



PCI資料安全標準

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）資料安全標準訂定了保護客戶及交易資料的具體作法，但是Visa Asia Pacific並不擔保，亦未聲稱實施這些標準即可避免安全危害或損失，另外並聲明，不論是否已完全實施支付卡產業資料安全標準，其所致之任何安全危害及損失，本公司一概不負任何責任。

重要

支付卡產業（PCI）資料安全標準是Visa Asia Pacific整套客戶資料安全（AIS）文件的一部分，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計劃詳情，歡迎上網<http://www.visa-asia.com/secured>查閱。

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

要求 2：不可使用供應商提供的出廠設定值作為系統密碼及其他的安全參數

保護持卡人資料

要求 3：保護儲存的資料

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

訂定及實施一套漏洞管理計劃

要求 5：使用防毒軟體並應經常更新

要求 6：研發及維持安全的系統和應用程式

實施堅實的存取控管措施

要求 7：限制僅營業必須知道之前提下始得存取資料

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

要求 9：限制對持卡人資料進行實體存取

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

要求 11：經常測試安全系統及程序。

訂定及實施一套資訊安全政策

要求 12：訂定及實施一套資訊安全政策

請注意，這些支付卡產業 (PCI) 資料安全要求適用於儲存、處理，或傳送持卡人資料的所有會員、特約商店，以及服務提供廠商。此外，這些安全要求適用於所有的「系統元件」，系統元件是指持卡人資料環境內含或相連之所有網路元件、伺服器，或應用軟體。網路元件包括但不限於防火牆、交換機、路由器、無線存取點、網路裝置，以及其他的安全裝置。伺服器包括但不限於網路、資料庫、驗證、DNS、郵件、代理伺服器，以及 NTP。應用程式包括所有外購及訂製的應用程式，其中包括內部及外部（網路）應用程式在內。

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。

防火牆是電腦裝置，用以控管允許從外面進入公司網路的電腦交通，以及進入公司內部網路內較敏感區域之交通。所有的系統都必須加以保護，以防止未經授權而從網際網路進行存取，不論是因為電子商務、員工利用桌上電腦瀏覽器從事網際網路存取，或是員工的電子郵件存取。通常，看起來無關緊要的進出網際網路路徑，往往都會變成進入重要系統而未加保護的路徑。防火牆是任何電腦網路的重要保護機制。

1.1 訂定防火牆配置標準，其中包含：

- 1.1.1 一套正式的程序，用以核准及測試所有的外部網路連結，以及防火牆配置的變更
- 1.1.2 目前的網路圖，附記和持卡人資料的所有連結，其中包括所有的無線網路在內
- 1.1.3 各網際網路連結，以及任何DMZ（隔離區）及企業內部網路之間，均要求設置防火牆
- 1.1.4 有關網路元件邏輯管理之分組、角色，以及職責的敘述
- 1.1.5 紀錄營業所需之服務/ports清單
- 1.1.6 除HTTP及SSL、SSH，以及VPN之外，如有任何可資利用的協定，均應加以驗證及紀錄
- 1.1.7 任何被允許的有風險協定（FTP等）均應加以驗證及紀錄，其中應包含使用該協定的理由，以及實施的安全措施
- 1.1.8 定期審核有關防火牆/路由器之全部規定
- 1.1.9 路由器的配置標準

1.2 建置一套防火牆配置，能拒絕來自於「不可靠」網路/主機的所有交通，下列除外：

- 1.2.1 網路協定 - HTTP (port 80)，以及安全插座層 (Secure Sockets Layer, SSL) (通常是port 443)
- 1.2.2 系統管理協定 (例如安全介殼程式 (Secure Shell, SSH) 或虛擬私有網路 (Virtual Private Network, VPN))
- 1.2.3 營業所需的其他協定 (例如因ISO 8583而需要)。

1.3 建置一套防火牆配置，能限制公眾可存取之伺服器及儲存持卡人資料之任何系統元件之間的連結，其中包括來自於無線網路的任何連結在內。本套防火牆配置應包含：

- 1.3.1 限制向內之網際網路交通不能到達DMZ內之IP位址 (入口過濾器)
- 1.3.2 限制向內及向外之網際網路交通不能到達ports 80及443
- 1.3.3 不允許內部位址通過網際網路進入DMZ (出口過濾器)

