



支付卡产业数据安全标准

1.0 版本
2004 年 12 月



VISA PAYMENT SECURITY SERVICES
ASIA PACIFIC

支付卡产业 数据安全标准



免责声明

本支付卡产业(PCI)数据安全标准定义了保护帐户和交易信息的方法。然而, Visa 亚太公司并不保证, 也未声称实施这些标准就可以防止安全危害或损失。同时声明, 无论是否实施支付卡产业数据安全标准, Visa 亚太公司也不对任何所发生的安全危害或损失, 承担任何责任和义务。

重要提示

此支付卡产业 (PCI) 数据安全标准是 Visa 亚太公司全套帐户信息安全 (AIS) 文件中的一部分。所有会员和其代理商 (商户和服务提供者) 应确保其在处理、储存和传输持卡人信息时必须符合 PCI 数据安全标准 (此标准取代 2000 年 3 月 Visa AIS 标准 1.4 版本)。

有关Visa亚太公司的AIS详细资料, 请访问<http://www.visa-asia.com/secured>。

支付卡产业
数据安全标准



建立和维护安全网络

- 要求 1: 安装和维护防火墙配置来保护数据
要求 2: 不要使用厂商提供的默认的系统密码和其他安全参数

保护持卡人数据

- 要求 3: 保护储存的数据
要求 4: 通过公共网络传输持卡人数据和敏感信息必须加密

维持防范弱点攻击的管理程序

- 要求 5: 使用和定期更新防病毒的软件
要求 6: 开发和维护安全系统和应用

实施有力的访问控制检测程序

- 要求 7: 限制访问数据，因业务需要也应知道
要求 8: 分配给每个人独特的 ID 来进入计算机
要求 9: 限制物理访问持卡人数据

定期监控和测试网络

- 要求 10: 跟踪和监控所有对网络资源和持卡人数据的访问
要求 11: 定期测试系统的安全和处理过程

保持信息安全的政策

- 要求 12: 保持涉及到信息安全的政策

注意，这些支付卡产业 (PCI) 数据安全要求适用于所有储存，处理或传输持卡人数据的会员、商户和服务提供商。另外，这些安全要求适用所有被定义成网络构成、服务器，或内置的应用，或连接至持卡人数据环境的“系统成份”。网络构成包括，但不仅限于，防火墙、转接、路由、无线接入点、网络应用和其他安全应用。服务包括，但不仅限于，互联网、数据库、验证、DNS、邮件、代理服务器和 NTP。应用包括所有购买和客户应用，包括内部和外部的（互联网）应用。

建立和维护安全的网络

要求 1: 安装和维护一个防火墙设置来保护数据.

防火墙是一个计算机的设施，来控制计算机的通信允许从外面进入到公司的网络，在公司的内部网络也控制进入到高敏感区域的通信。所有系统需要受保护来防止从因特网未经授权的访问，无论是电子商务、员工通过桌上型电脑浏览器以因特网方式访问，还是员工电子邮件访问。通常，表面上无关紧要的进出因特网的路径可以提供未经保护的途径访问到关键系统。防火墙对任何计算机网络是关键的保护机制。

1.1 建立防火墙设置标准包括:

- 1.1.1 一个正式的批准和测试所有外部网络连接和改变防火墙设置的处理方式
- 1.1.2 一个现在的所有连接持卡人数据的网络图，包括任何无线网络
- 1.1.3 在每一个因特网连接和在 DMZ 与内部互联网之间的防火墙要求
- 1.1.4 描述网络构成的逻辑管理的组、任务和责任
- 1.1.5 业务必须的服务/端口的文档列表
- 1.1.6 除了 HTTP、SSL、SSH 和 VPN 之外的其他有效协议的理由和文档
- 1.1.7 任何允许的风险协议（FTP 等）的理由和文档，包括使用这些协议和实施的安全特征的原因
- 1.1.8 定期审阅防火墙/路由器的规则设置
- 1.1.9 路由器的设置标准

1.2 建立防火墙的配置，来拒绝从“不信任”的网站/主机过来的所有通信，除了:

- 1.2.1 万维网协议 - HTTP (端口 80) 和安全的加密套接字协议层 (SSL) (典型的 443 端口)
- 1.2.2 系统管理协议，如，安全位置 (SSH) 或虚拟的专用网 (VPN)
- 1.2.3 其他的业务协议要求 (如，ISO 8583).

