支付卡行业 (PCI)
数据安全标准

PCI DSS 导航

了解要求的目的

1.2 版

2008 年 10 月

文件变更记录

日期	版本	描述
2008 年 10 月 1 日	1.2	与 PCI DSS 1.2 新版内容保持一致，并对原版 1.1 以来的版本实行了较小变更。

目录

序言

本文件说明支付卡行业数据安全标准 (PCI DSS) 的 12 项要求以及解释每项要求的目的之指南。本文件旨在帮助商户、服务提供商和金融机构更清楚地了解支付卡行业数据安全标准，以及对于支持持卡人数据环境的安全系统组件（服务器、网络和应用程序等）的详细要求，其背后包含的特定含义和目的。

注：《*PCI DSS 导航：了解要求的目的*》仅用于指导说明。当完成 PCI DSS 现场评估或自行评估调查问卷 (SAQ) 时，记录文件是《*PCI DSS 要求和安全性评估程序*》以及《*PCI DSS 自行评估调查文件 1.2 版*》。

PCI DSS 要求适用于包含在或连接至持卡人数据环境的所有系统组件。持卡人数据环境是处理持卡人数据或敏感验证数据的部分网络，包括网络组件、服务器和应用程序。

- 网络组件包括但不局限于防火墙、交换机、路由器、无线接入点、网络设备和其他安全设备。
- 服务器类型包括但不局限于以下种类：Web、数据库、验证、邮件、代理、网络时间协议 (NTP) 和域名服务器 (DNS)。
- 应用程序包括但不局限于所有购买和自定义的应用程序，包括内部和外部（互联网）应用程序。

充足的网络分段可以将存储、处理或传输持卡人数据的系统与那些不进行这些操作的系统隔离开来，从而缩小持卡人数据环境范围。合格安全性评估商 (QSA) 可以通过实施适当的网络分段，协助确定机构的持卡人数据环境的范围，并提供如何缩小 PCI DSS 评估范围的指南。有关具体实施是否符合标准或者“遵从”具体要求的问题，PCI SSC 建议公司咨询合格安全性评估商 (QSA)，来验证公司对技术和流程的实施和对 PCI 数据安全标准的遵从。QSA 应对复杂网络环境的专业知识非常有益于为努力达成合规的商户或服务提供商提供最优方法和指导。PCI SSC 的合格安全性评估商清单位于：https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf。

持卡人数据和敏感验证数据元素

下表描述了持卡人数据和敏感验证数据的常用元素，无论是允许还是禁止每项数据的**存储**，或者是必须**保护**每个数据元素。该表格的内容并非详尽无遗，它只用于列举适用于每种数据元素的不同类型的要求。

持卡人数据定义为主账户（“PAN”或信用卡号码）和作为支付交易一部分获得的其他数据，包括以下数据元素（请参阅下表了解详细信息）：

- PAN
- 持卡人姓名
- 失效期
- 业务代码
- 敏感验证数据：(1) 完整磁条数据，(2) CAV2/CVC2/CVV2/CID 和 (3) PIN/PIN 数据块

主账户 (PAN) 是 PCI DSS 要求与 PA-DSS 适用性方面的决定性因素。如果 PAN 未被存储、处理或传输，则 PCI DSS 与 PA-DSS 不适用。

	数据元素	允许存储	需要保护	PCI DSS 要求 3, 4
持卡人数据	主账户	是	是	是
	持卡人姓名[1]	是	是 [1]	否
	业务码 [1]	是	是 [1]	否
	失效日 [1]	是	是 [1]	否
敏感验证数据 [2]	完整磁条数据 [3]	否	不存在	不存在
	CAV2/CVC2/CVV2/CID	否	不存在	不存在
	PIN/PIN 数据块	否	不存在	不存在

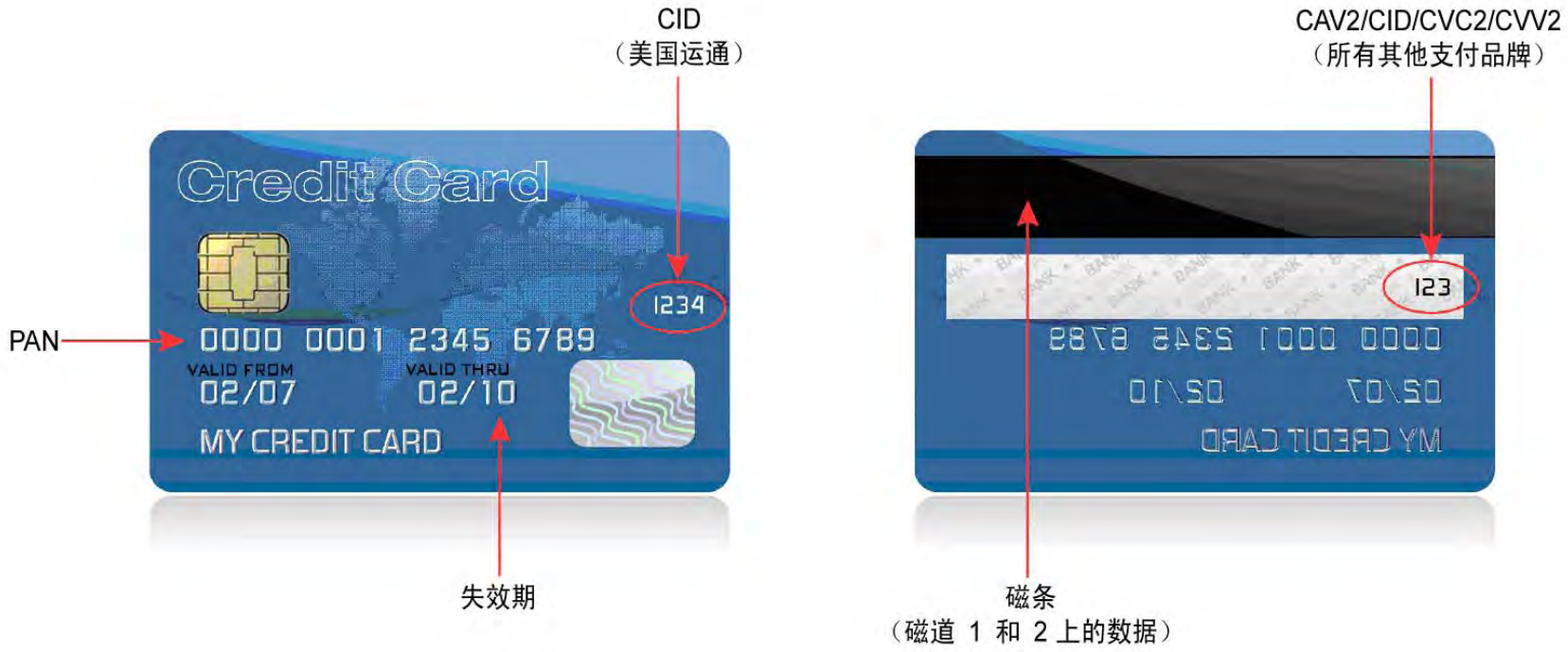
1 这些数据元素如果连同 PAN 一起存储，则必须对其进行保护。该保护措施应当符合 PCI DSS 对持卡人环境的一般保护的相关要求。此外，如果在业务过程中收集与消费者相关的个人数据，其他立法（例如，与消费者个人数据保护、隐私、身份盗窃或数据安全有关的法律）可能要求对此类数据进行特别保护，或要求对公司操作进行适当披露。然而，如果不对 PAN 进行存储、处理或传输，则 PCI DSS 不适用。

2 敏感验证数据不应在验证后存储（即便是经过加密的）。

3 来自磁条、芯片上的磁条图形或其他地方的全磁道数据。

持卡人数据和敏感验证数据的位置

敏感验证数据包括磁条（或磁道）数据[4]、卡验证值或代码[5] 和 PIN 数据[6]。**严禁存储敏感验证数据！**此类数据对于恶意个人非常有用，因为它使得这些人可以伪造支付卡并创建欺诈交易。请参阅 *PCI DSS 与 PA-DSS 术语、缩略语*，查看“敏感验证数据”的完整定义。下图是信用卡的正面与反面，显示了持卡人数据和敏感验证数据的位置。



[4] 编译在磁条中的数据，用于实卡交易中的授权。此数据还可以在芯片上的磁条图形中或卡的其他位置找到。交易授权之后，机构可能不会保留完整的磁条数据。可以被保留下来的磁道数据元素只能包括主账号、持卡人姓名、失效期与业务代码。

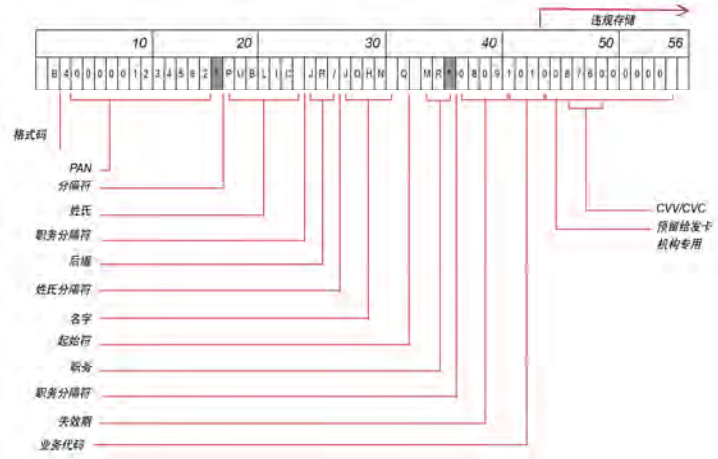
[5] 印在支付卡签名方格内或右侧或者印在支付卡面上的三或四位数值，用于验证无实卡交易。

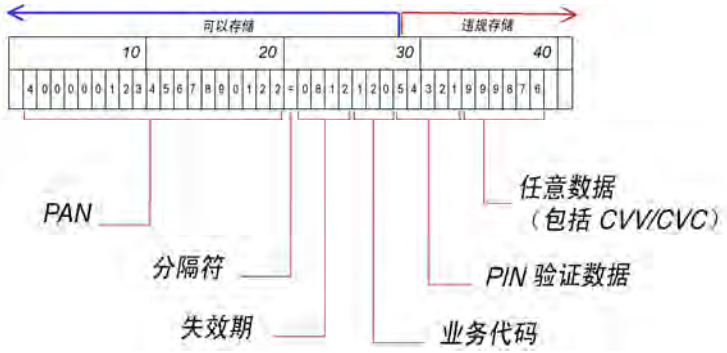
[6] 由持卡人在实卡交易时输入的个人识别码和/或出现在交易信息中的经加密的 PIN 数据块。

磁道 1 与磁道 2 数据

如果存储了全磁道（磁道 1 或磁道 2，来自磁条、芯片上的磁条图形或其他位置）数据，获得该数据的恶意个人就可以在全世界复制和销售支付卡。存储全磁道数据也违反了支付品牌的经营规则并可能导致罚款和惩罚。下图提供了有关磁道 1 和磁道 2 数据的信息，描述二者的差异并显示了存储在磁条上的数据的布局。

磁道 1	磁道 2
▪ 包含磁道 1 和磁道 2 的所有字段 ▪ 最大长度为 79 个字符	▪ 对于较旧的拨号传输装置，处理时间更短 ▪ 最大长度为 40 个字符