- 1.3.4 狀況檢查，又稱為動態封包過濾（dynamic packet filtering）（僅允許「既定的」連結進入網路）
- 1.3.5 將資料庫置於內部網路區內，安全防護DMZ
- 1.3.6 將向外之交通限制為支付卡環境所必須
- 1.3.7 安全及同步的路由器配置檔案（例如操作配置檔案 –用於路由器正常操作時，以及開機配置檔案 – 用於機器重新開機時，均應有相同牢靠的配置）。
- 1.3.8 所有其他未經特別允許之進出交通均拒絕之

- 1.3.9 在任何無線網路及支付卡環境之間安裝週邊防火牆，這些防火牆應配置成能拒絕，或（如各該交通係營業目的所必須者，則）控管來自於無線環境的任何交通
- 1.3.10 任何行動式及/或員工自有電腦，其和網際網路直接連結，用以存取公司網路者（例如員工使用的筆記型電腦），均應安裝個人防火牆軟體
- 1.4 外部網路及任何儲存持卡人資料之系統元件（例如資料庫）之間，均應禁止直接公眾存取
 - 1.4.1 採行DMZ過濾及篩選所有的交通，以禁止進出之網際網路交通使用直接途徑
 - 1.4.2 限制支付卡應用程式向外之交通進入DMZ內之IP位址。
- 1.5 實施網際網路協定（IP）偽裝，以防止內部位址被轉譯，並在網際網路上被透露。採用實施RFC 1918位址空間的技術，諸如Port Address Translation（PAT）或Network Address Translation（NAT）

要求 2：不可使用供應商提供的出廠設定值作為系統密碼及其他的安全參數。

（公司內部或外部的）駭客通常會使用供應商出廠設定密碼及其他供應商出廠設定以危害系統。這些密碼和設定都是駭客社群所熟知的，並能輕易藉助公開資訊判斷之。

- 2.1 務必在將系統安裝在網路上之前，先變更供應商提供的出廠設定值（例如密碼、SNMP共用字串，以及刪除不需要的帳戶）。
 - 2.1.1 如果是無線環境，應變更無線設備供應商之出廠設定，其中包括但不限於WEP金鑰、內建SSID、密碼，以及SNMP共用字串，並解除SSID之廣播功能。如有WPA功能，應啓動Wi-Fi保護存取（WPA）技術進行加密及驗證。
- 2.2 訂定所有系統元件的配置標準，確保這些標準能處理所有已知的安全漏洞，而且是業界最佳的實務作業。
 - 2.2.1 每一部伺服器（例如網路伺服器、資料庫伺服器，DNS應在另外的伺服器上執行）僅執行一項主要的功能
 - 2.2.2 終止所有不必要及不安全的服務和協定（執行該裝置之指定功能時，非直接需要的服務和協定）。
 - 2.2.3 配置系統安全參數，以免誤用
 - 2.2.4 移除所有非必要的功能，諸如文稿、驅動程式、配備功能、子系統、檔案系統（例如非必要的網路伺服器）。

2.3 將所有的非控制台管理存取加密。利用諸如SSH、VPN或SSL/TLS等技術進行網路管理，以及其他的非控制台管理存取。

保護持卡人資料

要求 3：保護儲存的資料

加密是終極的保護機制，因為即使有人能突破所有其他的保護機制，並能接近加密的資料，如果不能進一步的破解加密功能，仍然無法閱讀資料。這是深度防衛原則的一種說明。

3.1 儘可能儲存最少的持卡人資料。訂定一套資料留存及處置政策。依資料留存政策中之規定，按照營業、法律，及/或管制目的之需要，限制儲存數量及留存時間。

3.2 不可儲存授權後的敏感驗證資料（即使經過加密亦然）：

3.2.1 不可儲存（卡片背面、晶片內等之）磁條上任何磁軌的全部內容

3.2.2 不可儲存卡片確認碼（支付卡正面或背面列印的三位或四位數值（例如CVV2及CVC2資料））

3.2.3 不可儲存PIN驗證值（PVV）

3.3 提示時，應掩蓋帳號（提示時，最多僅能顯示前六碼或後四碼）。

請注意，本規定並不適用於有特別需求，必須看到信用卡全部號碼的員工及其他人。

3.4 不論將敏感的持卡人資料儲存於何處，都必須用下列的任何方法使其無法閱讀（其中包括儲存於可攜式媒體、備分媒體上、紀錄表內之資料，以及從無線網路接收，或以無線網路儲存之資料）：

