

PCI Data Security Standard

1. Summary

When consumers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. The Payment Card Industry Security Standards Council was founded as an independent body to develop, enhance, disseminate, and assist with implementation of security standards for payment account security. Through adoption and compliance of the PCI SSC Standards, retailers and consumers have policies, procedures and practices to assist them in staying the proverbial one step ahead of the "bad guys."

2. PCI DSS Framework

- 1. Build and Maintain a Secure Network:** requirements 1 and 2
- 2. Protect Cardholder Data:** requirements 3 and 4
- 3. Maintain a Vulnerability Management Program:** requirements 5 and 6
- 4. Implement Strong Access Control Measures:** requirements 7, 8 and 9
- 5. Regularly Monitor and Test Networks:** requirements 10 and 11
- 6. Maintain an Information Security Policy:** requirement 12

3. PCI Security Standard Framework

The PCI DSS 12 general requirements that describe the practices and procedures relating to are:

- 1. Requirement 1 - Installing and maintaining firewall configurations to protect cardholder data:** All systems must be protected from unauthorized access from the Internet, whether entering the system as e-Commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI Data Security Standard

- 2. Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters:** Hackers often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.
- 3. Requirement 3 - Protecting stored cardholder data:** Minimizing risk due to interception of protected data is the intent of requirement 3. Encryption is a critical component of cardholder data protection. With encryption cryptography, data is rendered unreadable and unusable unless the proper decrypting key is known. All methods of protecting stored data should be considered as potential risk mitigation opportunities. Examples include, storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.
- 4. Requirement 4 - Encrypting the transmission of cardholder data across open, public networks:** Encryption must also be applied to transmission media and methodologies. Secure tunneling protocols such as IP Security (IPSec) and encryption protocols such as Secure Socket Layer (SSL) must be used to secure data and avoid the probability of interception and diversion while in transit.
- 5. Requirement 5 - Use of and regular updates of anti-virus software or programs:** Many vulnerabilities and malicious viruses enter the network via e-mail activities, file transfers and other employee activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.
- 6. Requirement 6 - Developing and maintaining secure systems and applications:** Many system vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released and appropriate software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications,

PCI Data Security Standard

numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

- 7. Requirement 7 - Restricting access to cardholder data by business need-to-know:** This requirement ensures critical data can only be accessed by authorized personnel.
- 8. Requirement 8: Assigning unique IDs to each person with computer access:** Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.
- 9. Requirement 9 - Restricting physical access to cardholder data:** Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and must be appropriately restricted.
- 10. Requirement 10 - Tracking and monitoring all access to network resources and cardholder data:** The presence of logs in all environments allows thorough tracking, analysis and audits in the event that something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.
- 11. Requirement 11 - Regular testing of security systems and processes:** Vulnerabilities are an ongoing activity of hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested regularly to ensure security is maintained over time and with any changes in software.
- 12. Requirement 12: Maintaining policies that address information security for employees and contractors:** Security policy establishes a strong baseline for organizations and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it as well as changes to and updates applying to all policy activity.

PCI Data Security Standard

In addition to the 12 requirements in the PCI DSS the PCI Security Standards also include:

- ***PIN Entry Device (PED) Security Requirements***- PCI PED applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions. Merchants should use only PIN entry devices that are tested and approved by the PCI SSC. As of May 2009, 279 PEDs have been authorized by the PCI SSC are listed at: [PCI Approved PIN Entry Devices](#)
- ***Payment Application Data Security Standard (PA-DSS)*** - The PA-DSS is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants and third party agents to use payment applications that are validated independently by a PA-QSA company and accepted for listing by the PCI SSC. As of May 2009, a validated list of 275 applications are listed at: [PA-DSS Validated Payment Applications](#)

4. Merchant Compliance

Merchants who store, process, or transmit cardholder data are required through their acquirers (e.g. banks or other collecting/processing/scanning institutions) to validate compliance with the PCI DSS. Acquirers are responsible for ensuring that all of their merchants comply with the PCI DSS requirements. However, there are differing levels of collection activity depending of the size and type of merchant which can impact the merchant's ability to comply with the PCI DSS. Knowing this, the PCI SSC, has established a methodology of merchant

PCI Data Security Standard

levels through which merchants can identify their level of activity and an associated level of compliance validation and compliance timelines.

Merchant Level	Level Definition
1	<ul style="list-style-type: none">• Any merchant, "regardless of acceptance channel, processing over 6,000,000 Visa transactions per year.• Any merchant that has suffered a hack or an attack that resulted in an account data compromise.• Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.• Any merchant identified by any other payment card brand
2	<ul style="list-style-type: none">• Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year
3	<ul style="list-style-type: none">• Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year
4	<ul style="list-style-type: none">• Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year

5. PCI DSS Compliance Requirements

PCI Data Security Standard

Level	Validation Action	Validated By
1	<ul style="list-style-type: none"> • Annual On-site PCI Data Security Assessment and • Quarterly Network Scan 	<ul style="list-style-type: none"> • Qualified Security Assessor or Internal Audit if signed by Officer of the company • Approved Scanning Vendor
2	<ul style="list-style-type: none"> • Annual PCI Self-Assessment Questionnaire and • Quarterly Network Scan 	<ul style="list-style-type: none"> • Merchant • Approved Scanning Vendor
3	<ul style="list-style-type: none"> • Annual PCI Self-Assessment Questionnaire and • Quarterly Network Scan 	<ul style="list-style-type: none"> • Merchant • Approved Scanning Vendor
4	<ul style="list-style-type: none"> • Annual PCI Self-Assessment Questionnaire and • Quarterly Network Scan 	<ul style="list-style-type: none"> • Merchant • Approved Scanning Vendor