Information about this New Document

New Document	This *Payment Card Industry Data Security Standard*, dated January 2005, is an entirely new document.
Contents	This manual contains security requirements developed by MasterCard International and Visa. This Payment Card Industry (PCI) Standard has also been endorsed and adopted by the payment brands denoted on the cover page. These security requirements apply to members, merchants, and service providers that store payment card information.
Billing	MasterCard will not bill principal members for this document.
Questions?	If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk.
MasterCard is Listening…	Please take a moment to provide us with your feedback about the material and usefulness of the *Payment Card Industry Data Security Standard* document using the following e-mail address: publications@mastercard.com We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.

Payment Card Industry Data Security Standard

January 2005

Copyright

The information contained in this manual is proprietary and confidential to MasterCard International Incorporated (MasterCard) and its members.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Media

This document is available:

- On MasterCard OnLine®

- On the MasterCard Site Data Protection Web site, https://sdp.mastercardintl.com

MasterCard International Incorporated
2200 MasterCard Boulevard
O'Fallon MO 63366-7263
USA

1-636-722-6100

www.mastercard.com

Payment Card Industry Data Security Standard

This manual defines the requirements for the Payment Card Industry (PCI) Data Security Standard.

PCI Data Security Standard

These Payment Card Industry (PCI) Data Security Requirements apply to all members, merchants, and service providers that store, process or transmit cardholder data.

Additionally, these security requirements apply to all "**system components**" which is defined as any **network component**, **server**, or **application** included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, Web, database, authentication, Domain Name Service (DNS), mail, proxy, and Network Time Protocol (NTP). Applications include all purchased and custom applications, including internal and external (Web) applications.

The following **12 Requirements** comprise the Payment Card Industry Data Security Standard.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

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

Protect Cardholder Data

3. Protect Stored Data

4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Build and Maintain a Secure Network

Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via 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. Install and maintain a firewall configuration to protect data

1.1   Establish firewall configuration standards that include:

    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 Intranet.

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

    1.1.5   Documented list of services/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   Periodic review of firewall/router rule sets.

    1.1.9   Configuration standards for routers.

1.2   Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, **except for:**

    1.2.1   Web protocols—HTTP (port 80) and SSL (typically port 443).

      1.2.2   System administration protocols (for example, SSH, or VPN).

      1.2.3   Other protocols required by the business (for example, for ISO 8583).

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:

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

      1.3.2   Restricting inbound and outbound Internet traffic to ports 80 and 443.

      1.3.3   Not allowing internal addresses to pass from the Internet into the DMZ (egress filters).

      1.3.4   Stateful inspection, also known as dynamic packet filtering (only "established" connections are allowed into the network).

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

      1.3.6   Restricting outbound traffic to that which is necessary for the payment card environment.

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

      1.3.8   Denying all other inbound and outbound traffic not specifically allowed.

      1.3.9   Installation of perimeter firewalls between any wireless networks and the payment card environment, and configuration of these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment.

      1.3.10 Installation of personal firewall software on any mobile and/or 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 information (for example, databases).

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

    1.4.2 Restrict outbound traffic from payment card applications to Internet Protocol (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).

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 the vendor-supplied defaults **before** you install a system on the network (for example, 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, Wireless Equivalent Privacy (WEP) keys, default Service Set Identifier (SSID), passwords, and SNMP community strings, and disabling of SSID broadcasts. Enable Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.

2.2 Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices.

    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 (for example, unnecessary Web servers).

2.3   Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/Transport Layer Security (TLS) for Web-based management and other non-console administrative access.

Protect Cardholder Data

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle.

3. Protect Stored Data

3.1   Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your 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 (not even if encrypted):

3.2.1   Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.).

3.2.2   Do not store the card-validation code (CVC) (Three-digit or four-digit value printed on the front or back of a payment card (for example, CVV2, and CVC2 data).

3.2.3   Do not store the PIN Verification Value (PVV).

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

Note that this does not apply to those employees and other parties with a specific need to see full credit card numbers.

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

- One-way hashes (hashed indexes), such as SHA-1
- Truncation
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Triple-DES (Data Encryption Standard) 128-bit or AES 256-bit with associated key management processes and procedures

The minimum account information that needs to be rendered unreadable is the payment card account number.

3.5   Protect encryption keys 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, including:

3.6.1   Generation of strong keys.

3.6.2   Secure key distribution.

3.6.3   Secure key storage.

3.6.4   Periodic key changes.

3.6.5   Destruction of old keys.

3.6.6   Split knowledge and 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 (mainly for RSA keys).

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

4. Encrypt transmission of cardholder and sensitive information across public networks

Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit.

4.1   Use strong cryptography and encryption techniques (at least 128 bit) such as SSL, Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks.

4.1.1   For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless Local Area Network (LAN). Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.

4.2   Never send cardholder information via unencrypted e-mail.

Maintain a Vulnerability Management Program

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

5. Use and regularly update anti-virus software or programs

5.1   Deploy anti-virus mechanisms on all systems commonly affected by viruses (for example PC's and servers).

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

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 via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. 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.