◦ 單向雜湊（雜湊索引），例如SHA-1

◦ 串截

◦ 索引token裝置及PADs，PADs並應安全的儲存

◦ 強力加密，諸如Triple-DES 128-位元，或AES 256-位元，並應具備相關的金鑰管理步驟和程序。

最起碼必須無法被閱讀的客戶資料是支付卡帳號。

3.5 保護加密金鑰，以防止被揭露及誤用。

3.5.1 將金鑰之取用限制於必須的最少數量監管人

- 3.5.2 儘可能將金鑰安全的儲存在最少的地方及形式。
- 3.6 將所有的金鑰管理步驟和程序全部明文紀錄並實施之，其中包括：
 - 3.6.1 強力金鑰之產生
 - 3.6.2 穩當的分發金鑰
 - 3.6.3 安全的儲存金鑰
 - 3.6.4 定期的變更金鑰
 - 3.6.5 銷毀舊的金鑰
 - 3.6.6 分散知識及雙重控管金鑰（每一個人都只知道自己負責部份的金鑰，因此需要二或三人才能重建全部的金鑰）。
 - 3.6.7 防止未經授權的更換金鑰
 - 3.6.8 將已知或懷疑已被危害的金鑰換掉
 - 3.6.9 廢止舊的或失效的金鑰（主要是RSA金鑰）
 - 3.6.10 要求金鑰監管人簽署一張表格，明示監管人已經瞭解，並接受他們身為金鑰監管人的職責

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。

敏感資料透過網際網路傳送時必須要加密，因為在傳送的過程中，常見駭客可輕易的攔截及/或轉換資料。

- 4.1 使用強力的加密技術及加密處理技術（至少128位元），諸如安全插座層（Secure Sockets Layer，SSL）、點對點通道協定（Point-to-Point Tunneling Protocol，PPTP）、網際網路安全性協定（Internet Protocol Security，IPSEC），俾於透過公共網路傳送時，安全防護敏感的持卡人資料
 - 4.1.1 如果是無線網路傳送持卡人資料，具備WPA功能時，應使用Wi-Fi保護存取（WPA）技術，或使用VPN或128-位元的SSL加密傳送。禁止完全仰賴WEP保護機密性，以及存取無線LAN，應使用上述的一種方法，結合128位元的WEP，並應每季調換一次共用的WEP金鑰，並於人事有更迭時調換之。
- 4.2 禁止透過未經加密之電子郵件發送持卡人資料。

訂定及實施一套漏洞管理計劃

要求 5：使用防毒軟體或程式並應經常更新。

許多漏洞及惡意病毒會透過員工的收發電子郵件動作進入網路，所有的電子郵件系統及桌上型電腦都必須使用防毒軟體，以保護系統不受惡意軟體之傷害。

- 5.1** 常會被病毒感染的系統（例如個人電腦及伺服器）均應部署防毒機制。
- 5.2** 確保所有的防毒機制都是最新型、能有效操作，並能產生稽核紀錄表。

要求 6：研發及維持安全的系統和應用程式

無道德之人會利用安全漏洞取得存取系統之特權，這些漏洞中有許多是利用供應商的安全修補程式修復，所有的系統均應有最新的軟體修補程式，以保護防止被員工、外部駭客，以及病毒的不當利用。公司內部研發的應用程式，如果使用標準的系統研發程序及穩當的編碼技術，即可避免眾多的漏洞。

- 6.1** 確保所有的系統元件及軟體均有供應商提供的最新版安全修補程式。
 - 6.1.1** 在發行一個月之內安裝相關的安全修補程式。
- 6.2** 訂定一套程序，用以找出新發現的安全漏洞（例如訂購網際網路上免費的警告服務）。將標準更新，以處理新的漏洞問題。
- 6.3** 根據業界最佳的實務作業研發軟體應用程式，並於軟體研發生命週期中全程均將資訊安全納入。將下列各項納入：

