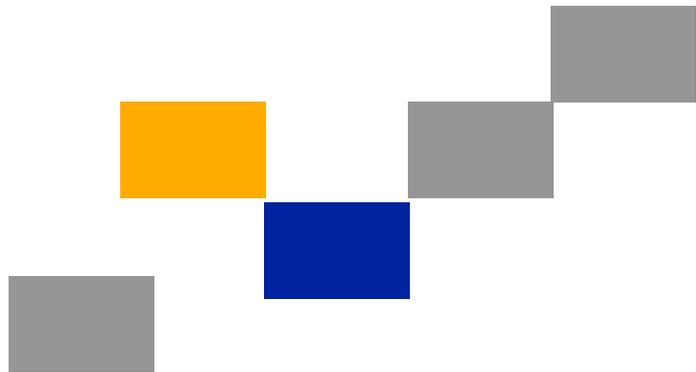**VISA**

ACCESS
INNOVATION
GROWTH

PCI Security Audit Procedures
Version 1.0
December 2004

Disclaimer

The Payment Card Industry (PCI) Security Audit Procedure is to be used as a 'guideline' to ensure all entities that store, process, or transmit Visa cardholder data meet PCI Data Security Standard. Visa Asia Pacific, however, makes no warranty or claim that completion or compliant with the audit procedures will prevent security breaches or losses, and disclaims any responsibility or liability for any security breaches or losses incurred, whether the audit procedures has been implemented or not.

Important

The Payment Card Industry (PCI) Security Audit Procedures is part of Visa Asia Pacific's Account Information Security (AIS) documentation suite. All Members and their agents (merchants and service providers) must ensure they process, store and transmit cardholder information in accordance with the PCI Data Security Standard (this standard supercedes Visa's AIS Standard v1.4, March 2000).

For more information on Visa Asia Pacific's AIS program please visit http://www.visa-asia.com/secured.

This document is to be used by those merchants and service providers who require an onsite review to validate compliance with the Payment Card Industry (PCI) Data Security Standard and to create the Report on Compliance.

Note that these 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, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including both internal and external (web) applications.

Scope of the Assessment

For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is processed, stored, or transmitted, unless otherwise specified.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is processed, stored, or transmitted, including:

- All external connections into the merchant network (e.g.; employee remote access, payment card company, third party access for processing, and maintenance)

- All connections to and from the authorization and settlement environment (e.g.; connections for employee access or for devices such as firewalls, and routers)

- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored.

- POS Terminals may be excluded, however:
  - If a POS environment is IP-based and there is external access, via Internet, wireless, VPN, dial-in, broadband, or publicly accessible machines (such as kiosks), to the merchant location, the POS environment must be must be included in the scope of the on-site review.
  - If a POS environment is either not IP-based or there is no external access to the merchant location, begin review at the connection into the authorization and settlement environment.

Note: The POS environment is the environment in which a transaction takes place at a merchant location (i.e. retail store, restaurant, hotel property, gas station, supermarket, or other point-of-sale location). An IP-based POS environment is one in which transactions are stored, processed, or transmitted on IP-based systems, or systems communicating via TCP/IP.

Wireless

If wireless technology is used to transmit, process, or store cardholder data (e.g., point-of-sale transactions, "line-busting", etc.), or if a wireless LAN is connected to or part of the cardholder environment (e.g., not clearly separated by a firewall), the Requirements and Testing Procedures for wireless environments must be performed as well. Wireless security is not mature yet, but these requirements specify that basic wireless security features be implemented to provide minimal protection. Since wireless technologies cannot yet be secured well, we recommend, before wireless technology is put in place, that a company carefully evaluate the need for the technology against the risk Consider deploying it only for non-sensitive data transmission, or waiting for more secure technology.

Outsourcing

For those entities that outsource processing, transmitting, or storage of cardholder data to third-party service providers, the Report On Compliance must document the role of each service provider; however, these service providers are responsible for validating their own compliance with the PCI Data Security Standard independent of their customers. Additionally, merchants and service providers must contractually require all associated third parties with access to cardholder data to adhere to the PCI Data Security Standard. Refer to Requirement 12.8 in this document for details.

Sampling

The assessor can select a sample of system components to test. The sample must be a representative selection of all of the types of system components, and include a variety of operating systems, functions, and applications as applicable to the area being reviewed. For example, the reviewer could choose Sun servers running Apache WWW, NT servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, Linux Servers running MYSQL, etc. If all applications run from a single OS (e.g., NT, Sun, etc.), then the sample should still include a variety of applications (e.g., database servers, web servers, data transfer servers, etc.).

See the first page of this document for the definition of "system components."

Report On Compliance

This document is to be used as the template to create the Report on Compliance. Acquirers, merchants, and service providers will need to follow each payment card company's respective reporting requirements to ensure each payment card company acknowledges an entity's compliance status. Please contact each payment card company to determine to whom the results should be submitted.

All assessors must apply the following report content and format when completing the Report On Compliance (ROC):

1. **Contact Information and Report Date**
   - Include contact information for the merchant or service provider, and assessor.
   - Date of report.

2. **Executive Summary**
   Include the following:
   - Business description.
   - List service providers, and other entities with which the company shares cardholder data.
   - List processor relationships
   - Whether entity is directly connected to a payment card company.
   - For merchants, POS products used

- Any wholly owned entities that require compliance with the PCI Data Security Standard.
- Any international entities that require compliance with the PCI Data Security Standard.
- Any wireless LANs and/or wireless POS terminals connected to the cardholder environment.