PCI 数据安全标准的相关指南

构建并维护安全的网络

要求 1：　安装防火墙配置并予以维护，以保护持卡人数据

要求 2：　系统密码和其他安全参数不使用供应商提供的默认设置

保护持卡人数据

要求 3：　保护存储的持卡人数据

要求 4：　在开放型的公共网络中对持卡人数据进行加密传输

维护漏洞管理程序

要求 5：　使用杀毒软件并定期更新

要求 6：　开发、维护安全系统和应用程序

执行严格的访问控制措施

要求 7：　只有具备业务需求的人才能访问持卡人数据

要求 8：　为每位拥有计算机访问权限的用户分配唯一的 ID

要求 9：　限制对持卡人数据的物理访问

定期监控和测试网络

要求 10：　跟踪和监控访问网络资源和持卡人数据的所有操作

要求 11：　定期测试安全系统和流程

维护信息安全政策

要求 12：　维护针对信息安全的政策

要求 1 和要求 2 指南： 构建并维护安全的网络

要求 1：安装防火墙配置并予以维护，以保护持卡人数据

防火墙是控制公司网络（内部）和不受信任网络（外部）之间的计算机流量以及进出公司内部受信任网络更敏感区域的流量的设备。持卡人数据环境是公司受信任网络内部更敏感区域的一个示例。

防火墙检测所有网络流量并阻止那些不满足特定安全标准的传输。

所有系统必须受到保护，防止从不受信任网络进行未授权访问，无论是通过互联网以电子商务形式、员工通过桌面浏览器进行的互联网访问、员工电子邮件访问、诸如企业对企业连接的专门连接、通过无线网络或是其他途径进入系统。通常看似无关紧要进出不受信任网络的途径都可能成为关键系统的未保护入口。防火墙是所有计算机网络的关键保护机制。

要求		指导说明
1.1	建立包含以下各项的防火墙和路由器配置标准：	防火墙和路由器是控制进出网络的架构的关键组件。这些设备是阻止不需要的访问并管理进出网络授权访问的软件或硬件设备。如果没有落实政策和程序来记录员工应如何配置防火墙和路由器，公司很容易失去数据保护防御阵地的第一道防线。政策和程序有助于确保公司数据保护防御阵地的第一道防线保持坚固。
1.1.1	批准和测试所有外部网络连接以及更改防火墙和路由器配置的正式流程	批准和测试所有连接以及更改防火墙和路由器配置的政策有助于预防因网络、路由器或防火墙配置不当导致的安全问题。
1.1.2	当前网络图表，带有至持卡人数据的所有连接，包括所有无线网络	网络图表可让公司确定所有网络设备的位置。此外，网络图表可用于映射持卡人数据通过网络和在单个设备之间的数据流，以便完全了解持卡人数据环境的范围。如果没有当前网络和数据流图表，带有持卡人数据的设备可能会被忽略，并在不知情的情况下被置于针对 PCI DSS 实施的多层安全控制之外，从而极易受到威胁。
1.1.3	每个互联网连接处和隔离区 (DMZ) 与内部网络区域之间的防火墙要求	在进出网络的每个连接处使用防火墙可让公司监视并控制进出访问，并尽量降低恶意个人获得对内部网络访问权限的可能性。
1.1.4	网络组件逻辑管理的组、角色和责任的说明	角色和责任分配的说明可确保个人明确地对所有组件的安全负责并意识到各自的责任，并确保没有设备未受到管理。

要求		指导说明
1.1.5	使用允许的所有服务、协议和端口的文档和业务原因，包括为那些认为不安全的协议实施的安全功能的文档	威胁通常是因未使用或不安全的服务和端口而引起，因为这些服务和端口常常存在已知的漏洞。许多公司易受这些类型威胁的原因是他们没有针对未使用的服务、协议和端口的安全漏洞安装补丁（即使这些漏洞仍然存在）。每个公司都应明确确定公司必需的服务、协议和端口，针对他们的记录进行记录，并确保所有其他服务、协议和端口已禁用或删除。而且公司应考虑阻止所有流量，然后只重新打开已确定并记录了需要的那些端口。 另外，企业需要（或在默认情况下已启用）的许多服务、协议或端口常常被恶意个人用来威胁网络。如果这些不安全的服务、协议或端口对于公司来说是必需的，则公司应清楚地了解并接受由使用这些协议所引起的风险、调整对协议的使用并应当记录和实施允许这些协议安全使用的安全功能。如果这些不安全的服务、协议或端口对于公司来说不是必需的，则应禁用或将其删除。
1.1.6	要求至少每 6 个月检查一次防火墙和路由器的规则设置	这一检查让公司有机会至少每 6 个月清除一次不需要的、过时的或错误的规则，并确保所有规则设置只允许与业务原因相符的授权服务和端口。 我们建议更频繁地实行这些检查（如每月检查一次），以确保规则设置是当前的并符合业务需要，而不会打开安全漏洞和承受不必要的风险。
1.2	设置一个限制持卡人数据环境中不受信任网络和任何系统组件之间的连接的防火墙配置 *注：“不受信任网络”是指属于受审查机构的网络以外的任何网络，和/或机构无法控制或管理的网络。*	在内部受信任网络和任何其他不受信任网络（外部和/或不在机构控制或管理能力之内）之间安装网络防护（即防火墙）是十分必要的。未能正确地实施这一措施意味着机构将易于受到恶意个人或软件的未授权访问。 如果已安装防火墙但没有规则来控制或限制某些流量，恶意个人仍可能利用有漏洞的协议和端口攻击您的网络。
1.2.1	限制持卡人数据环境必需的进出流量	这项要求旨在防止恶意个人通过未授权的 IP 地址或以未授权的方式（例如，从您的网络内部将获取的数据发送至外部未受信任的服务器）利用服务、协议或端口访问公司网络。 所有防火墙都应该包括一条规则，即拒绝并非特定需要的所有进出流量。这将可以防止允许其他非故意但存在潜在危害的流量进出的疏忽漏洞。

要求	指导说明
1.2.2 保护并同步路由器配置文件	尽管运行配置文件通常使用安全设置执行，但启动文件（路由器只在重新启动时运行这些文件）则不能使用相同的安全设置来执行，因为后者只偶尔运行。当路由器在没有与运行配置文件相同的安全设置的情况下重新启动，则可能导致规则更为薄弱而允许恶意个人进入网络，原因是启动文件不能使用与运行配置文件相同的安全设置来执行。
1.2.3 在任何无线网络和持卡人数据环境之间安装外围防火墙，并且将这些防火墙配置为禁止来自无线环境的任何流量或控制任何流量（如果业务目的需要这种流量）	在网络中实施和利用无线技术，不论已知或是未知，都是恶意个人获取对网络和持卡人数据访问权限的一种常见途径。如果无线设备或网络在没有得到公司许可的情况下安装，恶意个人则可以轻易“隐身”进入网络。如果防火墙不限制从无线网络访问支付卡环境，未经授权而访问无线网络的恶意个人则可以很容易地连接到支付卡环境并威胁账户信息。
1.3 **禁止**在互联网和**持卡人数据环境**中的任何系统组件之间进行直接公共访问	防火墙的目的是管理和控制公共系统和内部系统（尤其是存储持卡人数据的系统）之间的所有连接。如果允许在公共系统和存储持卡人数据的系统之间直接访问，则会绕过防火墙提供的保护，并且存储持卡人数据的系统组件可能会面临威胁。
1.3.1 实施 DMZ 以只限制那些持卡人数据环境需要的协议的进出流量。	这些要求旨在防止恶意个人通过未授权的 IP 地址或以未授权的方式（例如，从您的网络内部将获取的数据发送至外部未受信任网络中的未受信任服务器）利用服务、协议或端口访问公司网络。
1.3.2 限制进入 DMZ 内部 IP 地址的互联网流量	
1.3.3 不允许互联网和持卡人数据环境之间进出流量的任何直接路由	DMZ 是防火墙的一部分，它面对公共互联网并管理互联网和公司需要用于连接公共网络的内部服务（如网络服务器）之间的连接。将需要与内部网络通信的流量和不需要通信的流量隔离开来是进行防御的第一道防线。

要求	指导说明
1.3.4 不允许从互联网至 DMZ 的内部地址通过	包通常包含原先发送包的计算机 IP 地址。这就使得网络中的其他计算机知道包从何而来。在某些情况下，这一发送的 IP 地址会被恶意个人假冒利用。 例如，恶意个人使用假冒的地址发送包，以便（除非您的防火墙禁止）包可以从互联网进入您的网络，看上去好像是内部流量从而冒充合法流量。一旦恶意个人进入您的网络，则可以开始威胁您的系统。 输入过滤是一种您可以用在防火墙上过滤进入网络的包的技术，以确保不会“假冒”从您自己的内部网络发送包（含于其他内容中）。 有关包过滤的更多信息，请参考称为“输出过滤”的配套技术方面的信息。
1.3.5 限制从持卡人数据环境至互联网的出站流量，以便出站流量只能访问 DMZ 内部的 IP 地址	DMZ 也应该评估从网络内部输出的所有流量，以确保所有出站流量遵循已建立的规则。为了 DMZ 有效地实现这一功能，应该禁止从网络内部至网络外任何地址的连接，除非这些连接先通过 DMZ 并由 DMZ 评估为合法。
1.3.6 实施状态检测，也即动态包过滤（也就是只有“建立”的连接才允许进入网络。）	执行状态包检测的防火墙会针对每个至防火墙的连接保持“状态”。通过保持“状态”，防火墙能知晓貌似对前一连接的回应是真的回应（因为它“记住”了前一连接）还是恶意个人或软件试图假冒或欺骗防火墙以便允许该连接。
1.3.7 在内部网络区域（从 DMZ 隔离开来）中使用数据库	持卡人数据需要最高级别的信息保护。如果持卡人数据位于 DMZ 中，由于该区域需要穿透的层更少，因此外部攻击者更容易访问这一信息。
1.3.8 实施 IP 伪装以防止内部地址被转译和发布到互联网上，使用 RFC 1918 地址空间。使用网络地址转译 (NAT) 技术，例如端口地址转译 (PAT)。	由防火墙管理的 IP 伪装允许公司有只能在网络内看见的内部地址和可以在外部看见的外部地址。如果防火墙没有“隐藏”或掩盖内部网络的 IP 地址，恶意个人则可以发现内部 IP 地址并试图用假冒的 IP 地址访问网络。
1.4 通过至互联网的直接连接在任何移动和/或员工自有计算机（例如员工使用的笔记本电脑）上安装个人防火墙软件，用于访问公司网络	如果计算机没有安装防火墙或杀毒程序，间谍软件、木马、病毒、蠕虫和黑客软件（流氓软件）则可能在不知情的情况下下载和/或安装。如果直接连接至互联网并且没有受公司防火墙保护，计算机甚至更容易受到攻击。未受公司防火墙保护时下载至计算机的流氓软件随后可在计算机重新连接至公司网络时，恶意地针对网络内的信息进行攻击。