- 6.3.1** 研發之前，先測試所有的安全修補程式，以及系統及軟體的配置變更
 - 6.3.2** 研發/測試及生產環境應分開
 - 6.3.3** 研發/測試及生產環境之間的職責應分開
 - 6.3.4** 不得使用生產資料（真實的信用卡號）進行測試或研發
 - 6.3.5** 生產系統開始運作之前，應先移除測試資料及帳戶
 - 6.3.6** 應用程式開始運作或發行給顧客之前，應先移除訂製應用程式帳戶、使用者名稱，以及密碼。
 - 6.3.7** 發行進行生產或發行給顧客之前，應先查閱訂製碼，以找出是否有任何潛在的編碼漏洞
- 6.4** 遵循系統及軟體配置變更應適用之所有變更控管程序，程序中應納入：
- 6.4.1** 影響紀錄
 - 6.4.2** 適當層級管理階層之簽署放行
 - 6.4.3** 驗證操作功能之測試
 - 6.4.4** 備援程序。
- 6.5** 按照開放網路應用程式安全計畫（Open Web Application Security Project）綱要等明文安全綱要研發網路軟體及應用程式，查閱訂製應用程式碼，找出編碼漏洞。請查閱 www.owasp.org - 「十大最重要的網路應用程式安全漏洞」。在軟體研發程序中應避免常見的編碼漏洞，應納入：
- 6.5.1** 無效的輸入
 - 6.5.2** 破壞存取控管（例如惡意使用使用者ID）
 - 6.5.3** 破壞驗證/作業管理（使用帳戶憑據及作業cookies）
 - 6.5.4** 橫區編寫（XSS）攻擊
 - 6.5.5** 緩衝區溢滿
 - 6.5.6** 注射裂縫（例如SQL注射）
 - 6.5.7** 不正確的錯誤處理方式
 - 6.5.8** 不安全的儲存
 - 6.5.9** 拒絕服務
 - 6.5.10** 不安全的配置管理。

