？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	

經常監督及測試網路

要求 10：追蹤及監控對網路資源及持卡人資料所進行的所有存取

	問題	回答	
10.1	對持卡人資料所進行之所有存取，其中包括超級使用者（root）/管理者之存取在內，是否均有登錄？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.2	存取控管日誌是否內含成功及不成功的登入動作，以及對事件登錄日誌所做的存取動作？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.3	所有重要的系統時鐘及時間是否均已同步，事件日誌是否內含日期及時間紀錄？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.4	是否經常審核防火牆、路由器、無線網路基地台，以及驗證伺服器事件日誌，以查察未經授權的網路連線？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.5	所有重要系統的事件登錄日誌是否經常備份，並安全的至少在線上保存三個月，離線保存一年？	<input type="checkbox"/> 是	<input type="checkbox"/> 否

要求 11：經常測試安全系統及程序

	問題	回答		
11.1	如果使用無線技術，是否定期操作無線分析器，以找出所有的無線裝置？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 無資
11.2	連接網際網路的所有應用程式及系統是否在投入生產之前先執行漏洞掃描或侵入測試？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
11.3	網路上是否有使用入侵偵測系統或入侵預防系統？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
11.4	是否持續不斷的監控入侵偵測系統或入侵預防系統（IDS/IPS）發出的警告，以及是否安裝最新的IDS/IPS簽署（signitures）？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	

要求 12：訂定及實施一套資訊安全政策

問題	回答
12.1 資訊安全政策，包含存取控管、應用程式及系統開發、操作、網路，以及實體安全在內，是否均正式以文件紀錄？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.2 資訊安全政策及其他相關的安全資料是否均有宣導，讓所有的系統使用者週知（其中包括廠商、合約工及業務夥伴在內）？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.3 資訊安全政策是否每年至少審核一次，並於必要時加以更新？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.4 公司內部是否明確訂定資訊安全的分工及職責？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.5 是否有對所有的系統使用者實施與時俱進的資訊安全認知及訓練計畫？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.6 是否要求員工簽署一份合約，以證明他們已經閱讀並瞭解安全政策和程序？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.7 是否有對能存取帳號的所有員工進行背景調查（諸如在當地法律規定的限度內，進行信用紀錄及犯罪紀錄查核）？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.8 能存取敏感持卡人資料的所有第三人，是否均依合約規定必須遵守信用卡協會的安全標準？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.9 安全事件回應計劃是否有正式紀錄，並對相關的負責人進行宣導週知？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.10 安全事件是否有呈報給負責安全調查的人？	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.11 事件回應團隊是否已妥為準備，可在持卡人資料遭到危害時加以部署？	<input type="checkbox"/> 是 <input type="checkbox"/> 否

詞彙

名詞	定義
存取控管	限制僅獲得授權者或應用程式始能存取資訊或資訊處理資源之措施。
帳號蒐集	利用駭客程式，去收集有效的使用者帳號的方法，在錯誤訊息中提供太多資料將會揭露資訊，駭客將會更容易侵入或危害系統。
帳號	用以辨識發卡行及特定的持卡人帳號的支付卡號碼（借方或貸方）。
信用卡協會會員	和接受Visa或MasterCard卡之特約商店建立及維持關係的信用卡協會會員關係。
資產	企業的資訊或資訊處理資源。
事件登錄日誌	依時間順序所做的系統活動紀錄，足供重建、審核，以及檢驗與交易作業、程序或事件相關，或引導進行作業之環境及活動之自始至終的作業順序，有時特別是指安全稽核軌跡紀錄。
驗證	驗證一個物品或程序的程序。
授權	准許存取，或對使用者、程式或程序核准其他的權利
備份	為存檔目的或為保護防止損壞或損失而將資料複製。
卡片確認碼	支付卡簽名欄側列印的三碼數值，用以驗證未提示卡片的交易，如果是MasterCard支付卡，稱之為CVC2；如果是Visa支付卡，則稱之為CVV2。
持卡人	獲得核發卡片的顧客，或是被授權使用卡片的人。
持卡人資料	有關持卡人的所有個人識別資料以及與會員的關係（亦即帳號、到期日、會員提供的資料、特約商店/代理商收集的其他電子資料等等），本名詞也指有關持卡人其他詳細的個人資料（亦即地址、電話號碼等等）。
危害	侵入電腦系統，因而可能未經授權而揭露、修改或破壞持卡人資料。
本機	可用以存取及控制網路連結環境中之伺服器 / 大型主機的螢幕及鍵盤。
消費者	購買商品及/或服務的人。
記錄 Cookies	為維持作業的進行，在網路伺服器及網路瀏覽器之間交換的資料。Cookies可能內含使用者的偏好及個人資料。
資料庫	具有結構的格式，用以編排及保存資料，以便能輕易擷取，表格或試算表即是簡單的資料庫例證。
DBA	營業現況（Doing Business As）。遵循之確認等級係按照DBA或連鎖商店（非擁有數家連鎖店的公司）之交易量而定。