6.1.1   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 your standards to address new vulnerability issues.

6.3   Develop software applications based on industry best practices and include information security throughout the software development life cycle. Include the following:

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 (real credit card numbers) 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, to identify any potential coding vulnerability.

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

6.4.1   Documentation of impact.

6.4.2   Management sign-off by appropriate parties.

6.4.3   Testing that verifies operational functionality.

6.4.4   Back-out procedures.

6.5   Develop Web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. See www.owasp.org, "The Ten Most Critical Web Application Security Vulnerabilities." Cover prevention of common coding vulnerabilities in software development processes, to include:

6.5.1   Unvalidated input.

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

6.5.3   Broken authentication/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, 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.

Implement Strong Access Control Measures

This ensures critical data can only be accessed in an authorized manner.

7. Restrict access to data by business need-to-know

7.1   Limit access to computing resources and cardholder information to only 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.

8. Assign a unique ID to each person with computer access

This 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 username before allowing them to access system components or cardholder data.

8.2   Employ at least one of the methods below, in addition to unique identification, to authenticate all users:

   - Password
   - Token devices (for example, 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 Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) with tokens, or VPN 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:

   8.5.1   Control the 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 per user and change immediately after first use.

8.5.4   Immediately revoke accesses of 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 needed.

8.5.7   Distribute password procedures and policies to all users who have access to cardholder information.

8.5.8   Do not use group, shared, or generic accounts/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 information. This includes access by applications, administrators, and all other users.

9. Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data allows the opportunity to access devices or data, and 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. Audit this 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 information is accessible.

"Employee" refers to full-time and part-time employees, temporary employees/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:

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

    9.3.2   Given a physical token (for example, badge, or access device) that expires, and that identifies them 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 retain a physical audit 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 off-site facility, which may be either an alternate third-party or a commercial storage facility.

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

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

   9.7.1   Label the media so it can be identified as confidential.

   9.7.2   Send the media via secured courier or a delivery mechanism that can be accurately tracked.

9.8   Ensure management approves 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 information:

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

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

   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

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

10. Track and monitor all access to network resources and cardholder data

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

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

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 audit trails.

10.2.4 Invalid logical access attempts.

10.2.5 Use of identification and authentication mechanisms.

10.2.6 Initialization of the audit logs.

10.2.7 Creation and deletion of system-level objects.

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

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 audit trails so they cannot be altered, including the following:

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

   10.5.2 Protect audit trail files from unauthorized modifications.

   10.5.3 Promptly back-up audit 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/change detection software (such as Tripwire) 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 should include those servers that perform security functions like Intrusion Detection System (IDS) and Authentication, Authorization, and Accounting (AAA) servers (for example, RADIUS).

10.7   Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.

   An audit history usually covers a period of at least one year, with a minimum of 3 months available online.

11. Regularly test security systems and processes

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

11.1   Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts. Where wireless technology is deployed, use a wireless analyzer periodically 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 (for example, new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Note that external vulnerability scans must be performed by a scan vendor qualified by the payment card industry.

11.3   Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (for example, operating system upgrade, sub-network added to environment, Web server added to environment).

11.4   Use network intrusion detection systems, host-based intrusion detection systems, and/or 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 to alert personnel to unauthorized modification of critical system or content files, and perform critical file comparisons at least daily (or more frequently if the process can be automated).

Critical files are not necessarily 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 merchant or service provider.

Maintain an Information Security Policy

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

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

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

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:

12.3.1 Explicit management approval.

12.3.2 Authentication for use of the technology.

12.3.3 A 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 technology.

12.3.6 Acceptable network locations for these technologies.

12.3.7 A 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, disable storage of cardholder data onto local hard drives, floppy disks or other external media. Also, disable cut and paste, and print functions during remote access.

12.4 Ensure 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.

12.5.4 Monitor and control all access to data.

12.6 Make all employees aware of the importance of cardholder information security:

12.6.1 Educate employees (for example, through posters, letters, 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 who only have access to one card number at a time to facilitate a transaction, such as store cashiers, this requirement is a recommendation only.

12.8 Contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements. At a minimum, the agreement should address:

12.8.1 Acknowledgement that the 3rd party is responsible for security of cardholder data in their possession.

12.8.2 Ownership by each Payment Card brand, Acquirer, and Merchants of cardholder data and acknowledgement that such data can ONLY be used for assisting these parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for others uses specifically required by law.

12.8.3 Business continuity in the event of a major disruption, disaster, or failure.

12.8.4 Audit provisions that ensure that Payment Card Industry representative, or a Payment Card Industry approved third party, will be provided with full cooperation and access to conduct a thorough security review after a security intrusion. The review will validate compliance with Payment Card Industry Security Standards for protecting cardholder data.

12.8.5 Termination provision that ensures that 3rd party will continue to treat cardholder data as confidential.

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

12.9.1 Create an incident response plan to be used 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 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 Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.