實施堅實的存取控管措施

要求 7：限制僅營業必須知道之前提下始得存取資料。

如此可確保重要資料僅能在經過授權時才能被存取。

7.1 限制僅有工作上有需要者才能存取計算資源及持卡人資料。

7.2 有多位使用者之系統應建立一套機制，以使用者是否需要知道為存取限制前提，並應設定成除非經過特別允許，否則「全部拒絕」。

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。

如此可確保對重要資料及系統所採取之措施，均係由已知及經過授權之使用者負責執行，並能加以追蹤。

8.1 所有的使用者均能用獨一無二的使用者名稱加以辨識，然後才允許他們存取系統元件或持卡人資料。

8.2 除了獨一無二辨識法之外，至少運用下列的一種方法，對所有的使用者進行驗證：

- 密碼

- Token裝置（例如SecureID、憑證或公開金鑰）
- 生物測定。

8.3 對員工、管理者及第三人從遠端存取網路實施二段式驗證，使用諸如RADIUS或採用token裝置之TACACS，或是採用個別憑證之VPN。

8.4 在所有系統元件上在進行傳送或儲存時，應將所有密碼加密。

8.5 在所有的系統元件上，對非消費者之使用者及管理者確實正確進行使用者驗證及密碼管理：

8.5.1 對使用者ID、憑據，以及其他的物件識別碼之增刪修改進行控管。

8.5.2 在執行密碼重設之前，先驗證使用者身份。

8.5.3 每一位使用者均設定一個唯一數值的初次密碼，並於第一次使用之後立即變更

8.5.4 被終止之使用者，應立即廢止存取。

8.5.5 至少應每隔九十天移除一次無動作的使用者帳戶

8.5.6 只有在必要的時間內，才啓用供應商所使用的帳戶，以便進行遠端維護

8.5.7 將密碼程序及政策分發給能存取持卡人資料的所有使用者

8.5.8 不可使用群組、共用或一般的帳戶/密碼

8.5.9 至少應每隔九十天變更一次使用者密碼

8.5.10 要求密碼長度至少應有七個字元

8.5.11 使用含有文數字的密碼

8.5.12 不可允許任何人使用與其曾使用之任何密碼後四碼完全相同的新密碼

8.5.13 限制重複存取動作，方法是在六次動作以內即鎖住使用者ID

8.5.14 設定鎖住時間為三十分鐘，或直到管理者恢復使用者ID之作用爲止

8.5.15 如果動作過程閒置超過十五分鐘，應要求使用者重新輸入密碼，才能重新啓動終端機

8.5.16 存取任何內含持卡人資料之資料庫，均應進行驗證，其中包括應用程式、管理者，以及其他所有使用者之存取在內。

要求 9：限制對持卡人資料進行實體存取

對內含持卡人資料之資料或系統進行任何實體存取，即有機會能存取裝置或資料，並能移除系統或硬拷貝，應加以適當的限制。

9.1 採行適當的場所進入管制措施，以限制並監控對儲存、處理，或傳送持卡人資料之系統進行實體存取。

9.1.1 使用攝影機監控敏感的区域，稽查攝影資料及相關入口關聯資料，並至少儲存三個月，除非法律另有其他限制規定。

9.1.2 限制對公眾得存取之網路接頭進行實體存取。

- 9.1.3** 限制對無線存取點、閘道，以及手持式裝置進行實體存取。
- 9.2** 訂定能幫助所有人員均可輕易分辨員工及訪客的程序，特別是在能存取持卡人資料的地方。
「員工」是指全職及兼職員工、臨時員工/人員，以及「常駐」在公司現場的顧問。「訪客」是指供應商、員工的客人、維修人員，或需要短期進入設施的任何人，其時間通常不超過一天。
- 9.3** 確保所有的訪客均：
- 9.3.1** 經過授權才能進入處理或保存持卡人資料的地方
 - 9.3.2** 提供有使用期限的實體卡片（例如證章或出入證），用以辨識為非員工
 - 9.3.3** 要求在離開場所之前，或是在到期時繳回實體卡片。
- 9.4** 使用訪客紀錄表留下訪客活動的實體稽查追蹤紀錄，本紀錄表至少應保存三個月，除非法律另有其他限制規定。
- 9.5** 將備份媒體儲存在一個離開現場的安全場所中，該場所得為第三人之場所，或是一個商業儲存場所。
- 9.6** 實體安全防護內含持卡人資料的所有書面及電子媒體（例如電腦、電子媒體、網路連結及通訊硬體、電信線路、紙張收據、紙張報告，以及傳真）。
- 9.7** 對內或對外發送內含持卡人資料之任何類型媒體時，均應保持嚴格之管制
- 9.7.1** 在媒體上貼標籤，以便能看出是機密資料。
 - 9.7.2** 利用穩當的快遞業者，或是能精確追蹤的傳輸機制傳送媒體。
- 9.8** 確保所有媒體從安全地區移出時，均經過管理階層之核准（特別是將媒體交到個人手上時）。
- 9.9** 對於儲存及取得內含持卡人資料的媒體應保持嚴格之管制：
- 9.9.1** 正確的編製所有媒體的紀錄，並確定媒體均安全的存放。
- 9.10** 基於營業或法定之理由不再需要內含持卡人資料之媒體時，應加以銷毀：
- 9.10.1** 橫切絞碎、焚化，或絞爛硬拷貝材料
 - 9.10.2** 清除、去磁、絞碎，或是以其他方式銷毀電子媒體，俾使持卡人資料無法被重建。