要求 2：系统密码和其他安全参数不使用供应商提供的默认设置

恶意个人（公司外部和内部）通常使用供应商默认密码和其他供应商默认设置来危害系统。这些密码和设置为黑客集体所熟知，并且容易通过公开信息判断得出。

要求		指导说明
2.1	在网络上安装系统**以前**，务必更改供应商提供的默认项，例如包括密码、简单网络管理协议 (SNMP) 机构字串，并删除不必要的账户。	恶意个人（公司外部和内部）通常使用供应商默认设置、账户名和密码来危害系统。**这些**设置为黑客集体所熟知，并使您的系统极易受到攻击。
2.1.1	**对于**连接到持卡人数据环境或传输持卡人数据的**无线环境**，更改无线供应商默认项，包括但不局限于默认无线加密密钥、密码和 SNMP 机构字串。确保无线设备安全设置已启用，采用了严格的加密技术进行验证和传输。	许多用户未经管理层批准就安装这些设备，并且不更改默认设置或配置安全设置。如果无线网络没有实行足够的安全配置（包括更改默认设置），无线嗅探器则可以窃听网络流量、轻易捕获数据和密码、轻易进入网络并实施攻击。此外，802.11x 加密 (WEP) 密钥交换协议的较旧版本已被破解，从而致使加密无效。请确认已升级了设备上的固件以支持更为安全的协议，如 WPA/WPA2。
2.2	制定所有系统组件的配置标准。确保这些标准解决了所有已知的安全漏洞，并且符合行业接受的系统安全标准。	许多操作系统、数据库和企业应用程序都存在已知漏洞，也具有已知方法配置这些系统来修复安全漏洞。为了帮助那些并非安全专家的用户，安全公司已制定系统安全建议，对如何修正这些漏洞给出建议。如果系统存在这些漏洞，例如薄弱的文件设置或默认服务和协议（针对通常并不需要的服务或协议），攻击者将能够使用多种已知威胁来攻击有漏洞的服务和协议，从而访问您公司的网络。请访问以下三个网站示例，了解有关帮助您实施配置标准的行业最优方法的相关信息：www.nist.gov、www.sans.org 和 www.cisecurity.org。
2.2.1	每台服务器只执行一项主要功能。	这项要求旨在确保您公司的系统配置标准和相关流程满足需要有不同安全级别或可能会对同一台服务器上的其他功能引入安全漏洞的服务器功能。例如： 1. 需要部署严格安全措施的数据库如果与需要开放并直接面向互联网的网络应用程序共享一台服务器，则可能存在风险。 2. 未能对看似微小的功能应用补丁可能导致同一台服务器上的其他更重要的功能（如数据库）受到威胁。 这项要求主要针对服务器（通常基于 Unix、Linux 或 Windows）而不是主机系统。

要求		指导说明
	2.2.2 禁用所有不必要和不安全的服务和协议（*不直接需要用来执行设备特定功能的服务和协议*）。	如 1.1.7 所述，企业需要（或在默认情况下已启用）的许多协议常常被恶意个人用来威胁网络。要确保这些服务和协议在部署新服务器时始终被禁用，您的公司应该将这项要求纳入公司配置标准和相关流程。
	2.2.3 配置系统安全参数以防止滥用。	这项要求旨在确保您公司的系统配置标准和相关流程能具体解决存在已知安全隐患的安全设置和参数。
	2.2.4 删除所有不必要的功能，例如脚本、驱动程序、功能、子系统、文件系统和不必要的网络服务器。	服务器安全标准必须包括解决存在特定安全隐患的不必要功能的流程（例如，如果服务器不执行这些功能，则删除/禁用 FTP 或网络服务器）。
2.3	对所有非控制台管理访问进行加密。对于基于网络的管理和其他非控制台管理访问使用诸如 SSH、VPN 或 SSL/TLS 等技术。	如果没有对远程管理使用安全验证和加密通信，敏感的管理信息或操作层信息（如管理员密码）则可能暴露给窃听程序。恶意个人则可能使用这一信息访问网络、成为管理员并盗窃数据。
2.4	共享托管提供商必须保护每个机构的托管环境和数据。这些提供商必须满足*“附录 A：针对共享托管提供商的额外 PCI DSS 要求”*。	这项要求针对为同一台服务器上的多个客户端提供共享托管环境的托管提供商。当所有数据位于同一台服务器上并受单一环境的控制，这些共享服务器上的设置通常不能由单个客户端进行管理，也不允许客户端增加影响所有其他客户端环境安全的不安全功能和脚本，否则将使得恶意个人易于威胁某个客户端的数据并访问所有其他客户端的数据。请参阅附录 A。

要求 3 和要求 4 指南： 保护持卡人数据

要求 3：保护存储的持卡人数据

保护方法（例如加密、截词、掩模和散列等）是持卡人数据保护的关键组件。如果入侵者规避了其他网络安全控制并访问了加密数据，若没有正确的加密密钥，则仍不能读取并使用这些数据。也可考虑使用其他保护存储数据的有效方法来减小潜在风险。例如，最小化风险的方法包括除非绝对必要否则不存储持卡人数据，不需要完全的 PAN 时截断持卡人数据，以及不在未加密的邮件中发送 PAN。

请参阅 PCI DSS 与 PA-DSS 术语、缩略语关于“强效加密法”和其他 PCI DSS 词汇的定义。

要求		指导说明
3.1	使持卡人数据存储最小化。制定数据保留和处理政策。根据业务、法律和/或法规要求限制存储的大小和保留时间，如数据保留政策中所记录。	超过业务需求的持卡人数据扩展存储会形成不必要的风险。唯一需要存储的持卡人数据是主账户或 PAN（设为不可读）、失效期、姓名和业务代码。**请记住，如果不需要，就不要存储！**
3.2	不在授权后存储敏感的验证数据（即使已经加密）。 敏感验证数据包括下文要求 3.2.1 至 3.2.3 中列举的数据：	敏感验证数据包括磁条（或磁道）数据[7]、卡验证值或代码[8] 和 PIN 数据[9]。**严禁在授权后存储敏感验证数据！**此类数据对于恶意个人非常有用，因为它使得这些人可以伪造支付卡并创建欺诈交易。请参阅 *PCI DSS 与 PA-DSS 术语、缩略语*，查看“敏感验证数据”的完整定义。

[7] 编译在磁条中的数据，用于实卡交易中的授权。此数据还可以在芯片上的磁条图形中或卡的其他位置找到。交易授权之后，机构可能不会保留完整的磁条数据。可以被保留下来的磁道数据元素只能包括主账号、持卡人姓名、失效期与业务代码。

[8] 印在支付卡签名方格内或右侧或者印在支付卡面上的三或四位数值，用于验证无实卡交易。

9 由持卡人在实卡交易时输入的个人识别码和/或出现在交易信息中的经加密的 PIN 数据块。

要求		指导说明
3.2.1	不要存储磁条任意磁道上的完整内容（位于卡的背面、芯片上或其他位置）。该数据也可称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。 *注：在正常的业务过程中，以下磁条数据元素可能需要保留：* ▪ *持卡人姓名，* ▪ *主账户 (PAN)，* ▪ *失效期，以及* ▪ *业务代码* *为将风险降至最低，只存储业务所需的数据元素。* *注：有关更多信息*，请参阅 PCI DSS 与 PA-DSS 术语、缩略语。	如果存储了全磁道数据，获取该数据的恶意个人则可以在全世界复制并销售支付卡。
3.2.2	不要存储用于验证无实卡交易的卡验证代码或值（印在支付卡正面或背面的三或四位数字） *注：有关更多信息*，请参阅 PCI DSS 与 PA-DSS 术语、缩略语。	卡验证代码的目的是保护“无实卡”交易，即互联网或邮件订购/电话订购 (MO/TO) 交易，在这些交易中消费者和卡都不存在。因为卡的所有者持有卡并能够读取值，所以这些类型的交易可仅仅通过要求此卡的验证代码就确定来自卡的所有者。如果这一禁止存储的数据被存储并且随后被盗，恶意个人则可以执行互联网和 MO/TO 欺诈交易。
3.2.3	不要存储个人识别码 (PIN) 或经加密的 PIN 数据块。	只有卡的所有者或者发卡行应该知道这些值。如果这一禁止存储的数据被存储并且随后被盗，恶意个人则可以执行基于 PIN 的借方欺诈交易（例如，ATM 提款）。

要求		指导说明
3.3	显示 PAN 时对其进行适当掩盖（最多可显示的数位包括前六位与后四位）。 *注：* ▪ *此要求不适用于那些因特定需求要查看完整的 PAN 的员工和其他方；* ▪ *此要求不取代为显示持卡人数据而采用的更严格的要求，例如销售点 [POS] 收据。*	显示完整的 PAN 项目，如计算机屏幕、支付卡收据、传真或纸质报告，可能导致此类数据被未授权的个人获取并欺诈利用。PAN 可以在“商户备份材料”收据上以完整格式显示，而纸质收据应遵守与电子备份材料相同的安全要求，并遵循 PCI 数据安全标准指南，尤其是与物理安全相关的要求 9。还可以对具有合法业务需求需查看完整 PAN 的人显示完整的 PAN。
3.4	通过以下方法尽量使 PAN 在存储的地方不可读（包括在便携式数字媒体、备份媒体、日志中的数据）：	缺少对 PAN 的保护使得恶意个人可查看或下载此类数据。存储在主存储（数据库或平面文件，如文本文件电子表格）以及非主存储（备份、审核日志、异常或故障排除日志）中的 PAN 必须全部受到保护。确保 PAN 通过加密、截词或散列设为不可读，可减少传输过程中备份磁带被盗或丢失所造成的损害。由于必须保留审核、故障排除或异常日志，您可以将日志中的 PAN 设为不可读（或者删除或掩盖）以防止日志中的数据泄露。请参阅 *PCI DSS 与 PA-DSS 术语、缩略语*关于“强效加密法”的定义。
	▪ 基于强效加密法的单向散列	基于强效加密法的单向散列函数（如 SHA-1）可用于使持卡人数据不可读。如果不需要检索原始号码，则适合使用散列函数（单向散列是不可撤消的）。
	▪ 截词	截词的目的是只存储 PAN 的一部分（不超过前六位与后四位）。这种方法与掩模不同，掩模会存储整个 PAN 但在显示时会遮盖 PAN（即，只有部分 PAN 显示在屏幕、报表、收据等上）。
	▪ 索引记号与索引簿（索引簿必须安全地存储）	索引记号与索引簿也可用来使持卡人数据不可读。索引记号是根据指定索引将 PAN 替换为不可预测的值的加密记号。一次性索引簿是随机生成的私有密钥只使用一次来加密消息的系统，该消息随后使用匹配的一次性索引簿和密钥进行解密。
	▪ 带有相关密钥管理流程和过程的强效加密法。	强效加密法（请参阅 *PCI DSS 与 PA-DSS 术语、缩略语*中的定义和密钥长度）的目的是根据经行业测试并认可的算法（非专有或“自行开发”的算法）进行加密。

要求		指导说明
	在账户信息中，最应实现不可读的就是 PAN。 *注：* ▪ *如果因为某些原因，公司不能使 PAN 不可读，请参阅“附录 B：补偿性控制”。* ▪ *“强效加密法”*在 PCI DSS 与 PA-DSS 术语、缩略语中进行了*定义*。	
	3.4.1 如使用了磁盘加密（而不是文件级或列级数据库加密），则对逻辑访问的管理必须独立于本地操作系统的访问控制机制（例如，不使用本地用户账户数据库）。解密密钥决不能与用户账户绑定。	这项要求的目的是解决磁盘加密实现持卡人数据不可读的可接受性。磁盘加密会加密存储在计算机批量存储中的数据，并在授权用户请求时自动解密信息。磁盘加密系统拦截操作系统的读写操作，并在不需要用户任何特殊操作的情况下执行相应的加密转换，而不在会话开始时提供密码或密码短语。根据磁盘加密的这些特征，磁盘加密方法如果要符合这项要求，则不能： 1) 直接关联到操作系统，或者 2) 解密密钥与用户账户关联。
3.5	保护用于加密持卡人数据以防泄露和滥用的加密密钥：	加密密钥必须得到严密保护，因为获得访问权限的人将能够解密数据。
	3.5.1 将对加密密钥的访问限制为尽可能少的必要保管人	有权访问加密密钥的人数应该非常少，通常只是承担密钥保管责任的少数人。
	3.5.2 将加密密钥以尽量少的形式安全存储在尽量少的地方	加密密钥必须安全地存储，通常使用密钥加密密钥进行加密并存储在非常少的地方。