3. **Description of Scope of Work and Approach Taken**
   - Version of the Security Audit Procedures document used to conduct the assessment.
   - Timeframe of assessment.
   - Environment on which the assessment was focused (i.e., client's Internet access points, internal corporate network, processing points for the payment card company, etc.).
   - Any areas excluded from the review.
   - Brief description or high-level drawing of network topology and controls
   - List of those interviewed.
   - List of hardware and critical (e.g., database or encryption) software in use.
   - For Managed Service Provider (MSP) reviews, clearly delineate which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSPs' customers to include in their own reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans.

4. **Quarterly Scan Results**
   - Please briefly summarize the 4 most recent quarterly scan results in comments at Requirement 11.2
   - The scan should cover all externally accessible (Internet-facing) IP addresses in existence at the entity.

5. **Findings and Observations**
   - All assessors must utilize the following template to provide detailed report descriptions and findings on each requirement and sub-requirement.
   - Where applicable, document any compensating controls considered to conclude that a control is in place. See **Definitions** on the next page for further discussion of compensating controls.

Revalidation of Open Items

A "controls in place" report is required for compliance. If an initial report is issued with open items, the entity should correct all open items, and the assessor should revalidate that the remediation occurred and addressed all requirements. After the revalidation, the assessor should reissue a fully compliant ROC, submitted per the above instructions.

Definitions

For the purpose of the Security Audit Procedures, the following definitions will be used:

Requirements
The PCI Data Security Standard requirements by which an assessor validates an entity's compliance.

Compensating Controls
Controls put in place as alternatives to controls defined in the "Requirements" columns. These controls should also be examined by the assessor, and in the assessors' opinion, should meet the intention and rigor of the original requirement. Compensating controls should be "above and beyond" other PCI requirements - it is not a compensating control to simply be in compliance with other requirements in this document.

Testing Procedure
Processes to be followed by the assessor to address individual requirements and testing considerations. These testing procedures list detailed controls that the assessor should find in place to support the requirement. Where these detailed controls are not in place exactly as stated, or cannot be put in place due to technical or other constraints, the assessor should examine compensating controls.

In Place
Please provide a brief description of controls found in place, including those controls found to be in place as a result of compensating controls.

Not In Place
Please provide a brief description controls that are not in place. If a requirement is "Not Applicable" (N/A), please explain.

Target Date/ Comments
For those controls "Not In Place" include a target date that the entity expects to have controls "In Place". Any additional notes or comments may be included here as well.

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Requirement 1: Install and maintain a firewall configuration to protect data. *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' email 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:	**1.1** Obtain and inspect the firewall configuration standards and other documentation specified below to obtain evidence the standards are complete. Also obtain a copy of the following documentation:			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration.	**1.1.1** Obtain and examine the firewall configuration standards and verify a formal process is in place for all changes, including management approval and testing for all changes to external network connections and the firewall configuration.			
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks.	**1.1.2**. Obtain and examine a current network diagram, and verify that it documents all connections to cardholder data, including any wireless networks, and that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any DMZ and the Intranet.	**1.1.3** Obtain a current network diagram, and examine it verify that a firewall exists at each Internet connection and between any DMZ and the Intranet.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components.	**1.1.4** Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components.			
1.1.5 Documented list of services/ports necessary for business.	**1.1.5** Verify that firewall configuration standards include a documented list of services/ports necessary for business.			
1.1.6 Justification and documentation for any available	**1.1.6** Verify that firewall configuration standards include justification and documentation for any available protocols			

Visa Public

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
protocols besides HTTP and SSL, SSH, and VPN.	besides HTTP and SSL, SSH, and VPN.			
1.1.7 Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented.	**1.1.7** Verify that firewall configuration standards include justification and documentation for any risky protocols allowed (e.g., FTP), which includes reason for use of protocol, and security features implemented. Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured.			
1.1.8 Periodic review of firewall/router rule sets.	**1.1.8** Verify that firewall configuration standards require periodic review of firewall/router rule sets. Obtain evidence that the rule sets are periodically reviewed.			
1.1.9 Configuration standards for routers.	**1.1.9** Verify that firewall configuration standards include both firewalls and routers.			
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, **except for**:	**1.2** Choose a sample of (insert sample size) firewalls/routers 1) between the Internet and the DMZ and 2) between the DMZ and the internal network. The sample should include the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment. Examine firewall & router configurations to verify that inbound and outbound traffic is limited to:			
1.2.1 Web protocols – HTTP (port 80) and Secure Sockets Layer (SSL) (typically port 443).	**1.2.1** Web protocols (HTTP, HTTPS)			
1.2.2 System administration protocols (e.g., Secure Shell (SSH) or Virtual Private Network (VPN).	**1.2.2** System administration/remote access methods (VPN, SSH)			
1.2.3 Other protocols required by the business (e.g., for ISO 8583).	**1.2.3** Other allowed traffic required by the business and documented in the firewall policy.			

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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** Examine firewall/router configurations to verify that connections are restricted between publicly accessible servers and components storing cardholder data, as follows:			
1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters).	**1.3.1** Determine that inbound Internet traffic is limited to IP addresses within the DMZ.			
1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443.	**1.3.2** Determine that inbound and outbound Internet traffic is limited to ports 80 and 443.			
1.3.3 Not allowing internal addresses to pass from the Internet into the DMZ (egress filters).	**1.3.3** Determine that internal addresses cannot pass from the Internet into the DMZ.			
1.3.4 Stateful inspection, also known as dynamic packet filtering (only "established" connections are allowed into the network).	**1.3.4** Determine that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session (run NMAP on all TCP and UDP ports with "syn reset" or "syn ack" bits set – a response means packets are allowed through even if they are not part of a previously established session)).			
1.3.5 Placing the database in an internal network zone, segregated from the DMZ.	**1.3.5** Determine that the database is on an internal network zone, segregated from the DMZ.			
1.3.6 Restricting outbound traffic to that which is necessary for the payment card environment.	**1.3.6** Determine that outbound traffic is limited to that which is necessary and documented for the cardholder environment.			