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。

具備登入機制及追蹤使用者活動的能力十分的重要。所有的環境均具備紀錄表，即可在出錯時徹底加以追蹤及分析；如果沒有系統活動紀錄表，要判斷被危害的原因將會非常的困難。

- 10.1** 訂定一套程序，將對於系統元件所進行的所有存取（特別是特權使用者等有管理特權者所進行之存取動作）和特定個人連結在一起。

- 10.2** 對所有系統元件實施自動稽查追蹤，以重建下列的事件資料：
 - 10.2.1** 對持卡人資料進行存取之所有個別使用者
 - 10.2.2** 特權使用者或有管理特權者所採取之所有行動
 - 10.2.3** 對所有稽核追蹤資料所進行之存取
 - 10.2.4** 無效的邏輯存取動作
 - 10.2.5** 使用鑑別及驗證機制
 - 10.2.6** 將稽查紀錄表初始化
 - 10.2.7** 建立或刪除系統層級的物件。
- 10.3** 對於所有系統元件，至少應紀錄下列有關各事件之稽核追蹤內容：
 - 10.3.1** 使用者身分
 - 10.3.2** 事件的類型
 - 10.3.3** 日期及時間
 - 10.3.4** 成功或失敗的跡象
 - 10.3.5** 事件的緣起
 - 10.3.6** 受影響之資料、系統元件或資源的身分或名稱。
- 10.4** 讓所有重要的系統時鐘和時間同步。
- 10.5** 安全防護稽核追蹤資料，以免被修改，其中包括下列各項：
 - 10.5.1** 限制有相關工作上需求者始能查閱稽核追蹤資料
 - 10.5.2** 保護稽核追蹤資料檔案，防止未經授權而竄改
 - 10.5.3** 即時將稽核追蹤資料檔案備份到難以更改之中央紀錄表伺服器或媒體
 - 10.5.4** 將無線網路的紀錄表拷貝到內部LAN上的紀錄表伺服器內。
 - 10.5.5** 在紀錄表上使用檔案完整性監控/變更偵測軟體（例如Tripwire），以確保現有的紀錄表資料非經產生警告不會被變更（不過新增資料不應產生警告）。
- 10.6** 至少應每天查閱一次所有系統元件的紀錄表，查閱之紀錄表應包括IDS及驗證（AAA）伺服器（例如RADIUS）等執行安全功能的伺服器。
- 10.7** 稽核追蹤資料紀錄應保留一段能有效運用，以及法令所規定的期間。
稽核紀錄通常涵蓋最少一年的期間，至少應有三個月可供線上利用。

要求 11：經常測試安全系統及程序

駭客/研究人員會一直去發現漏洞，新軟體也會引進漏洞。系統、程序，以及訂製軟體均應經常加以測試，以確保長期及經過變更亦均能保持安全。

- 11.1** 經常測試安全控管裝置、限制、網路連結，以及禁止規定，以確保各該裝置功能能適當的找出或阻止任何未經授權的存取企圖。如果採用無線技術，應定期使用無線分析器找出使用中的所有無線器材。

11.2 至少每季應進行一次內部及外部網路漏洞搜尋，網路內部進行任何重大改變（例如安裝新的系統元件、網路拓撲學變更、防火牆規則修改、產品升級）之後亦同。

請注意，外部漏洞搜尋必須由符合支付卡產業規定資格之搜尋廠商負責執行。

11.3 至少一年應對網路基礎建設及應用程式執行一次侵入測試，並應於基礎建設或應用程式有任何重大升級或修改（例如作業系統升級、環境中添加子網路、環境中添加網路伺服器）後執行測試。

11.4 使用網路入侵偵測系統、建置於主機的入侵偵測系統，及/或入侵預防系統，以監控所有的網路交通，並對可疑的危害情況提出警告。所有的入侵偵測及預防系統均應保持常新。

11.5 部署檔案完整性監控功能，俾於重要系統或內容檔案未經授權而被修改時提出警告，並至少應每天執行一次重要的檔案比對（如果程式可自動進行，則應更頻繁的比對）。

重要檔案並不必然就是內含持卡人資料的檔案。基於檔案完整性監控的目的，重要檔案通常是不會經常改變的檔案，但是如果這些檔案被修改，即表示系統被危害或有被危害之虞。檔案完整性監控產品通常都會預先配置相關作業系統的重要檔案，其他的重要檔案，諸如訂製應用程式檔案，均必須由特約商店或服務提供廠商加以評估及界定。