1.3 建立防火墙的配置，限制公共访问服务器和任何储存持卡人数据的系统成份之间的连接，包括任何从无线网络的连接。这个防火墙设置应该包括:

- 1.3.1 限制内部的因特网进入在 DMZ (进入过滤) 内的 IP 地址
- 1.3.2 限制内部和外部的因特网通信进入端口 80 和 443
- 1.3.3 不允许内部的地址通过因特网进入 DMZ (出口过滤)
- 1.3.4 正式的检查，如已知的动态信息包过滤 (只有“已确定”的连接才可以进入网络)
- 1.3.5 在内部的网络区域里放置数据，通过隔离区进行隔离
- 1.3.6 限制外部的通信进入有关的必须进入的支付卡环境
- 1.3.7 保护和同步路由配置文件 (如，运行配置文件 - 用于日常的路由器运行；和启动配置文件 - 用于机器重新启动，必须保持一致的安全配置).
- 1.3.8 拒绝其他所有的内部和外部的非特定允许的通信
- 1.3.9 在任何无线网络和支付卡环境之间安装周边防火墙，并配置这些防火墙来拒绝任何从无线环境过来的通信，或控制它 (如果这些通信是因业务需求而必须的)
- 1.3.10 在所有可以直接连接到因特网的，可以用来进入公司的网络的手机和/或员工拥有的计算机 (如员工使用的台式机) 上安装个人防火墙软件。

1.4 禁止外部网络和所有储存持卡人信息 (如数据库) 的系统成份之间的直接进入。

- 1.4.1 安装一个隔离区来过滤和监视所有通信，禁止内部和外部的因特网通信直接发送。
- 1.4.2 限制外部通信通过支付卡应用进入到 DMZ 内的 IP 地址。
- 1.5 使用因特网协议 (IP) 转化法来防止内部的地址在因特网上被翻译和透露. 使用如端口地址转化 (PAT) 或网络地址转化 (NAT) 技术来实施 RFC 1918 地址间隔。

要求 2: 不要使用厂商提供的默认系统密码和其他安全参数。

骇客们 (公司外部的和内部的) 经常使用厂商的默认密码和其他缺省设置来危害系统。这些密码和设置在骇客群里是被熟知的，容易通过公众信息来确定。

- 2.1 在网络安装系统前一定要更改厂商提供的默认值 (如，密码，SNMP 群落串, 和消除不必要的帐户等。)
 - 2.1.1 对于无线环境，改变无线厂商的默认值，包括但不限于，WEP 密钥，默认 SSID，密码，SNMP 群落串, 和停止 SSID 播送。当有 WPA 能力时，应启用无线局域网保护访问 (WPA) 技术进行加密和验证。
- 2.2 对所有系统成份制订配置标准. 确保这些标准可以应对已知的安全弱点和符合行业最佳模式。
 - 2.2.1 对每一个服务器只执行一个基本的功能。(如，网站服务器，数据服务器, DNS 只应该安装在单独的服务器上)
 - 2.2.2 停止所有不必要的和不安全的服务和协议 (指完成设备所确定的功能时不直接需要的服务和协议)。
 - 2.2.3 配置系统安全参数防止误使用。
 - 2.2.4 消除所有不必要的功能，如脚本，驱动，特征，子系统，文件系统 (如不必要的网站服务器)。
- 2.3 加密所有非控制台的管理访问. 使用如 SSH, VPN, 或 SSL/TLS 技术用于以网站为基础的管理和其他非控制台的管理访问。