詞彙

名詞	定義
內建帳號	製造出廠之系統所預設的系統登入帳號，以便於首次使用系統時進行初次的存取。
出廠預設密碼	系統自製造廠商出廠時，系統管理及服務帳號的密碼，通常和出廠預設帳號相關。出廠預設帳號及密碼會被公布且眾所週知。
雙重管制	保留程序完整性的一種方法，其方式是由數人個別採取一些動作，某些交易才能完成。
DMZ（非軍事區，隔離區）	在私有網路及公共網路之間增加的網路，用以增加一道安全層。
出口	離開網路的連線。
加密	將資料轉換成除特殊加密金鑰持有人之外，任何人都難以理解之形式的程序。使用加密方式，在加密程序和解密程序（加密的逆向程序）之間保護資料，以防止未經授權而揭露。
防火牆	保護網路資源，阻隔其他網路之使用者的硬體及/或軟體。通常，一家企業的企業內部網路能讓其員工存取更為廣博的網際網路，即必須具備有防火牆，以防止從外面存取該企業自己的私有資料資源。
主機	軟體常駐的主要硬體。
資訊安全	保護資訊的機密性、完整性，以及可資利用性。
入口	進入網路的連線。
入侵偵測系統	入侵偵測系統（IDS）會檢查所有向內及向外的網路活動，並找出可能表示網路或系統遭到企圖闖入或危害系統者攻擊的可疑態樣。
IP位址	IP位址是一個數字碼，能獨一無二的辨識網際網路上的一台特定電腦。
IP位址欺偽（Spoofing）	一種用來無權存取電腦的技術，入侵者發送訊息給電腦，其所利用之IP位址表明該訊息係來自於可信任的主機。
ISO 8583	金融系統之間進行通訊的一套既定標準。
金鑰	在加密技術中，金鑰是未加密文本使用演算法製作成加密文本所應用的一個數值。金鑰的長度通常即決定將特定訊息之文本解密的困難度。
磁條資料（磁軌資料）	磁條內經過編碼的資料，用以在提示卡片之交易過程中進行授權。公司行號不得於交易授權之後留存全部的磁條資料，特別是在授權之後，服務碼、任意的資料/CVV，以及Visa保留值必須加以清除；不過帳號、到期日，以及姓名則得擷取及留存。
監控	審查網路上的活動。