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.3.7 Securing and synchronizing router configuration files (e.g., 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).	**1.3.7** Determine that router configuration files are secure and synchronized. (e.g., running configuration files - used for normal running of the routers, and start-up configuration files - used when machines are re-booted, have the same secure configurations).			
1.3.8 Denying all other inbound and outbound traffic not specifically allowed.	**1.3.8** Determine that all other inbound and outbound traffic not covered in 1.2.1 above is specifically denied.			
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.	**1.3.9** Determine that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into systems storing cardholder data.			
1.3.10 Installation of personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization's network.	**1.3.10** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active, which is configured by the organization to specific standards and not alterable by the employee.			
1.4 Prohibit direct public access between external networks and any system component that stores	**1.4** To determine that direct access between external public networks and components storing cardholder data are prohibited, perform the following, *specifically* for the			

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
cardholder information (e.g., databases).	firewall/router configuration implemented between the DMZ and the internal network:			
1.4.1 Implement a DMZ to filter and screen all traffic, to prohibit direct routes for inbound and outbound Internet traffic	**1.4.1** Examine firewall/router configurations and determine there is no direct route inbound or outbound for Internet traffic.			
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	**1.4.2** Examine firewall/router configurations and determine that internal outbound traffic from cardholder applications can only access IP addresses within the DMZ.			
1.5 Implement Internet Protocol (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).	**1.5** For firewall/router components, above, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading).			
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 the vendor-supplied defaults **before** you install a system on the network (e.g., passwords, SNMP community strings, and elimination of unnecessary accounts.).	**2.1** Use the sample of system components, and attempt to logon (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, WEP keys, default 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.	**2.1.1** Verify the following regarding vendor default settings for wireless environments: • WEP keys were changed were changed from default at installation, and are changed anytime any one with knowledge of the keys leaves the company or changes positions. • Default SSID was changed • Broadcast of the SSID was disabled • Default SNMP community strings on access points were changed • Default passwords on access points were changed. • WPA technology is enabled if the wireless system is WPA-capable. • Other security-related wireless vendor defaults, if applicable.			
2.2 Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices.	**2.2.a** Examine the organization's system configuration standards for network components and critical servers, including any wireless access points, and verify each item below is included in the standard. **2.2.b** Additionally determine that each item below is part of the process when new systems are configured.			
2.2.1 Implement only one primary function per server (e.g., web servers, database servers, and DNS should be implemented on separate servers).	**2.2.1** Only one primary function is implemented per server.			

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	**2.2.2** Obtain and inspect enabled system services, daemons, and protocols from the sample of (insert number and/or description of sample). Verify that unnecessary or insecure services or protocols are not enabled, and that any potentially dangerous ones are justified and documented as to appropriate use of the service (e.g. FTP is not used, or is encrypted via SSH or other technology).			
2.2.3 Configure system security parameters to prevent misuse.	**2.2.3.a** Inquire of system administrators and/or security managers to determine that they have knowledge of common security parameter settings for their operating systems, database servers, Web servers, and wireless systems. **2.2.3.b** Verify that common security parameter settings are included in the system configuration standards. **2.2.3.c** Select a sample of (insert number and/or description of sample) from all system components the samples of databases and critical servers (including wireless), and verify that common security parameters are set appropriately.			
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (e.g. unnecessary web servers).	**2.2.4** Obtain and inspect system files to determine that all unnecessary functionality (e.g., drivers, features, subsystems, file systems, etc.) is removed. Also, verify enabled functions are documented, support secure configuration, and are the only ones present on the sampled machines.			