保护持卡人数据

要求 3: 保护存储的数据

加密是最后的保护机制，因为即使有人突破了所有其他保护机制并获得进入了加密数据，没有攻破加密的话，他们仍旧没法读取数据。这是从深度原则上的一个防范说明。

- 3.1 最小限度的储存持卡人信息。制定数据保留和处置政策。限制因业务，法律和/或调整目的而储存的数目和保留时间，并在数据保留政策里标明。
- 3.2 不要储存敏感的可以用来授权的验证数据 (即使加密也不需要):
 - 3.2.1 不要储存从磁条上得到的任一磁道上的全部内容 (在卡片的背后，在芯片等等)
 - 3.2.2 不要储存卡片验证码 (印刷在支付卡的前面或后面的三位或四位数值。(如，CVV2 和 CVC2 数据))
 - 3.2.3 不要储存密码验证值 (PVV)
- 3.3 显示帐号时进行掩盖 (最多可显示前六位和最后四位)。

注意，这不适用于那些因特定需要来看信用卡完整号码的员工和其他组织。
- 3.4 无论何处储存敏感的持卡人数据时，使用以下任一方法来使之不可读，(包括在手提媒介中的数据、备份媒介、日志和从无线网络中得到和储存的数据):
 - 单方向的杂乱 (杂乱索引), 如 SHA-1
 - 截断
 - 索引记号和 PADs, 用 PADs 来安全储存
 - 强大的加密法, 如用相应的密钥管理步骤和程序进行的三重 DES 128 位或 AES 256 位。

最低需要使之不可读的帐户信息是支付卡的帐号。
- 3.5 保护加密密钥防止泄露和误用。
 - 3.5.1 限制必须使用密钥的最少管理人数。
 - 3.5.2 用可能的最少地点和方式来安全储存密钥。
- 3.6 全程记录和实施所有密钥管理步骤和程序，包括:
 - 3.6.1 强大的密钥产生
 - 3.6.2 安全的密钥分发
 - 3.6.3 安全的密钥储存
 - 3.6.4 定期的密钥更换
 - 3.6.5 过期密钥的销毁
 - 3.6.6 密钥的分开知道和双重控制 (因此需要 2 或 3 人，每一个只知道他自己的那部分密钥，而不能推测整个密钥)。
 - 3.6.7 防止非授权的密钥替换
 - 3.6.8 替换已知或怀疑泄露的密钥
 - 3.6.9 撤回过期或无效的密钥(主要是 RSA 密钥)
 - 3.6.10 要求密钥的保管者签署一份表格确认其理解和接受密钥管理者的责任

要求 4: 通过公共网络传输持卡人数据和敏感信息必须加密。

通过因特网传输敏感信息必须加密，因为它在传输的时候，骇客通常也很容易的截取和/或转移数据。

- 4.1** 使用强大的密码系统和加密术 (至少 128 位) 如加密套接字协议层 (SSL), 点对点通道协议 (PPTP), 因特网协议安全 (IPSEC)等, 在通过公共网络传输时保护敏感的持卡人数据。
- 4.1.1** 对于无线网络传输持卡人数据时, 如有WPA能力时, 使用无线局域网保护访问 (WPA) 技术来加密传输, 或128位的VPN或SSL。不要绝对地依赖WEP来保护机密信息和访问无线局域网。使用以上的一种方法和128位的WEP一起, 并每季度地旋转分享的WEP密钥, 并且只要有人员变动就更换。
- 4.2** 决不通过未加密的邮件传输持卡人信息。

维持防范弱点攻击的管理程序

要求 5: 使用并定期更新防病毒软件或程序

许多弱点攻击和恶意病毒通过员工的电子邮件活动,进入网络。防病毒软件必须用在所有的电子邮件系统和台式电脑来保护系统不受恶意软件影响。

- 5.1 在所有容易受病毒影响的系统, (如, 计算机和服务器), 布置防病毒机制。
- 5.2 确保所有防病毒的机制是最近的、有效地运行, 并有能力产生审查日志。

要求 6: 发展和维护安全系统和应用

不道德的个人使用安全弱点来获得进入系统的特权。许多这些弱点可以通过厂商的安全补丁来修补, 并且所有系统都应该要有最新的软件补丁, 来防范员工、外部骇客和病毒的侵害。对于自我开发的应用, 许多弱点可以通过使用标准的系统开发步骤和安全代码技术来避免。