要求		指导说明
3.6	全面记录并实施用于加密持卡人数据的加密密钥采用的所有密钥管理流程和过程，包括以下各项：	加密密钥的管理方式是加密解决方案持续安全的关键部分。良好的密钥管理流程，无论是手动流程还是作为加密产品一部分的自动流程，都应满足 3.6.1 至 3.6.8 所述的所有密钥要素。
3.6.1	强效加密密钥的生成	加密解决方案必须生成强效密钥，如 *PCI DSS 与 PA-DSS 术语、缩略语*的“强效加密法”中所定义。
3.6.2	安全的加密密钥分发	加密解决方案必须安全地分发密钥，即密钥不以明码的方式分发，并且只分发给 3.5.1 中确认的保管人。
3.6.3	安全的加密密钥存储	加密解决方案必须安全地存储密钥，即密钥不以明码的方式存储（使用密钥加密密钥对其进行加密）。
3.6.4	定期更改加密密钥 • 认为有必要并且由相关应用程序建议时更改（例如重新加密），首选自动 • 至少每年一次	如果由加密应用程序供应商提供，则按照供应商的任何流程或建议定期更改密钥。 每年更改加密密钥非常有必要，以尽可能降低有人获取加密密钥并解密数据的风险。
3.6.5	弃用或更改旧的或疑似泄露的加密密钥	不再使用或需要的旧密钥应该废除并销毁，以确保这些密钥不能再使用。如果旧密钥需要保留（以支持归档、加密数据等），则应该进行严密保护。（请参阅下文的 3.6.6。）加密解决方案还应允许执行和便于执行这一流程：替换已知受到威胁或怀疑受到威胁的密钥。
3.6.6	加密密钥双重控制的分开保管和建立	对密钥进行分开保管和双重控制的目的是消除一人访问整个密钥的可能性。这一控制措施通常适用于手动密钥加密系统，或者未通过加密产品实施密钥管理的环境。该类型的控制通常在硬件安全模块内实施。
3.6.7	防止加密密钥的未授权更改	加密解决方案不应允许或接受来自未授权来源或意外进程的替代密钥。
3.6.8	要求密钥保管人签署声明他们知道并接受密钥保管责任的文件	这一流程可确保个人承诺履行密钥保管的职务并了解自身的责任。

要求 4：在开放型的公共网络中对持卡人数据进行加密传输

在易于被恶意个人访问的网络中传输敏感信息时必须加密。配置不当的无线网络及旧有加密和验证协议的漏洞都可能继续成为恶意个人的攻击对象，他们利用这些漏洞获取对持卡人数据环境的特权访问。

要求		指导说明
4.1	使用强效加密法和安全协议（例如 SSL/TLS 或 IPSEC）以保护在开放型公共网络中传输敏感持卡人数据的安全。 *PCI DSS 范围内的开放型公共网络示例如：* ▪ *互联网，* ▪ *无线技术，* ▪ *移动通信的全球系统 (GSM) 和* ▪ *通用无线分组业务 (GPRS)。*	由于恶意个人在传输敏感信息时拦截和/或转换数据是非常容易和普遍的，因此在公共网络传输敏感信息时必须加密。安全套接层会对网页和进入网页的数据进行加密。使用 SSL 安全网站时，确保“https”是 URL 的一部分。 请注意 3.0 版以前的 SSL 版本包含攻击者可用于控制受影响系统的已记录的漏洞，如缓冲区溢出。
4.1.1	确保传输持卡人数据或连接到持卡人数据环境的无线网络使用了行业最优方法（例如 IEEE 802.11i）对验证和传输实施了强效加密。 ▪ *对于新的无线实施，自 2009 年 3 月 31 日起禁止实施 WEP。* ▪ *对于当前的无线实施，自 2010 年 6 月 30 日起禁止使用 WEP。*	恶意用户使用广泛提供的免费工具捕获无线通信。使用适当的加密措施可防止敏感信息在网络中被捕获和披露。对于只存储在有线网络中的持卡人数据，许多已知的威胁源自恶意用户通过不安全的无线网络获取了扩展的访问权限。 对持卡人数据的验证和传输采用强效加密是必需的，以防止恶意个人获得权限访问无线网络及网络中的数据或利用无线网络进入其他内部网络或获取数据。WEP 不使用强效加密。WEP 加密绝不能单独使用，原因是 WEP 密钥交换进程中的初始向量 (IV) 薄弱并缺少所需的密钥轮换而导致它存在漏洞。攻击者可使用免费的暴力破解工具穿透 WEP 加密。 当前的无线设备应该升级（例如，将访问点固件升级至 WPA）以支持强效加密。如果当前设备无法升级，则应购买新设备。 如果无线网络使用的是 WEP，则不应具有访问持卡人数据环境的权限。
4.2	切勿使用终端用户通讯技术（例如，电子邮件、即时通讯工具、聊天工具等）发送未加密的 PAN。	电子邮件、即时通讯工具和聊天工具在内部网络和公共网络中进行传送遍历时，很容易被包检测程序拦截信息。请勿使用这些通讯工具发送 PAN，除非它们能提供加密功能。

要求 5：使用并定期更新杀毒软件或程序

恶意软件（通常指“流氓软件”，包括病毒、蠕虫和木马）在许多业务认证的活动中进入网络，包括员工电子邮件和互联网使用、移动电脑和存储设备，从而导致系统漏洞被利用。必须在所有经常受流氓软件影响的系统上使用杀毒软件，防止受到当前和变种的恶意软件威胁。

要求		指导说明
5.1	在所有经常受恶意软件影响的系统上部署杀毒软件（特别是个人计算机和服务器上）。	对于相对安全的系统，也存在使用广泛发布的途径进行攻击的常量流，通常为“0 天”（在发现后一小时内发布并传播至整个网络）。如果不定期更新杀毒软件，这些新形式的恶意软件可攻击您的网络并使其瘫痪。 恶意软件可在不知情的情况下从互联网下载和/或安装，但在使用可移动存储设备（如 CD、DVD、USB 记忆棒和硬盘驱动器、数码照相机、个人数据助理 (PDA) 和其他外围设备）时计算机也很容易受到威胁。如果没有安装杀毒软件，这些计算机可能会成为进入您的网络的访问点，并且/或者在网络内恶意攻击信息。 尽管常受恶意软件影响的系统通常不包括主机和大多数 Unix 系统（请参见下文的详细信息），但所有机构都必须具备符合 PCI DSS 要求 6.2 的流程，以识别和解决新的安全漏洞并相应地更新他们的配置标准和流程。与机构所使用的操作系统相关的恶意软件趋势应该包括在对新安全漏洞的识别中，并且解决新趋势的方法应根据需要纳入公司的配置标准和保护机制。 通常，以下操作系统不常受到恶意软件的影响：主机和某些 Unix 服务器（如 AIX、Solaris 和 HP-Unix）。然而，恶意软件的行业趋势变化很快，每家公司都必须遵守要求 6.2 识别和解决新的安全漏洞并相应地更新他们的配置标准和流程。
	5.1.1 确保所有杀毒程序都能够监测、删除并防止所有已知类型的恶意软件的攻击。	防止**所有**类型和形式的恶意软件攻击非常重要。
5.2	确保所有杀毒机制都是最新并且在运行，而且能够生成审核日志。	如果杀毒软件没有当前的防病毒签名或者在网络或个人计算机上不处于活动状态，即使是最好的杀毒软件其有效性也会受到限制。审核日志提供监控病毒活动和杀毒反应的功能。

要求 6：开发、维护安全系统和应用程序

恶意个人使用安全漏洞获取对系统的特权访问。许多漏洞都能够通过供应商提供的安全补丁进行修复，必须由管理这些系统的机构安装。所有关键系统都必须具备最新发布的合适的软件补丁，以保护持卡人数据被恶意个人和恶意软件利用和破坏。

注：合适的软件补丁就是那些进行了充分评估和测试以确定这些补丁不与现有安全配置冲突的补丁。对于自行开发的应用程序，许多漏洞都可以通过使用标准系统开发程序和安全的编码技术避免。

要求		指导说明
6.1	确保所有系统组件和软件都安装了最新的供应商提供的安全补丁。在发布的一个月以内安装关键的安全补丁。 *注：机构可以考虑应用基于风险的方法来排定其补丁安装的优先级。例如，将关键的基础结构（例如，面向公众的设备、系统和数据库）优先于不那么重要的内部设备，以确保高优先级系统和设备在一个月内解决完，再在三个月内解决不那么重要的设备。*	对于相对安全的系统，也存在使用广泛发布的途径进行的大量攻击，通常为“0 天”（在该小时内发布）。若未尽可能快地在关键系统上实施最新的补丁，恶意个人则可以使用这些途径攻击网络并使其瘫痪。请考虑变更优先级，以便关键系统或正在遭受风险的系统上的关键安全补丁可以在 30 天内安装，而其他风险更低的变更在 2-3 个月内安装。
6.2	建立一个流程来识别新发现的安全漏洞（例如，订阅互联网上的免费警告服务）。根据 PCI DSS 要求 2.2 更新配置标准，以解决新的漏洞问题。	这项要求的目的是让公司针对新的漏洞随时更新，以便相应地保护公司网络并将新发现的相关漏洞纳入配置标准。
6.3	根据 PCI DSS（例如，安全的验证和登录）并基于行业最优方法开发软件应用程序，并将信息安全融入到整个软件开发生命周期中。这些程序必须包括以下各项：	如果未在软件开发的要求定义、设计、分析和测试阶段考虑安全问题，安全漏洞则会因疏忽或恶意引入生产环境。
	6.3.1 在部署前测试所有安全补丁、系统和软件配置变更 **6.3.1.1** 验证所有输入（防止跨站脚本、注入攻击、恶意文件执行等）。 **6.3.1.2** 验证正确的错误处理 **6.3.1.3** 验证安全加密存储 **6.3.1.4** 验证安全通信 **6.3.1.5** 验证正确的基于角色的访问控制 (RBAC)	确保所有安装和变更均按预期执行，并且没有任何意外、不需要或有害的功能。