Build and Maintain a Secure Network

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**2.3** From the sample of *(insert number and/or description of sample)* system components, verify that non-console administrative access is encrypted by: • Observing an administrator log on to each sampled system to determine that SSH (or other encryption method) is invoked before the administrator's password is requested. • Reviewing services and parameter files on sampled systems to determine that Telnet and other remote login commands are not available for use internally. • Verifying that administrator access to the wireless management interface is encrypted with SSL/TLS. Alternatively, verify that administrators cannot connect remotely to the wireless management interface (all management of wireless environments is only from the console).			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Requirement 3: Protect Stored 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.*				
3.1 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.	**3.1** Obtain the company policies and procedures for data retention and disposal, and observe that these policies and procedures include: • Legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (e.g., cardholder data needs to be held for X period for Y business reasons). • Disposal of data when no longer needed for legal, regulatory or business reasons, including disposal of cardholder data. • Coverage for all storage of cardholder data, including database servers, mainframes, transfer directories and bulk data copy directories used to transfer data between servers, and directories used to normalize data between server transfers. • A programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements. Alternatively, performance of an audit, at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements.			
3.2 Do not store sensitive authentication data subsequent to authorization (not even if encrypted):	**3.2** If sensitive authentication data is received and erased, obtain and review methodology for erasing the data to determine the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps.			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.2.1 Do not store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.).	**3.2.1** Examine the following from the sample selected, and obtain evidence that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Several database schemas			
3.2.2 Do not store the card-validation code—(Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 data or CVC2 data)).	**3.2.2** Examine the following from the sample selected, and obtain evidence that three-digit or four-digit card-validation code printed on the signature panel (CVV2/CVC2 data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Several database schemas			
3.2.3 Do not store the PIN Verification Value (PVV).	**3.2.3** Examine the following from the sample selected, and obtain evidence that the PIN Verification Value (PVV data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Several database schemas			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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.*	**3.3** Obtain and review written policies and review online displays of credit card data to determine that the credit card numbers are masked when displaying cardholder data, except for those with a specific need to see full credit card numbers.			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.4 Render sensitive cardholder data unreadable anywhere it is stored, (including data on portable 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 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.*	**3.4.a** Obtain documentation about the cryptographic system used to protect stored data, including the vendor, type of cryptographic system, and the encryption algorithms. Verify that data is rendered unreadable using one of the following algorithms: • One-way hashes (hashed indexes) such as SHA-1 • Truncation or masking • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management processes and procedures. **3.4.b** Examine several tables from each database server in the sample of database machines to verify the data is encrypted (i.e., not stored in plain text). **3.4.c** Examine a sample of removable media (e.g., backup tapes) to confirm that cardholder data is encrypted. **3.4.d** Examine a sample of audit logs to confirm that cardholder data is sanitized or removed from the logs. **3.4.e** Verify that any cardholder data received from wireless networks is encrypted wherever stored.			
3.5 Protect encryption keys against both disclosure and misuse:	**3.5** Verify processes to protect encryption keys against disclosure and misuse by performing the following:			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.5.1 Restrict access to keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to determine that access to cryptographic keys is restricted to very few custodians.			
3.5.2 Store keys securely in the fewest possible locations and forms.	**3.5.2** Review system configuration files to determine that storage of cryptographic keys in encrypted format and storage of key-encrypting keys separately from data-encrypting keys.			
3.6 Fully document and implement all key management processes and procedures including:	**3.6.a** Verify the existence of key management procedures. **3.6.b For Service Providers** only: If the Service Provider shares keys with their customers for transmission of cardholder data, verify that the Service Provider provides documentation to customers that includes guidance on how to securely store and change customer's encryption keys (used to transmit data between customer and service provider). Examine the key management procedures and determine the procedures require the following:			
3.6.1 Generation of strong keys.	**3.6.1** Generation of strong keys.			
3.6.2 Secure key distribution.	**3.6.2** Secure key distribution.			
3.6.3 Secure key storage.	**3.6.3** Secure key storage.			
3.6.4 Periodic key changes.	**3.6.4** Periodic key changes.			
3.6.5 Destruction of old keys.	**3.6.5** Destruction of old keys.			
3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).	**3.6.6** Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.6.7 Prevention of unauthorized substitution of keys.	**3.6.7** Prevention of unauthorized substitution of keys.			
3.6.8 Replacement of known or suspected compromised keys.	**3.6.8** Replacement of known or suspected compromised keys.			
3.6.9 Revocation of old or invalid keys (mainly for RSA keys).	**3.6.9** 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.	**3.6.10** Key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Requirement 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 Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks.	**4.1.a** Verify the use of encryption (e.g., SSL) wherever cardholder data is transmitted or received over the Internet by performing the following: • Verify that at least 128 bit encryption is used during data transmission. • For SSL implementations, verify that HTTPS appears as a part of the browser Universal Record Locator (URL), and that no cardholder data was required when HTTPS did not appear in the URL. • Select a sample of transactions as they are received, and observe transactions as they occur to verify that cardholder data is encrypted during transit. • Verify that only trusted SSL keys/certificates are accepted. **4.1.b** Verify that, for the encryption methodology in use, the proper encryption strength is implemented. For example: • 3DES – 128 bits • AES – 256 bits • RSA – 1024 bits • Check vendor recommendations/best practices for other encryption methodologies.			

Protect Cardholder Data

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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 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.	**4.1.1** For wireless networks transmitting cardholder data or connected to cardholder environments, verify that: • Appropriate encryption methodologies are in use for any wireless transmissions, such as: VPN, SSL/TLS at 128 bit, WEP (Wired Equivalency Protocol) at 128 bits, and/or WPA. • If WEP is used, verify processes are in place to rotate shared WEP keys at least quarterly and whenever key personnel leave. • If WEP is used, verify that another methodology is in use, in addition to WEP, to protect the data. • For automated key rotation processes, verify that keys change every 10-30 minutes.			
4.2 Never send cardholder information via unencrypted e-mail.	**4.2.a** Observe that email encryption software exists on employees' personal computers. **4.2.b** Verify existence of a policy stating that cardholder data is not to be sent via unencrypted emails. **4.2.c** Inquire of 3-5 employees to determine whether use of email encryption software is required for emails containing cardholder data.			

Maintain a Vulnerability Management Program

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Requirement 5: Use and regularly update anti-virus software. *Many vulnerabilities and malicious viruses enter the network via employees' email activities. Anti-virus software must be used on all email systems and desktops to protect systems from malicious software.*				
5.1 Deploy anti-virus mechanisms on all systems commonly affected by viruses (e.g., PCs and servers).	**5.1** For the sample of *(insert number and/or description of sample)* system components, verify that anti-virus software is installed.			
5.2 Ensure that all anti-virus mechanisms current, and actively running, and capable of generating audit logs.	**5.2** To verify that anti-virus software is current as of *(insert as-of date)*, actively running, and capable of generating logs, perform the following: • Obtain and review the policy requiring updates to anti-virus software and definitions. • Verify that the master installation of the software is enabled for automatic updates and periodic scans, and that the servers examined at 5.1 above have these features enabled. • Verify that log generation is enabled and that the logs are being retained in accordance with the company's retention policy.			
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 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** Using the sample of *(insert either number or description of sample)* system components and software, compare the list of security patches installed on each system to the most recent vendor security patch list, to determine that current vendor patches are installed.			
6.1.1 Install relevant security patches within one month of release.	**6.1.1** Examine policies related to security patch installation to determine they require installation of all relevant new security patches within 30 days.			