- 6.1 确保所有系统成份和软件都有最新的厂商提供的安全补丁。
 - 6.1.1 在出版 1 个月内, 安装相关的安全补丁。
- 6.2 建立一个步骤来确定最新发现的安全弱点(如, 在因特网上免费订阅警报服务)。更新你的标准来对付新的弱点问题。
- 6.3 开发基于行业最佳模式的软件应用, 并在开发整个周期里包含信息安全。包括:
 - 6.3.1 在实施前, 测试所有的改变过的安全补丁和系统、软件的配置。
 - 6.3.2 分隔开发/测试和生产环境。
 - 6.3.3 分隔开发/测试和生产环境的责任。
 - 6.3.4 生产数据(真实的信用卡号码)不可以用于测试或开发。
 - 6.3.5 在生产系统投产前, 消除测试数据和帐号。
 - 6.3.6 在应用投产或向客户发布前, 消除客户的应用帐号, 用户名和密码。
 - 6.3.7 在向客户发布产品前, 审阅客户的代码, 以确定任何潜在的代码弱点。
- 6.4 对所有系统和软件配置的改变, 必须遵守改变控制程序。这个程序必须包括:
 - 6.4.1 影响的文档
 - 6.4.2 适合的人员来停止管理
 - 6.4.3 测试来验证运作的功能
 - 6.4.4 收回程序
- 6.5 根据安全代码指南来开发网络软件和应用, 如开放式网络运用安全项目指南。审阅客户应用代码来确定代码弱点。参见 www.owasp.org - “十个最危险的网络运用安全代码”。在软件开发过程中, 应防范较常见的代码弱点包括:
 - 6.5.1 无效的输入
 - 6.5.2 破坏的访问控制 (如, 恶意的使用用户)
 - 6.5.3 破坏的验证/会话管理 (使用帐户信任和会话资料夹)
 - 6.5.4 跨场所的脚本 (XSS) 攻击
 - 6.5.5 缓冲器溢出
 - 6.5.6 入射缺陷(如, SQL 入射)

- 6.5.7 不当的错误操作
- 6.5.8 不可靠的储存
- 6.5.9 服务拒绝
- 6.5.10 不可靠的配置管理

实施有力的访问控制检测程序

要求 7: 限制访问数据,因业务需要也应知道。

这个是确保机密的数据只能通过一个经授权的方式来访问。

- 7.1 限制访问计算机源数据和持卡人信息,只有那些因工作需要的人员才可以访问。
- 7.2 对多用户的系统建立一个机制,根据只有一个用户才需知道的原则来限制访问,除非特别允许,应该设置成“全部拒绝”。

要求 8:分配给每一个人独特的 ID 来进入计算机。

这个是确保在处理机密的数据和系统时,只能由已知的并被授权的用户完成,并且能够被跟踪。

- 8.1 在允许他们访问系统组成或持卡人数据前,确定给所有用户一个独特的用户名。
- 8.2 除了独特的身份辨别外,雇主至少用以下一种方式,来验证所有用户:
 - 密码
 - “代码”设备(如,安全 ID,证书,或公钥)
 - 生物鉴定
- 8.3 员工,管理员和第三方使用远程访问系统时,实施两因子验证方法来验证。使用如 RADIUS 或 TACACS 代码等技术,或 VPN 来对个人验证。
- 8.4 在所有系统组成里,当传输和储存时,加密所有的密码。
- 8.5 在所有系统组成里,确保对非消费者的用户和管理者,有正确的用户验证和密码管理方法:
 - 8.5.1 对用户的 ID,信任状和其他检验对象进行增加、删除和修改时进行控制。
 - 8.5.2 在完成密码重置前,验证用户身份。
 - 8.5.3 对每一个用户设置一个唯一的首次密码,并在第一次使用时,立即更改。
 - 8.5.4 对已终止的用户立即撤销访问。
 - 8.5.5 至少每 90 天消除不活动的用户帐号。
 - 8.5.6 只有在需要的时候,才激活帐户让厂商进行远程维护使用。
 - 8.5.7 对需要访问持卡人信息的所有用户,分发密码的管理手续和政策。
 - 8.5.8 不要使用群,共享,或一般的帐户/密码。
 - 8.5.9 至少每 90 天更改用户密码。
 - 8.5.10 对密码的最低长度,有要求,至少 7 个字符。
 - 8.5.11 使用同时包含数字和字母字符的密码。
 - 8.5.12 不允许个人设置一个新密码时,和他/她曾使用过的最后 4 个密码相同。
 - 8.5.13 限制重复访问尝试,在不超过最多 6 次的尝试后应冻结用户 ID。
 - 8.5.14 设置冻结时间至 30 分钟或直到管理员来激活用户 ID。
 - 8.5.15 如果进程空闲超过 15 分钟,需要用户重新输入密码或再启动终端。
 - 8.5.16 包含持卡人信息的任何数据的所有访问都需要验证。这包括应用、管理和其他所有用户的访问。