要求		指导说明
6.3.2	分开开发/测试环境与生产环境	通常，开发和测试环境比生产环境更不安全。如果未充分隔开，生产环境和持卡人数据可能因漏洞或薄弱的内部流程而遭受风险。
6.3.3	开发/测试环境与生产环境中的职责分离	这项要求可尽可能减少访问生产环境和持卡人数据的人数，并有助于确保将访问限制在真正需要访问的人员上。
6.3.4	在测试或开发过程中不使用生产数据（真实的 PAN）	开发环境中的安全控制措施通常不那么严格。使用生产数据将给恶意个人提供未经授权访问生产数据（持卡人数据）的机会。
6.3.5	在生产系统启动前清除测试数据与账户	测试数据和账户应在启动应用程序前从生产代码中清除，因为这些项目可能会泄露有关应用程序运作的信息。拥有此类信息将易于对应用程序和相关持卡人数据造成威胁。
6.3.6	在启动应用程序或发布给用户以前，清除所有自定义应用程序账户、用户 ID 和密码	自定义应用程序账户、用户 ID 和密码应在启动应用程序前或发布给用户前从生产代码中清除，因为这些项目可能会泄露有关应用程序运作的信息。拥有此类信息将易于对应用程序和相关持卡人数据造成威胁。
6.3.7	在发布至生产或客户以前检查自定义代码，以识别所有潜在的编码漏洞 *注：代码检查的这项要求适用于所有自定义代码（包括内部和面向公众的代码），PCI DSS 要求 6.3 将它作为系统开发生命周期的部分进行要求。代码检查可以由有经验的内部人员进行。网络应用程序也受到更多控制（如果它们是面向公众的），以解决执行后不断产生的威胁和漏洞，如 PCI DSS 要求 6.6 所定义的。*	自定义代码中的安全漏洞常常被恶意个人利用，以获取对网络的访问权限并威胁持卡人数据。具有安全编码技术经验的人员应检查代码以识别漏洞。
6.4	跟踪对系统组件进行的所有更改的更改控制流程。该程序必须包括如下内容：	如果没有适当的软件更改控制措施，安全功能可能会被疏忽、有意忽略或设为不可运作，从而可能发生非常规处理事件或引入恶意代码。如果背景检查和系统访问控制的相关人事政策不充分，未受信任和未经培训的人员则可能毫无限制地访问软件代码，聘期结束的员工可能有机会威胁系统并且有可能检测不到未授权的操作。
6.4.1	影响记录	应记录更改所造成的影响，以便所有受影响方能够对任何处理变更进行相应计划。

要求		指导说明
	6.4.2 相关方管理层的签核意见。	管理层批准是指更改是合法的并且经过公司核准。
	6.4.3 对操作功能的测试	应执行完整的测试，以确保所有动作都是预期的、报表都是准确的并且所有可能的错误状态都已得到恰当应对等等。
	6.4.4 取消程序	针对每个更改都应该有取消程序，以防更改万一失败，取消程序可让系统恢复至先前状态。
6.5	所有网络应用程序的开发（内部的与外部的，并且包括对应用程序的网络管理访问）须基于安全编码指南，例如《*开放式网络应用程序安全项目指南*》。涵盖在软件开发过程中对常见编码漏洞的防护，包括以下各项： *注：6.5.1 至 6.5.10 中列举的漏洞都是 PCI DSS 1.2 版发布时 OWASP 指南中最新的。然而，如果 OWASP 指南有更新，则最新版本将用于这些要求。*	应用程序层风险很高，可能受到内部和外部的双重威胁。如果没有适当的安全措施，持卡人数据和其他机密的公司信息则可能泄露，致使公司、客户和公司声誉遭受损失。
	6.5.1 跨站脚本 (XSS)	所有参数在使用前都应进行验证。无论何时应用程序接收用户提供的数据并在没有验证或编译该内容前将其发送至网络浏览器，都有可能发生 XSS 攻击。XSS 允许攻击者在受害者的浏览器中执行脚本，这将可以劫持用户会话、使网站面目全非并有可能引入蠕虫等等。
	6.5.2 注入攻击，特别是 SQL 注入。同时还须考虑 LDAP、Xpath 等其他注入攻击。	验证输入以确保用户数据不能修改命令和查询的含义。注入攻击，特别是 SQL 攻击，在网络应用程序中非常普遍。当用户提供的数据作为命令或查询的一部分发送至解释器时，即发生注入。攻击者的恶意数据会欺骗解释器，使其执行不希望执行的命令或更改数据，并允许攻击者通过应用程序攻击网络内的组件，以启动攻击（如缓冲区溢出）或披露机密信息和服务器应用程序功能。这也是在启用了商务的网站上实施欺诈交易的一种常用方法。来自网络请求的信息应该先进行验证，然后再发送至网络应用程序，例如检查字母字符、字母和数字字符的组合等。
	6.5.3 恶意文件执行	验证输入以确保应用程序不会从用户那里接受意外的文件名或文件。易受远程文件包含 (RFI) 攻击的代码允许攻击者包含恶意代码和数据，从而发生破坏性攻击，如整个服务器受到威胁。恶意文件执行攻击会影响从用户那里接受文件名或文件的 PHP、XML 和任何框架。

要求		指导说明
6.5.4	不安全的直接对象引用	不要将内部对象引用暴露给用户。当开发人员将引用作为 URL 或形式参数暴露给内部执行对象，如文件、目录、数据库记录或密钥，即发生直接对象引用。攻击者可以利用这些引用在没有授权的情况下访问其他对象。
6.5.5	跨站请求伪造 (CSRF)	不要回复由浏览器自动提交的授权证书和令牌。CSRF 攻击会强制登录受害者的浏览器，发送验证前的请求至存在漏洞的网络应用程序，随后该应用程序强制受害者的浏览器执行有益于攻击者的恶意动作。CSRF 可以和它攻击的网络应用程序一样强大。
6.5.6	信息泄露与不正确的错误处理	不要通过错误消息或其他方式泄露信息。应用程序可能无意间泄露有关其配置和内部运作的信息，或者通过各种应用程序问题违反隐私。攻击者利用这一漏洞盗窃敏感数据或实施更为严重的攻击。此外，不正确的错误处理方式会提供有助于恶意个人威胁系统的信息。如果恶意个人能够创建网络应用程序不能正确处理的错误，则可以获取详细的系统信息、创建拒绝服务中断、导致安全措施发生故障或致使服务器崩溃。例如，消息“提供的密码错误”告诉他们所提供的用户 ID 是正确的，他们只应该将重点集中在密码上。请使用更为一般的错误消息，如“无法验证数据”。
6.5.7	失效的验证与会话管理	妥善验证用户，并保护账户证书与会话令牌。账户证书与会话令牌常常未得到妥善保护。攻击者威胁密码、密钥或会话令牌以假冒其他用户的身份。
6.5.8	非安全加密存储	防止加密攻击。应用程序极少正确使用加密功能来保护数据和证书。攻击者利用保护不利的数据实施身份盗窃和其他犯罪，如信用卡欺诈。
6.5.9	非安全通信	对所有已验证的敏感通信进行妥善加密。应用程序常常在必须加密以保护敏感通信的时候未加密网络流量。
6.5.10	未能限制 URL 访问	始终对所有的 URL 执行表示层和业务逻辑的访问控制。通常，应用程序只通过防止向未授权用户显示链接或 URL 来保护敏感功能。攻击者可以利用这一漏洞、通过直接访问这些 URL 进行访问并执行未授权操作。

要求		指导说明
6.6	对于面向公众的网络应用程序，经常解决新的威胁和漏洞，并确保保护这些应用程序不受到以下*任一*方法的攻击： ▪ 通过手动或自动应用程序漏洞安全评估工具或方法检查面向公众的网络应用程序，至少每年一次并在所有更改后进行检查 ▪ 在面向公众的网络应用程序前端安装网络应用程序防火墙	对面向公众的应用程序的攻击非常普遍并且经常得逞，并且能够通过较差的编码实践。这项要求要求检查应用程序或安装网络应用程序防火墙，旨在大大减少对面向公众的网络应用程序的威胁，这些威胁可导致持卡人数据泄露。 ▪ 可使用检查和/或扫描应用程序漏洞的手动或自动漏洞安全评估工具或方法来满足这项要求 ▪ 网络应用程序防火墙可过滤和阻止应用程序层的次要流量。配置得当的网络应用程序防火墙如果与基于网络的防火墙配合使用，可防止应用程序在编码或配置不当的情况下应用程序层受到攻击。 请参阅*“补充信息：要求 6.6 明确应用程序复审和网络应用程序防火墙”* (www.pcisecuritystandards.org)，了解更多信息。

要求 7、8 和要求 9 指南：　　执行严格的访问控制措施

要求 7：只有出于业务需求的人才能访问持卡人数据

为确保只有授权的人才能访问关键数据，必须采用系统和流程来限制根据需要知道和工作职责进行访问。“需要知道”是指当需要执行一项工作时需要授予的最少数据和权限。

要求	指导说明
7.1 将对系统组件和持卡人数据的访问限制为只有工作需要访问这些数据的人。访问限制必须包括以下项目： **7.1.1** 将特权用户 ID 的访问权限限制为执行工作职责要求的最小权限 **7.1.2** 根据个人工作划分和职能分配权限 **7.1.3** 要求管理层签署授权书以指明需要的权限 **7.1.4** 自动访问控制系统的实施	可访问持卡人数据的人越多，用户账户被恶意使用的风险也越大。将访问限制为只有具备正当业务理由访问这些数据的人可帮助公司防止因经验不足或恶意而误处理持卡人数据。仅根据执行工作所需的最少数据量和最小权限来授予访问权限，称为“需要知道”，而根据工作划分和职能为个人分配权限，称为“基于角色的访问控制”或 RBAC。公司应根据“需要知道”和使用“基于角色的访问控制”来创建清晰的数据访问控制政策和流程，以定义授予访问权限的方式和对象。
7.2 为多用户系统组件建立机制，根据用户需要知道的数据限制访问，并且设置为“禁止所有”，除非特别允许。此访问控制系统必须包含以下各项： *注：“需要知道”是指当需要执行一项工作时需要授予的最少数据和权限。* **7.2.1** 覆盖所有的系统组件 **7.2.2** 根据工作划分和职能为个人分配权限 **7.2.3** 默认的“禁止所有”设置	如果没有根据用户需要知道的数据限制访问的机制，则可能在不知情的情况下授予用户访问持卡人数据的权限。使用自动访问控制系统或机制对于管理多用户来说是至关重要的。这一系统应按照您公司的访问控制政策和流程（包括“需要知道”和“基于角色的访问控制”）来建立，应管理对所有系统组件的访问，并且应具有默认的“禁止所有”设置以确保不授予任何人访问权限，除非特别建立了授予此类访问权限的规则。

要求 8：为每位拥有计算机访问权限的用户分配唯一的 ID

为每位拥有访问权限的用户分配唯一的 ID 可确保每个人都能为其操作承担唯一责任。采用此责任制之后，只有获得授权的已知用户才能操作重要数据和系统，而且这种操作行为可以跟踪。

要求		指导说明
8.1	在**允许用户**访问系统组件或持卡人数据之前为所有用户分配唯一的 ID。	通过确保每位用户能够唯一识别，而不是几位员工共用一个 ID，公司可保持个人对行为负责并对每位员工保留有效的核查记录。这将有助于在误用或恶意企图出现时加快问题的解决和控制。
8.2	除分配唯一的 ID 之外，至少采用以下一种方法验证所有用户的身份： ▪ 密码或口令 ▪ 双因素验证（例如令牌设备、智能卡、生物测定技术或公共密钥）	除使用唯一的 ID 之外，这些验证项目也有助于保护用户的唯一 ID 免受威胁（因为试图制造威胁的人需要知道唯一 ID 和密码或其他验证项目）。
8.3	员工、管理员和第三方采用双因素验证以远程访问（从网络外进行网络级的访问）网络。使用远程拨入用户认证服务 (RADIUS)、带有令牌的终端访问控制器访问控制系统 (TACACS) 或带有个人证书的 VPN（基于 SSL/TLS 或 IPSEC）等技术。	双因素验证要求对高风险访问（比如从网络外进行访问）采用两种验证形式。为了更加安全，从安全性较低的网络访问安全性较高的网络时，例如从公司桌面（安全性较低）访问有持卡人数据的生产服务器/数据库（安全性高）时，您的公司也可以考虑使用双因素验证。
8.4	使用强效加密法使密码在所有系统组件中传输和存储时不可读（在 *PCI DSS 与 PA-DSS 术语、缩略语*中定义）。	许多网络设备和应用程序在网络中传输用户 ID 和未加密密码，并且/或者不加密存储密码。恶意个人可以使用“检测程序”轻易地拦截传输中的未加密或可读的用户 ID 和密码，或直接访问存储在文件中的用户 ID 和未加密密码，并用这些偷来的数据获取未授权的访问权限。
8.5	确保在所有系统组件上都对非消费者用户和管理员采用正确的用户身份验证和密码管理，具体如下：	恶意个人用来威胁系统的起初一个步骤是利用漏洞或不存在的密码，因此执行良好的用户验证和密码管理流程至关重要。
8.5.1	控制用户 ID、证书和其他识别对象的添加、删除和修改操作。	要确保添加到系统的所有用户都是有效和认可的用户，应该由一个具有特定权限的小组来管理和控制用户 ID 的添加、删除和修改操作。管理这些用户 ID 的权限应该只限于这个小组。
8.5.2	重置密码前确定用户身份。	许多恶意个人使用“社会工程”，如访问帮助桌面和作为合法用户进行操作，来更改密码以使用用户 ID。重设密码前请考虑使用只有正确用户能回答的“机密问题”来帮助管理员识别用户。确保妥善保护这些问题并且不进行共享。