Maintain a Vulnerability Management Program

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.2 Establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet). Update your standards to address new vulnerability issues.	**6.2** Inquire of those responsible for processes in place to identify new security vulnerabilities, and verify that the process includes using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2 as new vulnerability issues are found.			
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** Obtain and review written software development processes to confirm they are based on industry standards and that security is included throughout the life cycle. From review of written software development processes, inquiry of software developers, and review of relevant data (network configuration documentation, production and test data, etc.), determine the following:			
6.3.1 Testing of all security patches and system and software configuration changes before deployment.	**6.3.1** All changes (including patches) are tested before being deployed into production.			
6.3.2 Separate development/test and production environments.	**6.3.2** The test/development environments are separate from the production environment, with access control in place to enforce the separation.			
6.3.3 Separation of duties between development/test and production environments.	**6.3.3** There is a separation of duties between those personnel assigned to the development/test environments, and those assigned to the production environment.			
6.3.4 Production data (real credit card numbers) are not used for testing or development.	**6.3.4** Examine data used in the testing and development environments, and verify that production data (real credit card numbers) is not used for testing and development purposes, or is sanitized before use.			
6.3.5 Removal of test data and accounts before production systems become active.	**6.3.5** Test data and accounts are removed before a production system becomes active.			

version 1.0 December 15, 2004

Visa Public

Maintain a Vulnerability Management Program

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.	**6.3.6** Custom application accounts, usernames and/or passwords are removed before system goes into production or is released to customers.			
6.3.7 Review of custom code prior to release to production or customers, to identify any potential coding vulnerability.	**6.3.7.a** Obtain and review written policies to confirm they dictate that code reviews are required, and must be performed by individuals other then the originating author of the code. **6.3.7.b** Confirm that code reviews are occurring for new code as well as after code changes.			
6.4 Follow change control procedures for system and software configuration changes. The procedures should include:	**6.4** Obtain company change-control procedures related to implementing security patches and software modifications, and determine the procedures require items **6.4.1** – **6.4.4** below. Select a sample of system components. Find the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Determine that change control processes are implemented, as follows:			
6.4.1 Documentation of impact.	**6.4.1.a** Obtain evidence that documentation of customer impact in included in the change control documentation for each sampled change.			
6.4.2 Management sign-off by appropriate parties.	**6.4.2** Obtain evidence that management sign-off by appropriate parties is present for each sampled change.			
6.4.3 Testing that verifies operational functionality.	**6.4.3** Obtain evidence that testing that verifies operational functionality was performed for each sampled change.			
6.4.4 Back-out procedures.	**6.4.4** Obtain evidence that that back-out procedures are prepared for each sampled change..			

Maintain a Vulnerability Management Program

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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.a** Obtain and examine software development processes for any web-based applications. Confirm the process requires training in secure coding techniques for developers, and is based on guidance such as the OWASP guidelines. **6.5.b** For any web-based applications, inquire of a sample of *(insert sample size)* web developers and obtain evidence that they are knowledgeable in secure coding techniques. Alternatively, determine that periodic external code reviews or application penetration tests are performed based on OWASP guidelines, and that all coding vulnerabilities were corrected and re-evaluated. For any web-based applications, determine that processes are in place to determine that web applications are not vulnerable to the following:			
6.5.1 Unvalidated input.	**6.5.1** Unvalidated input.			
6.5.2 Broken access control (e.g., malicious use of user IDs).	**6.5.2** Malicious use of user IDs.			
6.5.3 Broken authentication and session management (use of account credentials and session cookies).	**6.5.3** Malicious use of account credentials and session cookies.			
6.5.4 Cross-site scripting (XSS) attacks.	**6.5.4** Cross-site scripting.			
6.5.5 Buffer overflows.	**6.5.5** Buffer overflows due to unvalidated input and other causes.			
6.5.6 Injection flaws (e.g., SQL injection).	**6.5.6** SQL injection and other command injection flaws.			
6.5.7 Improper error handling.	**6.5.7** Error handling flaws.			
6.5.8 Insecure storage.	**6.5.8** Insecure storage.			