要求 9: 限制物理访问持卡人数据

任何物理访问含有持卡人数据或系统的地方,都有可能访问到设备或数据,也会移动系统或硬拷贝,应该适当地限制。

- 9.1 使用适当的访问控制设备来限制和监控物理访问储存、处理或传输持卡人数据的系统。
 - 9.1.1 使用摄像头监控敏感区域。审查这些数据并和其他的访问联系起来。保存至少三个月,除非其他另有法律的限制。
 - 9.1.2 限制物理访问公众可进入的网络接口。
 - 9.1.3 限制物理访问无线接入点,网关和手持设备。
- 9.2 制定程序来帮助所有职员很容易的区分员工和访客,特别是涉及到持卡人信息的地方。

“员工”是指工作在公司里的全职或兼职的雇员、临时雇员/职员和顾问。一个“访客”是指那些需要短期进入公司,而通常不超过一天的厂商、雇员的客人、服务职员和其他人员。
- 9.3 确保所有的访客都:
 - 9.3.1 在进入处理和维持持卡人数据的区域前得到核准
 - 9.3.2 得到一个有期限的物理的标志(如,徽章或进入图案),并可以识别他们为非雇员
 - 9.3.3 要求他们在离开公司或在到期日交还物理标志。
- 9.4 使用访客日志来保留对访客活动的物理踪迹审查。保留这些日志至少三个月,除非法律另有限制。
- 9.5 在安全的公司外部保存备份的媒介,可以是预备的第三方或商业储存公司。
- 9.6 所有包含持卡人信息的纸张和电子媒介必须物理安全。(如,计算机、电子媒介、网络和通讯硬件、无线电通讯线路、收据、报告和传真)。
- 9.7 任何形式的内部或外部分发含有持卡人信息的媒介都需要严格控制。
 - 9.7.1 标注这些媒介,使它可以被识别为机密。
 - 9.7.2 通过安全的快递或传输机制来递送这些媒介,并可以被精确地追踪。
- 9.8 从一个安全的地方移动所有的媒介时,必须确保得到管理者批准。(特别是媒介是分发到个人的时候)。
- 9.9 对储存和可访问持卡人信息的媒介,维持一个严格的控制:
 - 9.9.1 所有媒介都要有完全的详细目录并确保是安全储存。
- 9.10 当含有持卡人信息的媒介因业务或法律原因不再需要使用时,应当销毁:
 - 9.10.1 交叉切割成碎片,烧成灰,或把硬拷贝变成纸浆。
 - 9.10.2 清除、消磁、粉碎或其他销毁电子媒介的方法,使持卡人数据不能被恢复。