要求 12：訂定及實施一套員工及合約商適用的資訊安全政策。

一套堅強的安全政策能為整個公司訂定安全基調，並讓員工知道自己該怎麼做。所有員工均應瞭解資料的敏感性，及其保護資料的責任。

12.1 訂定、公佈、實施，以及宣傳一套安全政策，該政策：

12.1.1 說明本規範的所有要求。

12.1.2 內含一套用以找出威脅及漏洞的年度程序，並應將結果呈現為正式的風險評估

12.1.3 內含一年至少一次的審核，並應於環境改變時加以更新。

12.2 制訂與本規範中之要求一致的每日作業安全程序（例如使用者帳戶維護程序、紀錄表審查程序）

12.3 針對數據機及無線裝置等重要的顧客使用技術訂定使用政策，以界定所有的員工及合約商應如何正確的使用這些技術。這些使用政策應確實要求：

12.3.1 管理階層明確的核准

12.3.2 使用技術應驗證

12.3.3 所有各該裝置及使用人的清單

12.3.4 在裝置上標示擁有人、連絡資料，以及目的

12.3.5 可接受的技術使用情況

12.3.6 可接受使用這些技術的網路位置

12.3.7 公司核准產品清單

12.3.8 一段特定時間無動作之後，自動中斷數據機作業

12.3.9 只有在供應商需要時，才為供應商開啓數據機，並應於使用後立即解除功能。

12.3.10 透過數據機遠端存取持卡人資料時，應解除將持卡人資料儲存在操作者本地硬碟、軟碟或其他外部媒體的功能。另外並應於進行遠端存取時，解除剪下及貼上，以及列印的功能。

12.4 安全政策及程序應確實明確界定所有員工及合約商的資訊安全責任。

12.5 賦予個人或團隊下列的資訊安全管理責任：

12.5.1 訂定安全政策及程序，做成文件，並分發以資遵循

12.5.2 監控並分析安全警訊及資料，並分發給相關的人員

12.5.3 訂定安全事件反應及逐步處理程序，做成文件，並分發以資遵循，以確保能即時及有效的處理所有狀況

12.5.4 管理使用者帳戶，其中包括增刪修改在內

12.5.5 監督及控管對資料進行的所有存取。

12.6 讓所有的員工都瞭解持卡人資料安全的重要性

12.6.1 教育員工（例如利用海報、信函、便箋、會議，以及倡導活動）。

12.6.2 要求員工以書面承認他們都已閱讀並瞭解公司的安全政策及程序。

12.7 篩選出可能的員工，以避免出自內部來源的攻擊風險。

對於商店出納員之類為進行交易一次只能存取一個卡號的員工，本項要求僅只是建議而已。

12.8 以合約要求所有能存取持卡人資料的第三人遵守支付卡產業安全要求，合約中最起碼應規定：

12.8.1 承認第三人對其所掌有的持卡人資料應負責任。

12.8.2 持卡人資料係各支付卡品牌、信用卡協會會員及特約商店所有，並承認各該資料僅能用於協助這些第三人完成交易、支援顧客忠誠計畫、提供詐欺管制服務，或是因法律之特別規定而供他人使用。

12.8.3 如遇重大破壞、災難或故障時，能繼續營業。

12.8.4 稽核相關規定，以確保在發生安全入侵事件之後，支付卡產業代表或支付卡產業核准之第三人能獲得充分之合作，並能進入進行澈底的安全查察，安全查察將確認是否遵守為保護持卡人資料所訂定的支付卡產業資料安全標準。

12.8.5 有關合約終止後之規定，以確保第三人應繼續以保密方式處理持卡人資料。

12.9 實施事故反應計畫，系統違失時要有萬全的立即反應準備。

12.9.1 訂定事故反應計畫，俾於系統被危害時採用。該計畫最起碼應載明特定的事故反應程序、恢復及繼續營業程序、資料備份程序、分工及職責，以及通訊及連絡策略（例如通知信用卡協會會員及信用卡協會）。

12.9.2 該計畫至少每年應測試一次。

12.9.3 指派特定人員採24/7方式待命對警訊做出反應。

12.9.4 負有安全違失反應職責之人員應加以訓練。

12.9.5 將入侵偵測、入侵預防，以及檔案完整性監控系統發出的警告納入。

12.9.6 建立一套程序，以便能根據過去所學習到的教訓修改及改善事故反應計畫，並應將業界之發展納入。