要求		指导说明
8.5.3	为每位用户的初始密码设置唯一值，第一次使用后立即更改。	如果为每位新用户设置的是相同的密码，内部用户、以前的员工或恶意个人可能知道或容易发现这个密码，并用它来获取账户访问权限。
8.5.4	立即撤销任何已终止用户的访问权限。	如果员工已经离职，但仍能通过他们的用户账户访问网络，则可能发生对持卡人数据的不必要或恶意访问。这一访问可能来自以前的员工或利用旧账户和/或未使用账户的恶意用户。请考虑和 HR 共同实施员工聘期结束时立即通知的流程，以便快速撤消这一用户账户。
8.5.5	至少每 90 天撤除/停用一次非活动的用户账户。	非活动账户的存在使未授权用户有可能利用未使用过的账户访问持卡人数据。
8.5.6	仅在所需时段启用供应商用于远程维护的账户。	允许供应商（如 POS 供应商）为支持您的系统每周 7 天、每天 24 小时可访问您的网络会增加未授权访问的机会，这种访问可能来自供应商环境中的用户或发现并使用这一随时可用的外部入口进入网络的恶意个人。另请参阅 12.3.8 和 12.3.9 了解关于该主题的更多信息。
8.5.7	向拥有访问持卡人数据权限的所有用户通报密码程序和政策。	向所有用户通报密码程序可以帮助他们了解和遵守政策，警惕企图利用他们的密码访问持卡人数据的恶意个人（例如，通过给员工打电话询问密码以便来电者可以“解决问题”）。
8.5.8	不要使用组、共享或常规账户和密码。	如果多位用户共享一个账户和密码，就不可能针对个人行为指定责任或有效记录个人行为，因为特定行为可能是由共享账户和密码的小组中的任何人实施。
8.5.9	至少每 90 天更改一次用户密码。	强效密码是网络防御的第一道防线，因为恶意个人常常试图先找到有漏洞或不存在密码的账户。如果密码较短、容易猜出或不加更改长期使用，恶意个人就有更多机会找到这些薄弱的账户，并伪装有效的用户 ID 威胁网络。通过启用操作系统（如 Windows）、网络、数据库和其他平台随附的密码和账户安全功能，可以根据这些要求来执行和维护强效密码。
8.5.10	密码必须至少有七个字符长。	
8.5.11	使用包含数字和字母字符的密码。	
8.5.12	不允许个人提交和前四次使用过的任何密码相同的新密码。	
8.5.13	用户尝试次数达到六次后锁定该用户 ID，以限制尝试反复访问。	如果没有账户锁定机制，攻击者可以通过手动或自动工具（如密码破解）持续尝试猜测密码，直到成功获取用户账户的访问权限。

要求		指导说明
8.5.14	将锁定时长设置为至少 30 分钟或直到管理员启用用户 ID 为止。	如果账户因为某人持续尝试猜测密码而被锁定，延缓重新激活锁定账户的控制措施可以阻止恶意个人持续猜测密码（他们必须至少停止 30 分钟直到账户重新激活）。此外，如果必须请求才能重新激活账户，管理员或帮助桌面可以验证账户所有者是锁定的引发者（因输入错误）。
8.5.15	如果会话保持空闲状态超过 15 分钟，则需要用户重新输入密码以重新激活终端。	当用户离开可以访问重要网络或持卡人数据的公共计算机时，其他人可能在用户离开的情况下使用这台计算机，从而导致账户的未授权访问和误用。
8.5.16	验证访问任何数据库（其中包括持卡人数据）的所有操作。这包括应用程序、管理员和所有其他用户的访问操作。	如果没有访问数据库和应用程序的用户验证，未授权或恶意访问的可能性就会增加，并且由于用户未经验证因而不被系统知晓，此类访问也无法记录下来。此外，应该只通过程序化方法（例如，已存储的程序）授予数据库访问权限，而不是由最终用户直接访问数据库（DBA 除外，他们为了管理可以直接访问数据库）。

要求 9：限制对持卡人数据的物理访问

任何物理访问数据或存储持卡人数据的系统的操作都会为个人提供访问设备或数据从而删除系统或硬拷贝的机会，这种行为应适当限制。

要求		指导说明
9.1	使用适当的机构入口控制，以在持卡人数据环境中限制和监控系统的物理访问。	如果没有物理访问控制，未授权人员则有可能进入建筑物并访问敏感信息、更改系统配置、将漏洞引入网络或者毁坏或盗窃设备。
9.1.1	使用摄像头或其他访问控制机制，以监控个人对敏感区域的物理访问。检查收集的数据并与其他入口相关联。至少保存三个月，法律另有规定的除外。 *注：“敏感区域”指的是任何数据中心、服务器室或任何放置存储持卡人数据的系统的区域。它不包括仅存在销售点终端的区域（例如零售店的收银区域）。*	当调查物理漏洞时，这些控制措施有助于识别对这些存储持卡人数据的区域进行物理访问的个人。
9.1.2	限制对公共网络插座交换机的物理访问。	限制对网络插座交换机的访问可以阻止恶意个人插入容易获得的网络插座交换机，使他们可以访问内部网络资源。不使用时请考虑关闭网络插座交换机，只在需要时重新激活。在公共区域（如会议室）建立允许供应商和访客只访问互联网的专用网络，这样他们就不会进入您的内部网络。
9.1.3	限制对无线访问点、网关和手持式设备的物理访问。	如果访问无线组件和设备不能确保安全，恶意用户就可以使用您公司无人值守的无线设备访问您的网络资源，甚至将他们的设备与您的无线网络连接，以便不经授权进行访问。请考虑在安全存储区设置无线访问点和网关，比如在带锁的房间或服务器室。确保启用了强效加密法。对无线手持式设备启用长时间空闲后自动锁定设备的功能，并将设备设置成开机时要求输入密码。
9.2	制订相关程序，以帮助所有人员迅速区分员工和访客，尤其是在可以访问持卡人数据的区域。 *为明确这一要求，“员工”指的是全职和兼职员工、临时员工以及“常驻”在机构的承包商和顾问。“访客”指的是供应商、员工的客人、服务人员或需要进入机构作短暂停留（一般不超过一天）的任何人。*	如果没有工卡系统和门控措施，未授权和恶意用户则可以很容易地访问您的机构，盗窃、禁用、中断或破坏重要系统和持卡人数据。要获得最佳控制，请考虑在包含持卡人数据的工作区内外实施工卡或卡访问系统。

要求		指导说明
9.3	确保遵循以下程序对待所有访客：	访客控制对于防止未授权和恶意个人访问您的机构（并潜在访问持卡人数据）非常重要。
	9.3.1 进入处理或维护持卡人数据的区域之前，必须获得授权。 **9.3.2** 提供可以将访客识别为非员工而且使用后会过期的物理令牌（例如工卡或访问设备）。 **9.3.3** 要求访客在离开机构之前或在失效期交出物理令牌。	访客控制对确保访客只进入授权进入的区域来说非常重要，这样员工能将他们识别为访客并监控他们的活动，他们的访问也被限制在合法的访问时段。
9.4	使用访客日志，以保持访客活动的实体核查记录。在日志上记录访客姓名、所属公司以及授权访客进行物理访问的员工。将该日志至少保存三个月，法律另有规定的除外。	记录最少量访客信息的访客日志容易维护且维护费不高，并且在调查潜在数据漏洞时，有助于识别对建筑物或房间的物理访问和对持卡人数据的潜在访问。请考虑在机构入口，特别是进入存有持卡人数据的区域入口执行日志记录。
9.5	将媒介备份存放在安全的地方，最好存放在机构之外的场所，例如替代或备份场所或商业性的存储机构。至少每年检查一次该场所的安全性。	如果存放在不安全的场所，包含持卡人数据的备份可能因恶意目的而容易丢失、被盗或复制。要确保安全存储，请考虑联系商业性的数据存储公司；对于较小的机构，则可以考虑使用银行的保险箱。
9.6	采用物理方式保护包含持卡人数据的所有纸质媒介和电子媒介。	如果存储在便携式媒介中、打印或留在某人桌上时未受保护，持卡人数据易受未授权查看、复制或扫描的威胁。对于分发给内部和/或外部用户的媒介中的持卡人数据，请考虑保护程序和流程。如果没有此类程序，数据容易丢失、被盗和被用于欺诈性目的。
9.7	始终严格控制在内部或外部分发任何类型的包含持卡人数据的媒介，包括以下内容：	
	9.7.1 将媒介分类，以便将其标识为机密。	未标识为机密的媒介可能不会受到所需程度的保护，并且可能丢失或被盗。请在程序中纳入上述要求 9.6 中建议的媒介分类流程。
	9.7.2 使用安全的快递服务或其他可准确跟踪的传送方式寄送媒介。	如果使用不能跟踪的方式（如普通邮局邮件）寄送，媒介可能丢失或被盗。使用安全的快递服务寄送包含持卡人数据的媒介，这样您可以使用他们的跟踪系统保留清单和运输地点。

要求		指导说明
9.8	将任何和所有包含持卡人数据的媒介从安全区域转移时（尤其是当媒介发放给个人时），务必确保管理层已同意。	持卡人数据不经管理层批准流程而离开安全区域，可能导致丢失或被盗。没有公司流程则无法追踪媒介位置，也就没有针对数据去向或保护方式而制定的流程。请在程序中纳入上述要求 9.6 建议的针对移动媒体制定的管理层批准流程。
9.9	始终严格控制对媒介（其中包含持卡人数据）的存储和访问操作。	如果没有细致的盘存方法和存储控制，被盗或丢失的媒介可能会被无限期地忽略。请在程序中纳入上述要求 9.6 建议的流程，限制访问含有持卡人数据的媒介。
9.9.1	正确保存所有媒介的盘存记录，媒介至少每年盘存一次。	如果不盘存媒介，被盗或丢失的媒介可能会长时间被忽略。请在程序中纳入上述要求 9.6 建议的针对媒介盘存和安全存储而制定的流程。
9.10	包含持卡人数据的媒介由于业务原因或法律原因不再需要时应予以销毁，具体如下：	如果不采取措施销毁包含在 PC 硬盘、CD 和纸上的信息，对这类信息的处理可能会导致威胁和财务或声誉损失。例如，恶意个人可能使用称为“垃圾搜寻”的技术搜索垃圾筒和回收站，并使用找到的信息发动攻击。请在程序中纳入上述要求 9.6 建议的流程，正确销毁含有持卡人数据的媒介，包括在销毁前妥善存放这类媒介。
9.10.1	对硬拷贝材料进行粉碎、焚烧或打浆，让持卡人数据无法复原。	
9.10.2	使电子媒介上的持卡人数据不可恢复，确保持卡人数据不可复原。	