Maintain a Vulnerability Management Program

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.5.9 Denial of service.	**6.5.9** Denial of service.			
6.5.10 Insecure configuration management.	**6.5.10** Insecure configuration management.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Requirement 7: Restrict access to data by business need-to-know. *This ensures critical data can only be accessed in an authorized manner.*				
7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.	**7.1** Obtain the written policy for data control, and determine that it includes the following: - Access rights for privileged User IDs are restricted to least privileges necessary to perform the job. - Assignment of privileges to individuals is based on job classification and function. - Requirement for an authorization form that is signed by management and specifies required privileges. - An automated access control system			
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.	**7.2** Examine system settings and vendor documentation to verify there is an access control system in place, and that it is implemented to include the following: - Coverage of all system components. - Assignment of privileges to individuals based on job classification and function. "Deny-all" setting by default (some access control systems are set by default to "allow-all" thereby allowing access unless/until a rule is written to specifically deny it).			
Requirement 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.	**8.1** For the sample of *(insert number and/or description of sample)* system components, review user ID listings and verify that all users have a unique username for access to system components or cardholder data.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.2 Employ at least one of the methods below, in addition to unique identification, to authenticate all users: • Password • Token devices (i.e., SecurId, certificates, or public key) • Biometrics	**8.2** To verify that users are authenticated using unique ID and additional authentication item (e.g., password) for access to the cardholder environment, perform the following: • Obtain documentation describing the authentication method(s) used. • For each type of authentication method used and once for each type of system component, observe an authentication to verify authentication is working according to documented authentication method(s).			
8.3 Implement 2-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates.	**8.3** To determine that 2-factor authentication is in place for all remote network access, observe an employee (e.g., an administrator) while they connect remotely to the network, and verify that both a password and an additional authentication item (Smart card, token PIN, etc.) are required.			
8.4 Encrypt all passwords during transmission and storage, on all system components.	**8.4.a** For selected system components in the cardholder environment, examine password files to verify that passwords are unreadable. Include password files for all system components **8.4.b** For **Service Providers** only, observe password files to verify that customer passwords are encrypted.			
8.5 Ensure proper user authentication and password management for non-consumer users and administrators, for all system components.	**8.5** Verify, via review of procedures and discussions that procedures exist for user authentication and password management, by performing the following:			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.5.1 Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.5.1.a** Select a sample of *(insert number)* user IDs, including both administrators and general users, from sampled system components. To verify that each user is authorized per company policy, perform the following: • Obtain an authorization form for each ID. • Verify the IDs are implemented in accordance with the authorization form (e.g., with privileges as specified, all signatures obtained, etc.), by tracing information from the authorization form to the system. **8.5.1.b** Determine that only administrators have access to management consoles for wireless networks.			
8.5.2 Verify user identity before performing password resets.	**8.5.2** Examine password procedures and observe security personnel to confirm that if a user requests a password reset via phone, email, web, or other non-face-to-face method, that user's identity is verified before the password is reset.			
8.5.3 Set first-time passwords to a unique value per user and change immediately after first use	**8.5.3** Examine password procedures and observe security personnel to confirm that first-time passwords for new users are set to a unique value per user, and changed after first use.			
8.5.4 Immediately revoke accesses of terminated users.	**8.5.4** Select a sample of *(insert number)* employees terminated in the last 6 months, and review user access listings as of *(insert as-of date)* to verify their IDs have been inactivated or removed.			
8.5.5 Remove inactive user accounts at least every 90 days.	**8.5.5** From the sample of user IDs selected above, verify there are no inactive accounts over 90 days old.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.5.6 Enable accounts used by vendors for remote maintenance only during the time needed.	**8.5.6** Verify that any accounts used by vendors to support and maintain system components are inactive, enabled only when needed by the vendor, and monitored while being used..			
8.5.7 Distribute password procedures and policies to all users who have access to cardholder information.	**8.5.7** From the sample of user IDs selected above, and inquire about their awareness of password procedures.			
8.5.8 Do not permit group, shared, or generic accounts/passwords.	**8.5.8.a** For the sample of *(insert number and/or description of sample)* system components, review user ID listings and verify the following: • Generic ID's and accounts are disabled or removed • Shared IDs for system administration activities and other critical functions do not exist. • Shared and generic IDs are not used to administer wireless LANs and devices. **8.5.8.b** Review password procedures to verify that group and shared passwords are explicitly prohibited. **8.5.8.c** Interview system administrators to verify that group and shared passwords are not given out even if requested.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.5.9 Change user passwords at least every 90 days.	**8.5.9** For the sample of *(insert number and/or description of sample)* system components, obtain and inspect system configuration settings as of *(insert as-of date)* to verify that user password parameters are set to require users to change passwords at least every 90 days For **Service Providers** only, verify via review of internal processes and customer/user documentation, that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords should change.			
8.5.10 Require a minimum password length of at least seven characters.	**8.5.10** For the sample of *(insert number and/or description of sample)* system components, obtain and inspect system configuration settings as of *(insert as-of date)* to verify that password parameters are set to require passwords to be at least seven characters long. For **Service Providers** only, verify via review of internal processes and customer/user documentation, that customer passwords are required to meet minimum length requirements.			
8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11** For the sample of *(insert number and/or description of sample)* system components, obtain and inspect system configuration settings as of *(insert as-of date)* to verify that passwords parameters are set to require passwords to contain both numeric and alphabetic characters. For **Service Providers** only, verify via review of internal processes and customer/user documentation, that customer passwords are required to contain both numeric and alphabetic characters.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords used.	**8.5.12** For the sample of *(insert number and/or description of sample)* system components, obtain and inspect system configuration settings as of *(insert as-of date)* to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. For **Service Providers** only, verify via review of internal processes and customer/user documentation, that new customer passwords cannot be the same as the previous four passwords.			
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13** For the sample of *(insert number and/or description of sample)* system components, obtain and inspect system configuration settings as of *(insert as-of date)* to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts. For **Service Providers** only, verify via review of internal processes and customer/user documentation, that customer accounts are temporarily locked-out after not more than six invalid access attempts.			
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID.	**8.5.14** For the sample of *(insert number and/or description of sample)* system components, obtain and inspect system configuration settings as of *(insert as-of date)* to verify that password parameters are set to require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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.	**8.5.15** For the sample of *(insert number and/or description of sample)* system components, obtain and inspect system configuration settings as of *(insert as-of date)* to verify that system/session idle time out features have been set to 15 minutes.			
8.5.16 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.	**8.4.16.a** Review database configuration settings for a sample of *(insert number)* databases to verify that access is authenticated, including that for individuals, applications, and administrators. **8.4.16.b** Review database configuration settings and database accounts to verify that direct SQL queries to the database are prohibited (there should be very few individual database login accounts, limited to database administrators).			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Requirement 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** Verify the existence of the following physical security controls for each computer room, data center and other physical areas with systems that contain cardholder data: • Observe that access is controlled via badge readers and authorized badges, lock and key, etc. • Have a system administrator attempt to log into consoles for three randomly selected systems in the cardholder environment, and verify they are "locked" to prevent unauthorized use.			
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.	**9.1.1** Observe that video cameras are present to monitor the entry/exit points of data centers where cardholder data is stored or present. Video cameras should be internal to the data center or otherwise protected from tampering or disabling. Determine that the cameras are monitored and that the data from the cameras is stored for at least three months.			
9.1.2 Restrict physical access to publicly accessible network jacks.	**9.1.2** Inquire of network administrators and also determine by observation that network jacks are only enabled when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.	**9.1.3** Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.			
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.*	**9.2.a** Review processes for assigning badges to employees, contractors, and visitors, and verify these processes include: • Processes for granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges. • Limited access to badge system. **9.2.b** Observe people within the facility to determine that it is easy to distinguish between employees and visitors.			
9.3 Make sure all visitors are:	**9.3** Verify the following employee/visitor controls are present:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	**9.3.1** Observe visitors to verify the use of ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.			
9.3.2 Given a physical token (e.g., badge or access device) that expires, and that identifies them as non-employees.	**9.3.2** Observe employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outsiders and that visitor badges expire.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration date.			
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.	**9.4** Verify that a visitor log is in use for physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted. Confirm the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least 3 months.			
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.	**9.5** Review policies and procedures for backups and visit the off-site storage facility to determine that backup media are stored in a physically secure, fireproof, offsite location.			
9.6 Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.	**9.6** Obtain the policies and procedures for protecting all paper and electronic media that contains cardholder data. Verify that the process includes controls for paper and electronic media in computer rooms and data centers, as well as paper receipts, paper reports, faxes, CDs and disks in employee desks and open workspaces, and PC hard drives.			
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information:	**9.7** Verify that a policy exists to control distribution of cardholder information, covers all distributed media including that distributed to individuals, and that this policy requires the following:			
9.7.1 Label the media so it can be identified as confidential.	**9.7.1** All media should be labeled so that it can be identified as "confidential".			
9.7.2 Send the media via secured courier or a delivery mechanism that can be accurately tracked.	**9.7.2** All media sent outside the facility is logged and authorized by management, and sent via secured courier or other delivery mechanism that can be tracked.			