定期监控和测试网络

要求 10: 追踪和监控所有对系统资源和持卡人数据的访问。

登录机制和可追踪用户行为是很重要的。有错误发生时，在所有环境里日志的存在可以十分彻底地追踪和分析。没有系统活动日志要确定泄露的原因是很困难的。

- 10.1** 对每一个个人用户所有连接进入系统成份的建立一个过程 (特别是那些以管理者特权，如根用户，来进行的)。
- 10.2** 对所有系统成份，实施自动追踪索引来反映以下事件:
 - 10.2.1** 所有个人用户访问持卡人数据
 - 10.2.2** 所有以根或管理员特权进行的个人活动
 - 10.2.3** 访问所有审查索引的
 - 10.2.4** 不合乎逻辑的访问尝试
 - 10.2.5** 使用辨别和验证机制
 - 10.2.6** 初始化审查日志
 - 10.2.7** 建立和删除系统级的对象。
- 10.3** 对所有系统成份，对每项事件至少记录以下的审查索引:
 - 10.3.1** 用户验证
 - 10.3.2** 事件的类型
 - 10.3.3** 日期和时间
 - 10.3.4** 成功或失败指示
 - 10.3.5** 事件的发源
 - 10.3.6** 受影响的数据、系统成份或资源的身份或名称。
- 10.4** 同步所有重要系统的时种和时间。
- 10.5** 保护审核索引使之不能被改变，包括以下:
 - 10.5.1** 限制因工作相关需要而需浏览审核索引
 - 10.5.2** 保护审核索引文件防止非授权修改
 - 10.5.3** 及时备份审核索引文件，并集中到日志服务器或媒介中，使之不容易改变
 - 10.5.4** 复制无线网络的日志到内部局域网的日志服务器中
 - 10.5.5** 在日志上使用完整的文件监控/改变侦测软件 (如 Tripwire)，来确保现有的日志数据在不产生警告下没法改变 (尽管新增数据不应该产生警告)。
- 10.6** 至少每天审阅所有系统成份的日志。日志审阅应该包括完成安全功能的服务器，如 IDS 和验证 (AAA) 服务器 (如，RADIUS)。
- 10.7** 保留你的审核索引历史记录一段时间，与它的有效使用相一致，也要符合法律规定。
一个审核记录一般要反映至少一年的历史，至少在线 3 个月有效。

要求 11: 定期测试系统的安全和处理过程

弱点可以不断地被骇客/研究者通过新的软件被发现。系统、处理过程和客户软件应该经常被测试以确保安全一直、并在有改变的时候都有保护。

- 11.1 测试安全控制、限制、网络连接和例行限制，都是为确保他们可以充分辨别和停止任何非经授权的访问尝试。当无线技术有应用的时候，定期使用无线分析器来辨别所有在用的无线设备。
- 11.2 至少每个季度或网络里有任何显著改变后，（如新安装系统成份、改变网络拓扑、防火墙规则改变、产品升级），进行内部和外部网络的弱点扫描。
注意，外部弱点扫描必须由支付卡产业验证的扫描服务商进行。
- 11.3 对网络架构和应用至少每年一次，或任何显著的架构和应用升级或修改，（如，操作系统升级、分网络增加到环境中、网络服务器增加到环境中），完成渗透测试。
- 11.4 使用网络侵入侦测系统、基于主机的侵入侦测系统，和/或侵入防止系统来监控所有的网络交易和提醒职员有嫌疑的泄露。保持所有的侵入侦测和防止系统运行在最新的状态。
- 11.5 布置完整的监控文档，来提醒职员有非授权的重要系统和目录文件的修改，并至少每天完成重要文件的比对(如果可以进行自动处理，可以更频繁些)。
重要文件并不是一定包含持卡人数据。为完整文件监控目的，重要文件通常是那些不经常更改，但一旦修改，可能会引起系统危害或风险危害。完整文件监控产品通常用操作系统相关的重要文件已预先确定的方式进行。其他重要文件，如客户应用，必须由商户或服务提供商来评估和确定。