要求 10：跟踪和监控访问网络资源和持卡人数据的所有操作

记录机制和跟踪用户活动的功能对于预防、检测和消除数据泄漏的不良影响至关重要。在所有环境中使用日志可在出现问题时详细地跟踪、发出警报并进行分析。如果没有系统活动日志，确定威胁原因将会非常困难。

要求		指导说明
10.1	为每个个人用户建立一个可链接访问所有系统组件（尤其是具有根权限等管理权限的访问）的流程。	对用户（特别是具有管理权限的用户）来说，拥有可将用户访问链接至被访问系统组件的流程或系统至关重要。该系统生成审核日志并提供追踪特定用户可疑活动的功能。事故后取证团队很大程度上依赖于这些日志展开调查。
10.2	针对所有系统组件实施自动核查记录，以重建以下事件： **10.2.1** 对持卡人数据的所有个人访问 **10.2.2** 具有根权限或管理权限的任何个人实施的所有操作 **10.2.3** 访问所有核查记录 **10.2.4** 无效的逻辑访问尝试 **10.2.5** 识别和验证机制的使用 **10.2.6** 初始化审核日志 **10.2.7** 创建和删除系统级对象	网络中的恶意个人通常会对目标系统尝试多次访问。生成可疑活动核查记录可提醒系统管理员，将数据发送至其他监控机制（如入侵检测系统），并为事故后跟进提供历史记录。
10.3	针对每个事件的所有系统组件至少记录以下核查记录条目： **10.3.1** 用户身份 **10.3.2** 事件类型 **10.3.3** 日期和时间 **10.3.4** 成功指示或失败指示 **10.3.5** 事件起源 **10.3.6** 受损数据、系统组件或资源的特征或名称	通过在 10.2 中记录这些可核查事件条目，可以迅速识别潜在的威胁，并了解人物、事件、时间、地点和方式等详细情况。

要求		指导说明
10.4	同步所有重要的系统时钟和时间。	如果恶意个人进入了网络，他们通常会尝试在审核日志中更改他们的活动的时间戳，以防止检测到他们的活动。对事故后取证团队来说，每个活动的时间在确定系统如何受到威胁的过程中十分关键。如果访问限制不当，恶意个人也可能尝试直接更改时间服务器上的时钟，把时间重设为他进入网络之前的时间。
10.5	保护核查记录，以避免篡改。	进入网络的恶意个人通常会尝试编辑审核日志来隐藏他们的活动。如果没有对审核日志进行足够的保护，则无法保证日志的完整性和准确性，审核日志可能在威胁出现后作为调查工具时毫无用处。
	10.5.1 仅限有工作需要的人员查看核查记录。 **10.5.2** 保护核查记录文件，防止未经授权的修改操作。 **10.5.3** 将核查记录文件迅速备份到不易篡改的中心日志服务器或媒介。 **10.5.4** 将外部式技术的日志写入外部 LAN 上的日志服务器。	对审核日志的足够保护包括强效访问控制（仅根据“需要知道”限制访问日志）和使用内部隔离（使日志更难以被发现和修改）。通过记录外部式技术（如无线、防火墙、DNS 和邮件服务器）的日志，可以降低日志丢失或被篡改的风险，原因是日志位于内部网络中而更加安全。
	10.5.5 针对日志使用文件完整性监控软件和更改检测软件，以确保现有的日志数据在不生成警报的情况下不会更改（尽管添加新数据不会引发警报）。	文件完整性监控系统检查对重要文件的更改，并在发现更改时进行通知。针对文件完整性监控目的，机构通常监控不会定期更改、一旦更改则表示可能受到威胁的文件。针对日志文件（确实频繁更改），应该监控的项目有日志文件被删除的时间、日志突然增大或缩小，以及恶意个人已篡改日志文件的任何其他迹象。可以使用现货供应和开放资源工具监控文件完整性。
10.6	每天至少检查一次所有系统组件的日志。日志检查必须包括检查执行入侵检测系统 (IDS) 和验证、授权等安全功能的服务器以及记账协议 (AAA) 服务器（例如 RADIUS）。 *注：可根据要求 10.6 中的规定，使用日志收集工具、分析工具和报警工具*	许多漏洞在检测到的几天或几个月前就已出现。每天检查一次日志可以缩短潜在漏洞存在和暴露的时间。日志检查流程无须手动操作。特别是对拥有大量服务器的机构，应考虑使用日志收集工具、分析工具和报警工具。

要求		指导说明
10.7	核查历史记录至少保留一年，至少可以立即准备（例如在线、已归档或从备份中恢复）三个月的历史记录以供分析。	由于注意到威胁已经发生或正在发生需要一段时间，因此日志至少应保留一年，以便允许调查者有足够的日志历史记录来更好地确定潜在漏洞存在的时间和受到影响的潜在系统。通过立即准备三个月的日志，机构可以迅速地确定并减少数据漏洞的影响。不在现场存放备份磁带将需要更长的时间来恢复数据、执行分析和确定受影响的系统或数据。

要求 11：定期测试安全系统和流程

恶意个人和研究者总是可以不断发现漏洞，一些新软件也可以引发漏洞。因此应经常测试系统组件、流程和自定义软件，以确保根据不断变化的环境持续实施安全控制。

要求	指导说明
11.1 至少每季度使用一次无线分析仪或部署可识别所有在用无线设备的无线 IDS/IPS，以测试无线访问点是否存在。	在网络中实施和/或运用无线技术是恶意个人访问网络和持卡人数据的最常见途径。如果无线设备或网络在没有得到公司许可的情况下安装，恶意个人则可以轻易“隐身”进入网络。除了无线分析仪，也可以使用端口扫描仪和其他检测无线设备的网络工具。 因为无线访问点可以很容易地连接到网络、很难检测到它们的存在以及未授权无线设备所带来的风险不断增加，所以即使有政策禁止使用无线技术，也必须执行这些扫描。 作为事故反应计划的一部分，公司应该有一旦检测到未授权无线访问点后可执行的记录程序。无线 IDS/IPS 应该设置成自动生成警报，但如果手动无线扫描时检测到未授权设备，该计划也必须记录反应程序。
11.2 至少每季度以及在网络有任何重大变动后（例如安装新的系统组件、更改网络拓扑、修改防火墙规则、产品更新）运行一次内部和外部网络漏洞扫描。 *注：每季度一次的外部漏洞扫描必须由支付卡行业安全标准委员会 (PCI SSC) 认证的授权扫描供应商 (ASV) 执行。网络变动后的扫描工作可由公司内部员工执行。*	漏洞扫描是针对外部和内部网络设备和服务器运行的自动工具，旨在暴露潜在漏洞和识别网络中可被恶意个人发现和利用的端口。一旦这些漏洞得以识别，机构应予以纠正，然后重复扫描以证实漏洞已被纠正。 在机构首次进行 PCI DSS 评估时，四次季度扫描都尚未执行是有可能的。如果最近一次扫描的结果符合扫描通过标准，并且落实了针对以后的季度进行扫描的政策和程序，即达到了这项要求的目的。如果这些条件都满足，则没有必要因缺少四次扫描而推迟针对这项要求的“到位”评估。
11.3 外部和内部穿透测试每年至少执行一次，基础架构或应用程序有任何重大升级或修改后（例如操作系统升级、环境中添加子网络或环境中添加网络服务器）也应执行。此类穿透测试必须包括以下内容： **11.3.1** 网络层穿透测试 **11.3.2** 应用程序层穿透测试	网络和应用程序穿透测试与漏洞扫描的不同之处在于，穿透测试通常是手动的，尝试实际利用扫描中识别出的漏洞，并且包括恶意个人使用的利用薄弱安全系统或流程的技术。 应用程序、网络设备和系统发布至生产环境前，应使用最佳安全方法使其更加安全（要求 2.2）。漏洞扫描和穿透测试可以暴露攻击者以后可发现和利用的任何剩余漏洞。

要求		指导说明
11.4	使用入侵检测系统和/或入侵防御系统，以监控持卡人数据环境中的所有流量并在发现可疑威胁时提醒员工。随时更新所有入侵检测引擎和入侵防御引擎。	这些工具使用数千种威胁类型（黑客工具、木马和其他流氓软件）的已知“签名”比较进入网络的流量，并在发生威胁尝试时发送警报和/或阻止威胁。如果没有通过这些工具检测未授权活动的主动方法，对计算机资源的攻击（或误用）无法即时发现。应该监控这些工具生成的安全警报，这样就可以阻止入侵企图。 现存的威胁类型有数千种，而且每天都会发现更多的类型。这些系统的旧版本没有当前“签名”，无法识别可能引起未检测到的破坏的新漏洞。这些产品的供应商提供频繁（通常每天一次）的更新。
11.5	部署文件完整性监控软件，如发现未经授权修改重要系统文件、配置文件或内容文件的操作将提醒员工；配置该软件，使其至少每周比较一次重要文件。 *注：对于文件完整性监控软件来说，重要文件通常是不经常更改的文件，但是修改此类文件会引发系统威胁或有可能造成威胁。文件完整性监控软件通常需要使用相关操作系统的重要文件进行预配置。其他的重要文件（例如自定义应用程序的文件）则必须由机构（即商户或服务提供商）来评估和定义。*	文件完整性监控 (FIM) 系统检查对重要文件的更改，并在检测到更改时进行通知。可以使用现货供应和开放资源工具监控文件完整性。如果执行不当并且 FIM 输出受到监控，恶意个人就可以更改配置文件内容、操作系统程序或应用程序可执行文件。如果未检测到此类未授权更改，则可能使当前的安全控制措施失效和/或导致持卡人数据被盗，而感觉不到它对正常流程的影响。

要求 12 指南：　维护信息安全政策

要求 12：维护针对员工和承包商信息安全的政策。

有效的安全政策不仅可以为整个公司设置安全基准，还可告知员工他们的职责。所有员工应了解数据的敏感性以及他们有保护数据的责任。为明确这一要求，“员工”指的是全职和兼职员工、临时员工以及“常驻”在公司的承包商和顾问。