Implement Strong Access Control Measures

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
9.8 Ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite media tracking logs, and verify the presence in the logs of tracking details and proper management authorization.			
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder information:	**9.9** Obtain the policy for controlling storage and maintenance of hardcopy and electronic media, and verify this policy requires periodic media inventories. Verify related processes by performing the following:			
9.9.1 Properly inventory all media and make sure it is securely stored.	**9.9.1.a** Obtain and review the media inventory log to verify that periodic media inventories are performed. **9.9.1.b** Obtain and review processes in place to verify that media is securely stored.			
9.10 Destroy media containing cardholder information when it is no longer needed for business or legal reasons:	**9.10.a** Obtain the periodic media destruction policy and verify it covers all media with cardholder data. **9.10.b** Additionally perform the following:			
9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials	**9.10.1.a** Verify that hard-copy materials are cross cut shredded, incinerated, or pulped , in accordance with ISO 9564-1 or ISO 11568-3. **9.10.1.b** Observe storage containers for information to be destroyed to verify that containers are secured. For example, verify that a 'to be shredded' container has a lock preventing access to the contents.			
9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.	**9.10.2** Verify that electronic media is destroyed beyond recovery by using a military wipe program to delete files, or via degaussing or otherwise physically destroying the media.			

Regularly Monitor and Test Networks

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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 when 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 those with administrative privileges such as root) to an individual user.	**10.1** Verify, via observation and inquiry of the system administrator, that audit trails are enabled and active, including for any connected wireless networks.			
10.2 Implement automated audit trails to reconstruct the following events, for all system components:	**10.2** Confirm though inquiry, review of audit logs, and review of audit log settings for *(insert as-of dates)* for the samples of *(insert number and/or description of sample)* system components, that the following events are logged:			
10.2.1 All individual accesses to cardholder data.	**10.2.1** Logging of access to cardholder data			
10.2.2 All actions taken by any individual with root or administrative privileges.	**10.2.2** Logging of actions taken by any individual with root or administrative privileges			
10.2.3 Access to all audit trails.	**10.2.3** Logging of access to all audit trails			
10.2.4 Invalid logical access attempts.	**10.2.4** Logging of invalid logical access attempts			
10.2 5 Use of identification and authentication mechanisms.	**10.2.5** Logging of use of identification and authentication mechanisms			
10.2.6 Initialization of the audit logs.	**10.2.6** Logging of initialization of audit logs			
10.2.7 Creation and deletion of system-level objects.	**10.2.7** Logging of 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** Confirm through inquiry and observation, for each auditable event mentioned at 10.2 above, that the audit trail captures the following information:			

Regularly Monitor and Test Networks

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
10.3.1 User identification	**10.3.1** User identification			
10.3.2 Type of event	**10.3.2** Type of event			
10.3.3 Date and time	**10.3.3** Date and time stamp			
10.3.4 Success or failure indication	**10.3.4** Success or failure indication, including those for wireless connections.			
10.3.5 Origination of event	**10.3.5** Origination of event			
10.3.6 Identity or name of affected data, system component, or resource	**10.3.6** Identity or name of affected data, system component, or resources			

Regularly Monitor and Test Networks

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
10.4 Synchronize all critical system clocks and times.	**10.4** Obtain and review the process for getting and distributing the correct time within the organization. Also obtain and review related system parameter settings for the sample of *(insert number and/or description of sample)* system components. Verify the following is included in the process and implemented: • NTP or similar technology is used for time synchronization. • Two or three central time servers within the organization receive external time signals (directly from a special radio, GPS satellites, or other external sources - based on International Atomic Time and UTC (formerly GMT)), peer with each other to keep accurate time, and share the time with other internal servers (i.e., internal servers should not be all be receiving time signals from external sources). • NTP is running the most recent version. • Specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information			
10.5 Secure audit trails so they cannot be altered in any way, including the following:	**10.5** Verify the following via inquiry of the system administrator and review of file permissions:			

Regularly Monitor and Test Networks

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Only individuals who have a job-related need can view audit trail files.			
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.			
10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Current audit trail files are promptly backed up 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.	**10.5.4** Offload or copy logs for wireless networks onto a centralized internal log server or media that is difficult to alter.			
10.5.5 Use file integrity monitoring/change detection software (such a 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).	**10.5.5** Verify the use of file integrity monitoring or change detection software for logs by observing system settings and monitored files, as well as results from monitoring activities.			
10.6 Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like IDS and authentication (AAA) servers.	**10.6.a** Obtain security policies and procedures and determine that they include procedures to review security logs at least daily, and that follow-up to exceptions is required. **10.6.b** Through observation and interviews, determine that regular log reviews are performed for all system components.			