詞彙

名詞	定義
網路	網路是指二台或多台電腦相互連結在一起，俾使這些電腦能共享資源。
網路位址轉譯(Network Address Translation, NAT)	將某一網路內所用的網際網路通訊協定位址 (IP位址)，轉譯成其他網路中已知的其他IP位址。
非消費者之使用者	除消費客戶外，任何對系統進行存取之使用者，其中包括但不限於員工、管理者，以及第三人。
密碼	當作使用者驗證裝置的一串字元。
修補程式	對一段程式進行快速修理工作。在軟體產品試用版的發行過程中或是試用期間內，以及在產品正式發行以後，總是會發現一些問題，修補程式即是提供給使用者的立即解決方案。
侵入	成功繞過系統安全機制的行爲。
侵入測試	偵測電腦系統或網路之安全的做法，用以找出攻擊者會利用的安全弱點。測試的做法是試圖侵入系統，以便測試者能找出漏洞，並提出改善安全的建議步驟。
系統週邊設備掃描	一種非侵入式測試，其方式是偵測對外的系統，並就對外網路所提供的服務提出報告 (亦即網際網路上所能提供的服務)。
政策	企業層級的規定，內容是有關可接受之計算資源使用方式、安全措施，以及發展作業程式的指導綱領。
程序	實踐適用政策內容的一套程序，是實踐政策的「做法」，告訴整個企業組織執行政策的程序。
通訊協定	一種在網路內使用，經過合意的通訊方法。產品在網路上執行活動應遵守之規則及程序的一套規範。
風險分析	又稱為風險評估，一套用系統化的方式辨識珍貴的系統資源，以及對這些資源的威脅，根據預估的發生頻率和成本，將損失暴露 (亦即可能的損失) 量化的程序，並會 (選擇性的) 建議應如何分配資源進行反制，俾以降低整體的暴露。
路由器	路由器是一件將二個以上的網路連結在一起的硬體或軟體。路由器的功能是分類器及解譯器，會注意位址，將資料傳送到正確的目的地。軟體路由器有時稱為閘道。
清除處理 (Sanitization)	從檔案、裝置或系統上刪除敏感的資料；或是修改資料，使得資料無攻擊之用處。
安全職員	負責企業之安全相關事務主要責任的人。
安全政策	一組法律、規則，以及實務作法，用以規範企業掌管、保護，以及發送敏感資料的作業。

詞彙

名詞	定義
敏感的持卡人資料	如果未經授權而被揭露，即可能會被用作詐騙交易的資料，其中包含帳號、磁條資料、CVC2/CVV2，以及到期日。
責任分工	將系統功能分成幾個步驟，分給數人執行的一種作法，以防止程序被人破壞。
伺服器	為其他電腦提供處理通訊、檔案儲存，或列印功能等服務的電腦。
SQL Injecion	一種對資料庫網站進行的攻擊型態，攻擊者會利用和網際網路連接之系統上不安全的編碼，執行未經授權的SQL指令。 SQL injection 攻擊係用來竊取資料庫的資料，通常該資料都不能取得，及/或不能透過載有該資料庫的電腦存取企業的主機電腦。
SSL	一套既定的業界標準，用以將網路瀏覽器和網路伺服器之間的通道加密，以確保在該通道上傳送之資料的隱密性和可信賴性。
防止擅入 (Tamper-resistance)	如果一套系統難以修改或破壞，即使是攻擊者對該系統進行實體存取亦然，則該系統即稱之為防止擅入。
威脅	可能導致資訊或資訊處理資源因故意或過失而喪失、修改、暴露、可被存取，或以其他方式影響企業損傷的一種狀況。
Token裝置	執行動態驗證的裝置。
交易資料	和電子支付相關的資料。
切截功能	移除資料片段的一種作法，通常，將帳號切截的時候，會將前十二碼刪除，只留下最後四碼。
二段式驗證	使用者必須製作二份憑據的驗證方法 – 有些是他們所擁有的（例如智慧卡或硬體token裝置），有些則是他們所知道的（例如密碼）。如要對系統進行存取，使用者必須製作二個係數。
使用者識別碼UserID	一段字元串，用以獨一無二的辨識系統的每一位使用者。
病毒	會自我複製，以及會修改或破壞軟體或資料的程式或一串編碼。
安全弱點	系統安全程序、系統設計、運作或內部控管上會被利用的漏洞，因而違反系統安全政策。
掃描安全弱點	一種自動化的工具，會檢查特約商店或服務提供廠商之系統的漏洞，本工具能根據對外的網際網路通訊協定（IP）位址，從遠端查察網路及網路應用程式。掃描作業能找出作業系統、服務及裝置中可能被駭客用以瞄準公司私有網路的安全弱點。