保持信息安全的策略

要求 12: 对员工和合约人保持一个用于信息安全的策略。

一个强硬的安全策略对整个公司规范了安全特征，并使员工知道什么是期望他们遵守的。所有的员工必须意识到保护数据安全性是他们的责任。

- 12.1** 建立、出版、保持和发布一个安全策略，应该：
 - 12.1.1** 在这规范里确定所有的要求。
 - 12.1.2** 应包括一本处理手册来确定危害，弱点，并在正式风险评估里给出结果。
 - 12.1.3** 应至少一年一次或当环境变化时进行审查和更新。
- 12.2** 实施日常的操作安全程序来和规范里所确定的要求相一致。(如，用户帐户的维护程序，日志审阅程序)
- 12.3** 对重要的技术方面的员工实施使用政策，如调制解调器和无线，对所有的员工和合约人确定使用这些技术的正确方法。确保这些使用政策包括：
 - 12.3.1** 清楚的管理者批准
 - 12.3.2** 使用这技术的验证
 - 12.3.3** 所有这些设备和使用者的名单
 - 12.3.4** 表明设备的拥有者，联系方式和用途
 - 12.3.5** 许可的使用技术的方法
 - 12.3.6** 许可的这些技术的网络位置
 - 12.3.7** 公司批准的产品名单
 - 12.3.8** 在一定的不活动期限后，自动断开调制解调器进程
 - 12.3.9** 只有需要厂商时，才对厂商激活调制解调器，使用后应立即停止激活。
 - 12.3.10** 当通过调制解调器远程进入持卡人数据时，不允许把持卡人数据存储在本地硬盘、软驱或其他外部媒介。同样在远程进入时不允许剪裁复制和打印功能。
- 12.4** 确保这些安全政策和程序对所有员工和合约人明确定义了信息安全的责任。
- 12.5** 以下信息安全管理责任，应分配给个人或团队：
 - 12.5.1** 建立、文档化和分发安全政策和策略
 - 12.5.2** 监控和分析安全警告和信息，并发送给适当的人员
 - 12.5.3** 建立、文档化和分发安全事件的响应和逐级上报的程序，确保及时和有效地处理所有的情况
 - 12.5.4** 管理者用户帐号，包括增加、删除和修改。
 - 12.5.5** 监控和控制所有数据的访问。
- 12.6** 使所有员工意识到持卡人信息安全的重要性
 - 12.6.1** 员工教育(如，通过海报、信函、备忘录、会议和晋升)。
 - 12.6.2** 要求员工书面确认他们已经阅读和理解了公司的安全政策和程序。
- 12.7** 监控有可能可疑的员工，将来自内部的风险侵袭危害最小化。

那些有可能可疑的员工，是指一次仅只涉及一张卡号并熟悉交易过程，如商店收银员等。这个要求仅作参考。

- 12.8** 以合约方式要求所有的第三方公司在访问持卡人数据时，必须追随支付卡产业安全要求。作为最低要求，合约必须涉及到：
- 12.8.1** 确认第三方公司对持卡人数据的安全拥有责任。
 - 12.8.2** 每一个支付卡品牌、收单行和商户的持卡人数据的所有人，确认这些数据只用于帮助那些公司完成交易，支持忠诚项目，提供欺诈控制服务，或其他法律确定的使用。
 - 12.8.3** 如果发生大的破坏、灾难或故障，如何确保业务连续性。
 - 12.8.4** 审核规定来确保支付卡产业代表，或一个支付卡产业批准的第三方公司，在发生安全侵入后，可以被提供全面的合作和访问来进行彻底的安全审查。这审核将确认是否依从支付卡产业数据安全标准来保护持卡人数据。
 - 12.8.5** 终止规定来确保第三方公司将继续视持卡人数据为机密信息。
- 12.9** 执行一个应急响应计划，准备着迅速响应系统破坏。
- 12.9.1** 建立一个应急响应计划来用于如果发生系统危害。确保计划至少含：特定的应急响应程序、业务恢复和继续程序、数据备份过程、角色和责任，和通讯和联系策略。(如，通知收单行和信用卡组织)。
 - 12.9.2** 至少每年进行测试。
 - 12.9.3** 任命特定的人员可以 7*24 小时响应警告。
 - 12.9.4** 为员工提供相应的安全破坏响应责任培训。
 - 12.9.5** 包括侵入侦测警报、侵入防范，和文档完整性监控系统。
 - 12.9.6** 应有一个步骤，根据所学到的教训和适应产业发展而修改和改进应急响应计划。