要求		指导说明
12.1	建立、发布、维护和散发可实现以下标准的安全政策： **12.1.1** 处理所有 PCI DSS 要求。 **12.1.2** 包括可识别威胁和漏洞的年度流程并能生成正式的风险评估。 **12.1.3** 包括至少每年执行一次检查并在环境变动时予以更新。	公司的信息安全政策为执行安全措施保护最有价值的资产提供指南。有效的安全政策不仅可以为整个公司设置安全基准，还可告知员工他们的职责。所有员工应了解数据的敏感性以及他们有保护数据的责任。 安全威胁和保护方法全年都在迅速演变。如果未更新安全政策以反映这些变化，则没有制定新的保护措施来防御这些威胁。
12.2	根据此规格中的要求制订每日操作安全程序（例如用户帐户维护程序和日志查看程序）。	每日操作安全程序作为“桌面说明”供员工在日常系统管理和维护活动中使用。未记录的操作安全程序将使员工意识不到任务的全部范围，新员工不能很容易地重复流程，并且这些流程中存在的潜在差距可能使恶意个人能访问重要系统和资源。
12.3	针对面向员工的重要技术（例如远程访问技术、无线技术、可移动电子媒介、笔记本电脑、个人数据助理 (PDA)、电子邮件使用和因特网使用）制订使用政策，以定义所有员工和承包商正确使用这些技术的政策。确保此类使用政策要求以下内容：	员工使用政策可以禁止使用公司政策规定的某些设备和其他技术，或为员工提供正确使用和执行的指导。如果使用政策不到位，员工则可能使用违反公司政策的技术，从而使恶意个人能访问重要系统和持卡人数据。.一个例子是，在不知情的情况下安装没有安全措施的无线网络。要确保遵守公司标准和只实施获得批准的技术，请考虑将实施权限只限制在操作团队中，并且不允许非专业/普通员工安装这些技术。
	12.3.1 管理层的明确许可	如果实施这些技术不要求管理层的适当批准，员工可能会因业务需要简单地实施一个解决方案，但也为恶意个人打开了通向重要系统和数据的巨大漏洞。
	12.3.2 使用技术的验证	如果实施的技术未经过适当验证（用户 ID 和密码、令牌、VPN 等），恶意个人则可轻易使用这种未受保护的技术访问重要系统和持卡人数据。
	12.3.3 所有此类设备和获得访问权限的员工列表	恶意个人可能破坏物理安全并将他们自己的设备放置在网络中作为“后门”。

要求		指导说明
	12.3.4 给设备贴标签并注明所有者、联系信息和用途	员工也可能绕过程序安装设备。正确地给设备贴标签的确切清单可以快速识别未经批准的安装。请考虑为设备制定一个官方命名规范，并根据制定的清单控制给所有设备贴标签并进行记录。
	12.3.5 可接受的使用技术	通过定义公司批准的设备和技术的合理业务用途和位置，公司能够更好地管理和控制配置与操作控制之间的差距，确保没有为恶意个人打开访问重要系统和持卡人数据的“后门”。
	12.3.6 可接受的技术网络位置	
	12.3.7 公司许可的产品列表	
	12.3.8 非活动状态达到特定时限后自动中断远程访问技术的会话	远程访问技术常常是通向重要资源和持卡人数据的“后门”。通过未使用时中断远程访问技术（比如，POS 或其他供应商用来支持系统的技术），可减少对网络的访问和风险。请考虑使用控制措施在非活动状态持续 15 分钟后中断设备连接。请参阅要求 8.5.6 了解关于该主题的更多信息。
	12.3.9 仅在供应商需要时为其激活远程访问技术，并在使用后立即停用	
	12.3.10 通过远程访问技术访问持卡人数据时，禁止将持卡人数据复制、移动和存储到本地硬盘和可移动电子媒介。	要确保员工意识到自己有责任不将持卡人数据存储或复制到本地个人计算机或其他媒介，公司应该有明确禁止此类活动的政策。
12.4	确保安全政策和程序明确定义了所有员工和承包商的信息安全职责。	如果没有明确定义分配的安全角色和职责，与安全小组的合作将不协调，从而导致实施不安全的技术或使用过时或不安全的技术。
12.5	针对个人或团队分配以下信息安全管理职责： **12.5.1** 建立、记录和分配安全政策和程序。 **12.5.2** 监控、分析安全警报和安全信息并将其分配给相关人员。 **12.5.3** 创建、记录和分配安全事故响应程序和逐层上报程序，以确保及时有效地处理所有情况。 **12.5.4** 管理用户账户，包括添加、删除和修改 **12.5.5** 监控和控制所有的数据访问操作。	每个对信息安全管理负有责任的员工或团队应通过特定政策清楚地认识到自己的责任和相关任务。如果没有这一责任感，流程中的差距可能允许对重要资源或持卡人数据的访问。
12.6	实施正式的安全意识计划，使所有员工都能了解持卡人数据安全的重要性。	如果用户没有受过安全责任的培训，已经实施的安全防护措施和流程就可能因为员工的失误或有意行为而变得无效。
	12.6.1 员工一经雇用后立即培训，之后每年至少培训一次。	如果安全意识计划没有包括每年一次的复习课程，员工就可能忘记或忽略关键的安全流程和程序，从而导致重要资源和持卡人数据泄露。

要求		指导说明
	12.6.2 要求员工每年至少确认一次他们已阅读并了解了公司的安全政策和程序。	要求员工确认（例如，通过书面或电子形式确认）有助于确保他们已经阅读并了解了安全政策/程序，并且已承诺遵守这些政策。
12.7	雇用员工前筛选应征者（请参阅以上 9.2 中的“员工”定义），以尽量减少内部人员发起攻击的风险。 *对于门店收银员这样的员工，这一要求仅作建议，因为他们在交易时一次只能访问一个卡号。*	对于公司希望授予访问持卡人数据权限的员工，在雇用前进行彻底的背景调查，可以减少有可疑或犯罪背景的个人未经授权使用 PAN 和其他持卡人数据的风险。我们希望公司有背景审查的政策和流程，包括针对哪种背景审查结果会影响雇用决策（以及是什么样的影响）的自行决策流程。
12.8	如持卡人数据与服务提供商共享，应维护和实施管理服务提供商的政策和程序，以包括以下各项：	如果商户或服务提供商与另一服务提供商共享持卡人数据，那么适用于确保持续保护数据的某些要求将由此类服务提供商执行。
	12.8.1 保留服务提供商列表。	了解服务提供商有哪些可以确定风险扩展到公司外的哪些地方。
	12.8.2 要求服务提供商出具书面协议，由其确认对自己拥有的持卡人数据的安全性负责，并保留此协议。	服务提供商的确认书可以证明他们承诺维护从客户端获得的正确持卡人数据的安全性并为其负责。
	12.8.3 确保已建立了雇用服务提供商的流程（包括雇用前相应的尽职调查）。	该流程可以确保服务提供商的雇用经过公司内部的彻底审查，应包括与服务提供商建立正式关系前的风险分析。
	12.8.4 始终遵循计划，以监控服务提供商的 PCI DSS 遵从性状态。	了解服务提供商的 PCI DSS 遵从性状态可以进一步确保他们与公司遵从相同的要求。
12.9	实施事故响应计划。随时准备立即响应系统漏洞事故。	如果没有由负责方正确传播、解释和理解的全面的安全事故响应计划，混乱局面和缺乏统一的响应将使公司业务进一步停滞，并引起不必要的公共媒介曝光和新的法律责任。

要求		指导说明
12.9.1	创建事故响应计划，以便在发现系统漏洞时实施。确保计划至少可以处理以下各项： ▪ 发生漏洞时的角色、职责和沟通策略以及联系策略，至少包括通知支付品牌 ▪ 特定的事故响应程序 ▪ 业务恢复和业务连续性程序 ▪ 数据备份流程 ▪ 分析报告漏洞的法律要求 ▪ 所有重要系统组件的范围和响应 ▪ 参考或包括支付品牌的事故响应程序	事故响应计划应该全面并包含所有关键因素，以使您的公司在发生可能影响持卡人数据的破坏事件时能有效响应。
12.9.2	至少每年测试一次计划。	如果没有正确的测试，则可能漏掉在事故中限制泄露的关键步骤。
12.9.3	指定一天 24 小时、一周 7 天随时准备响应警报的特定人员。	如果没有经过培训和随时可用的事故响应团队，则可能造成更大的网络损坏，并且对目标系统的不当处理可能“污染”重要数据和系统。这会对成功进行事故后调查形成阻碍。如果内部资源不可用，请考虑联系提供这些服务的供应商。
12.9.4	向负责响应安全漏洞的员工提供相应培训。	
12.9.5	包括来自于入侵检测系统、入侵防御系统和文件完整性监控系统的警报。	这些监控系统旨在关注潜在的数据风险，对采取快速行动防止破坏来说至关重要，而且必须包括在事故响应流程中。
12.9.6	根据以往的经验教训、结合行业发展情况制订有关修改和改进事故响应计划的流程。	发生事故后将“经验教训”纳入事故响应计划中可以使计划保持最新状态，并能够对出现的威胁和安全趋势作出反应。

要求 A.1 指南：　针对共享主机提供商的额外 PCI DSS 要求

要求 A.1：共享主机提供商保护持卡人数据环境

根据要求 12.8 中的规定，所有可访问持卡人数据的服务提供商（包括共享主机提供商）必须遵守 PCI DSS。此外，要求 2.4 指出共享主机提供商必须保护每个机构的托管环境和数据。因此，共享主机提供商还必须额外遵守附录中的要求。

要求		指导说明
A.1	根据 A.1.1 至 A.1.4 的规定，保护每个机构（即商户、服务提供商或其他机构）的托管环境和数据： 主机提供商必须满足这些要求和 PCI DSS 中所有其他相关章节中的要求。 *注：即使主机提供商可能会满足这些要求，但使用主机的机构却不保证遵从性。每个机构必须遵守 PCI DSS 并证明其遵从性（如适用）。*	PCI DSS 附录 A 适用于希望向商户和/或服务提供商客户提供符合 PCI DSS 的托管环境的共享主机提供商。除了所有其他 PCI DSS 相关要求外，还应满足这些步骤。
A.1.1	确保每个机构运行的流程仅包括访问该机构的持卡人数据环境。	如果允许商户或服务提供商在共享服务器上运行自己的应用程序，则应该使用商户或服务提供商的用户 ID，而不是作为特权用户运行这些应用程序。特权用户可以象访问自己的持卡人数据环境一样访问所有其他商户和服务提供商的持卡人数据环境。
A.1.2	每个机构的访问权限和特权仅限访问他们自己的持卡人数据环境。	要确保将访问和特权限制在只有商户或服务提供商能访问自己的持卡人数据环境，请考虑以下几点：(1) 商户或服务提供商的 Web 服务器用户 ID 特权；(2) 授权读写和执行文件；(3) 授权写入系统二进制文件；(4) 授权访问商户和服务提供商的日志文件；和 (5) 确保商户或服务提供商不能独占系统资源的控制措施。
A.1.3	确保已启用日志和核查记录，它们对每个机构的持卡人数据环境都是唯一的，而且符合 PCI DSS 要求 10。	日志应该在共享主机环境中可用，以便商户和服务提供商能访问和查看特定于他们的持卡人数据环境的日志。
A.1.4	启用在任何托管商户或服务提供商出现漏洞时及时提供取证调查的流程。	共享主机提供商必须有针对威胁需取证调查时提供快速和便捷响应的流程，并细化到相应级别的详情信息，以便可以使用个人商户或服务提供商的详情。

附录 A： PCI 数据安全标准：相关文件

创建以下文件的目的是帮助商户和服务提供商了解 PCI 数据安全标准和合规要求与责任。

文件	受众
PCI 数据安全标准要求和安全评估程序	所有商户和服务提供商
PCI DSS 导航：了解要求的目的	所有商户和服务提供商
PCI 数据安全标准：自行评估调查问卷指南与说明	所有商户和服务提供商
PCI 数据安全标准：自行评估调查问卷 A 和证明书	商户[10]
PCI 数据安全标准：自行评估调查问卷 B 和证明书	商户[10]
PCI 数据安全标准：自行评估调查问卷 C 和证明书	商户[10]
PCI 数据安全标准：自行评估调查问卷 D 和证明书	商户[10] 和所有服务提供商
PCI DSS 和 PA-DSS 术语、缩略语	所有商户和服务提供商

[10] 要确定适合的自行评估调查问卷，请参阅《*PCI 数据安全标准：自行评估指南与说明*》中的“选择最适合您公司的 SAQ 和证明书”。