PCI Security Standards Council ™

Payment Card Industry (PCI) Data Security Standard

Version 1.1

Release: September, 2006

Build and Maintain a Secure Network

Requirement 1:   Install and maintain a firewall configuration to protect cardholder data

Requirement 2:   Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3:   Protect stored cardholder data

Requirement 4:   Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5:   Use and regularly update anti-virus software

Requirement 6:   Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7:   Restrict access to cardholder data by business need-to-know

Requirement 8:   Assign a unique ID to each person with computer access

Requirement 9:   Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10:   Track and monitor all access to network resources and cardholder data

Requirement 11:   Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12:   Maintain a policy that addresses information security

Preface

This document describes the 12 Payment Card Industry (PCI) Data Security Standard (DSS) requirements. These PCI DSS requirements are organized in 6 logically related groups, which are "control objectives."

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether **storage** of each data element is permitted or prohibited; **and if each data element** must be **protected**. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*

These security requirements apply to all "system components." System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

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.

1.1 Establish firewall configuration standards that include the following:

    1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration

    1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks

    1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

    1.1.4 Description of groups, roles, and responsibilities for logical management of network components

    1.1.5 Documented list of services and ports necessary for business

    1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)

    1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented

    1.1.8 Quarterly review of firewall and router rule sets

    1.1.9 Configuration standards for routers.

1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.

1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:

    1.3.1 Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)

    1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ

    1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)

    1.3.4 Placing the database in an internal network zone, segregated from the DMZ

    1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment

    1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration

1.3.7 Denying all other inbound and outbound traffic not specifically allowed

1.3.8 Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)

1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).

1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic

1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.

1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Hackers (external and internal to a company) 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.

2.1 Always change vendor-supplied defaults **before** installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).

2.1.1 **For wireless environments**, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Assessment Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

2.2.1 Implement only one primary function per server (*for example, web servers, database servers, and DNS should be implemented on separate servers)*

2.2.2 Disable all unnecessary and insecure services and protocols *(services and protocols not directly needed to perform the devices' specified function)*

2.2.3 Configure system security parameters to prevent misuse

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted).

Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3*:*

3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data

In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements. Note: See "Glossary" for additional information.

3.2.2 Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions

Note: See "Glossary" for additional information.

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).

3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- Strong one-way hash functions (hashed indexes)
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures.

The MINIMUM account information that must be rendered unreadable is the PAN.

If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls for Encryption of Stored Data."

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control

mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.

    3.5.1 Restrict access to keys to the fewest number of custodians necessary

    3.5.2 Store keys securely in the fewest possible locations and forms.

3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

    3.6.1 Generation of strong keys

    3.6.2 Secure key distribution

    3.6.3 Secure key storage

    3.6.4 Periodic changing of keys

- As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically
- At least annually.

    3.6.5 Destruction of old keys

    3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)

    3.6.7 Prevention of unauthorized substitution of keys

    3.6.8 Replacement of known or suspected compromised keys

    3.6.9 Revocation of old or invalid keys

    3.6.10 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).

    4.1.1 **For wireless networks transmitting cardholder data**, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address.

4.2 Never send unencrypted PANs by e-mail.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

5.1   Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)

       Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.

       5.1.1   Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.

5.2   Ensure that all anti-virus mechanisms are current, actively running, and capable of generating assessment logs.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

6.1   Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

6.2   Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.

6.3   Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.

       6.3.1   Testing of all security patches and system and software configuration changes before deployment

       6.3.2   Separate development, test, and production environments

       6.3.3   Separation of duties between development, test, and production environments

       6.3.4   Production data (live PANs) are not used for testing or development

       6.3.5   Removal of test data and accounts before production systems become active

       6.3.6   Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers

       6.3.7   Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.

6.4   Follow change control procedures for all system and software configuration changes. The procedures must include the following:

       6.4.1   Documentation of impact

       6.4.2   Management sign-off by appropriate parties

       6.4.3   Testing of operational functionality

6.4.4 Back-out procedures

6.5 Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:

6.5.1 Unvalidated input

6.5.2 Broken access control (for example, malicious use of user IDs)

6.5.3 Broken authentication and session management (use of account credentials and session cookies)

6.5.4 Cross-site scripting (XSS) attacks

6.5.5 Buffer overflows

6.5.6 Injection flaws (for example, structured query language (SQL) injection)

6.5.7 Improper error handling

6.5.8 Insecure storage

6.5.9 Denial of service

6.5.10 Insecure configuration management

6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

- Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security

- Installing an application layer firewall in front of web-facing applications.

Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

This requirement ensures critical data can only be accessed by authorized personnel.

7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.

7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

Requirement 8: Assign a unique ID 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.

8.1   Identify all users with a unique user name before allowing them to access system components or cardholder data.

8.2   In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password
- Token devices (e.g., SecureID, certificates, or public key)
- Biometrics.

8.3   Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

8.4   Encrypt all passwords during transmission and storage on all system components.

8.5   Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

     8.5.1   Control addition, deletion, and modification of user IDs, credentials, and other identifier objects

     8.5.2   Verify user identity before performing password resets

     8.5.3   Set first-time passwords to a unique value for each user and change immediately after the first use

     8.5.4   Immediately revoke access for any terminated users

     8.5.5   Remove inactive user accounts at least every 90 days

     8.5.6   Enable accounts used by vendors for remote maintenance only during the time period needed

     8.5.7   Communicate password procedures and policies to all users who have access to cardholder data

     8.5.8   Do not use group, shared, or generic accounts and passwords

     8.5.9   Change user passwords at least every 90 days

     8.5.10   Require a minimum password length of at least seven characters

     8.5.11   Use passwords containing both numeric and alphabetic characters

     8.5.12   Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used

     8.5.13   Limit repeated access attempts by locking out the user ID after not more than six attempts

     8.5.14   Set the lockout duration to thirty minutes or until administrator enables the user ID

     8.5.15   If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

     8.5.16   Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

Requirement 9: Restrict 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 should be appropriately restricted.

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

    9.1.1 Use cameras to monitor sensitive areas. Assessment collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law

    9.1.2 Restrict physical access to publicly accessible network jacks

    9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.

9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.

    "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

9.3 Make sure all visitors are handled as follows:

    9.3.1 Authorized before entering areas where cardholder data is processed or maintained

    9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees

    9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.

9.4 Use a visitor log to maintain a physical assessment trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.

9.5 Store media back-ups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.

9.6 Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.

9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:

    9.7.1 Classify the media so it can be identified as confidential

    9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.

9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).

9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.

    9.9.1 Properly inventory all media and make sure it is securely stored.

9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:

    9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials

    9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

10.2 Implement automated assessment trails for all system components to reconstruct the following events:

    10.2.1 All individual user accesses to cardholder data

    10.2.2 All actions taken by any individual with root or administrative privileges

    10.2.3 Access to all assessment trails

    10.2.4 Invalid logical access attempts

    10.2 5 Use of identification and authentication mechanisms

    10.2.6 Initialization of the assessment logs

    10.2.7 Creation and deletion of system-level objects.

10.3 Record at least the following assessment trail entries for all system components for each event:

    10.3.1 User identification

    10.3.2 Type of event

    10.3.3 Date and time

    10.3.4 Success or failure indication

    10.3.5 Origination of event

    10.3.6 Identity or name of affected data, system component, or resource.

10.4 Synchronize all critical system clocks and times.

10.5 Secure assessment trails so they cannot be altered.

    10.5.1 Limit viewing of assessment trails to those with a job-related need

    10.5.2 Protect assessment trail files from unauthorized modifications

    10.5.3 Promptly back-up assessement trail files to a centralized log server or media that is difficult to alter

    10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.

    10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

    Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.

10.7 Retain assessment trail history for at least one year, with a minimum of three months online availability.

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

11.1   Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.

11.2   Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

   Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.

11.3   Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

   11.3.1   Network-layer penetration tests

   11.3.2   Application-layer penetration tests.

11.4   Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

11.5   Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.

   Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

    12.1.1 Addresses all requirements in this specification

    12.1.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment

    12.1.3 Includes a review at least once a year and updates when the environment changes.

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:

    12.3.1 Explicit management approval

    12.3.2 Authentication for use of the technology

    12.3.3 List of all such devices and personnel with access

    12.3.4 Labeling of devices with owner, contact information, and purpose

    12.3.5 Acceptable uses of the technologies

    12.3.6 Acceptable network locations for the technologies

    12.3.7 List of company-approved products

    12.3.8 Automatic disconnect of modem sessions after a specific period of inactivity

    12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use

    12.3.10 When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.

12.5 Assign to an individual or team the following information security management responsibilities:

    12.5.1 Establish, document, and distribute security policies and procedures

    12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel

    12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations

    12.5.4 Administer user accounts, including additions, deletions, and modifications

    12.5.5 Monitor and control all access to data.

12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

    12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)

12.6.2 Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

12.7 Screen potential employees to minimize the risk of attacks from internal sources.

For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.

12.8 If cardholder data is shared with service providers, then contractually the following is required:

12.8.1 Service providers must adhere to the PCI DSS requirements

12.8.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)

12.9.2 Test the plan at least annually

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts

12.9.4 Provide appropriate training to staff with security breach response responsibilities

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems

12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

12.10.1. Maintain a list of connected entities

12.10.2. Ensure proper due diligence is conducted prior to connecting an entity

12.10.3. Ensure the entity is PCI DSS compliant

12.10.4. Connect and disconnect entities by following an established process.

Appendix A: PCI DSS Applicability for Hosting Providers

Requirement A.1: Hosting providers protect cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that hosting providers must protect each entity's hosted environment and data. Therefore, hosting providers must give special consideration to the following:

A.1   Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, as in A.1.1 through A.1.4:

    A.1.1   Ensure that each entity only has access to own cardholder data environment

    A.1.2   Restrict each entity's access and privileges to own cardholder data environment only

    A.1.3   Ensure logging and assessment trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10

    A.1.4   Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not necessarily guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*

Appendix B: Compensating Controls

Compensating Controls – General

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. See the PCI DSS Glossary for the full definition of compensating controls.

The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments. Each compensating control must be thoroughly evaluated after implementation to ensure effectiveness.

The following guidance provides compensating controls when companies are unable to render cardholder data unreadable per requirement 3.4.

Compensating Controls for Requirement 3.4

For companies unable to render cardholder data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered. *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Companies that consider compensating controls for rendering cardholder data unreadable must understand the risk to the data posed by maintaining readable cardholder data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable cardholder data. The controls considered must be in addition to controls required in the PCI DSS, and must satisfy the "Compensating Controls" definition in the PCI DSS Glossary. Compensating controls may consist of either a device or combination of devices, applications, and controls that meet **all of the** following conditions:

1. Provide additional segmentation/abstraction (for example, at the network-layer)
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
    *   IP address/Mac address
    *   Application/service
    *   User accounts/groups
    *   Data type (packet filtering)
3. Restrict logical access to the database
    *   Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
4. Prevent/detect common application or database attacks (for example, SQL injection).