Regularly Monitor and Test Networks

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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 three months available online.*	**10.7.a** Obtain security policies and procedures and determine that they include audit log retention policies and require audit log retention for at least one year. **10.7.b** For the sample of (*insert number and/or description of sample)* system components, verify that audit logs are available online or on tape for at least one year.			
Requirement 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.	**11.1.a** Confirm through inquiry of security personnel that periodic security testing of the devices within the cardholder environment occurs. **11.1.b** Verify that a wireless analyzer is used periodically to identify all wireless devices in use. **11.1.c** For **Service Providers** only, examine relevant code, documentation, and processes to verify that velocity checks and other transaction trend data are monitored in real-time and collected to detect fraudulent transaction attempts.			

Regularly Monitor and Test Networks

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., 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.*	**11.2.a** Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs. Confirm the scan process includes rescans until "clean" results are obtained. **11.2.b** To verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, inspect output from the four most recent quarters of external vulnerability scans to verify the following: • Four quarterly scans occurred in the most recent 12-month period. • The results of each scan satisfy the PCI Security Scanning Procedures (e.g., no urgent, critical, or high vulnerabilities. • The scans were completed by a vendor approved to perform the PCI Security Scanning Procedures.			
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 (e.g., operating system upgrade, sub-network added to environment, web server added to environment).	**11.3** Obtain results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Confirm that any noted vulnerabilities were corrected.			

Regularly Monitor and Test Networks

REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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.	**11.4** Observe the use of network intrusion detection and/or prevention software on the network. Confirm IDS and/or IPS is in place to monitor and alert personnel of suspected compromises. Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.			
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*	**11.5** Verify the use of file integrity monitoring products by observing system settings and monitored files, as well as reviewing results from monitoring activities.			

Maintain an Information Security Policy

<table>
<tr>
<td colspan="5">Requirement 12: Maintain a policy that addresses information security for employees and contractors.
<i>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.</i></td>
</tr>
<tr>
<td>12.1 Establish, publish, maintain, and disseminate a security policy that:</td>
<td>12.1 Read the information security policy, and verify the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners). Also verify that:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.1.1 Addresses all requirements in this specification.</td>
<td>12.1.1 The policy addresses all requirements in this specification.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.</td>
<td>12.1.2 The information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.1.3 Includes a review at least once a year and updates when the environment changes.</td>
<td>12.1.3 The information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.2 Develop daily operational security procedures that are consistent with the requirements in this specification (e.g., user account maintenance procedures, log review procedures).</td>
<td>12.2.a Review the daily operational security procedures. Verify they are consistent with this specification, and include administrative and technical procedures for each of the requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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:</td>
<td>12.3 Obtain and examine the modem usage policy and verify that it specifies and/or requires:</td>
<td></td>
<td></td>
<td></td>
</tr>
</table>

Maintain an Information Security Policy

12.3.1 Explicit management approval	**12.3.1** Explicit management approval to use the devices.			
12.3.2 Authentication for use of the technology	**12.3.2** All device use is authenticated with username and password or other authentication item (e.g., token).			
12.3.3 A list of all such devices and personnel with access	**12.3.3** A list of all devices and personnel authorized to used the devices			
12.3.4 Labeling of devices with owner, contact information, and purpose	**12.3.4** Labeling of devices with owner, contact information, and purpose.			
12.3.5 Acceptable uses of the technology	**12.3.5** Acceptable uses for the technology.			
12.3.6 Acceptable network locations for these technologies	**12.3.6** Acceptable network locations for the technology.			
12.3.7 A list of company-approved products	**12.3.7** A list of company-approved products.			
12.3.8 Automatic disconnect of modem sessions after a specific period of inactivity	**12.3.8** 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.	**12.3.9** Activation of modems used by 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.	**12.3.10** Disabling storage of cardholder data onto local hard drives, floppy disks or other external media when accessing such data remotely via modem. Also disabling of cut-and-paste, and print functions during remote access.			

Maintain an Information Security Policy

12.4 Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.	**12.4** Verify that information security policies clearly define information security responsibilities for both employees and contractors.			
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			
12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Creating and distributing security policies and procedures is formally assigned.			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Monitoring and analyzing security alerts, and distributing information to appropriate information security and business unit management personnel, is formally assigned.			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**12.5.3** Creating and distributing security incident response and escalation procedures is formally assigned.			
12.5.4 Administer user account and authentication management, including additions, deletions, and modifications.	**12.5.4** Administering user account and authentication management is formally assigned.			
12.5.5 Monitor and control all access to data.	**12.5.5** Monitoring and controlling all access to data is formally assigned.			
12.6 Make all employees aware of the importance of cardholder information security:	**12.6** Obtain security awareness program documentation, and verify that it contains the following components:			

Maintain an Information Security Policy

12.6.1 Educate employees (e.g., through posters, letters, memos, meetings, and promotions).	**12.6.1** Multiple methods of communicating awareness and educating employees (posters, letters, meetings, etc.).			
12.6.2 Require employees to acknowledge in writing they have read and understood the company's security policy and procedures.	**12.6.2** Requirement for employees to acknowledge in writing that they have read and understood the company's information security policy.			
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.*	**12.7** Inquire of Human Resource department management and determine that there is a process in place to perform background checks on potential employees who will have access to systems, networks, or cardholder data. These background checks should include pre-employment, criminal, credit history, and reference checks.			
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** Obtain contracts between the organization and any 3rd parties that handle cardholder data (e.g., backup tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes). Verify that the PCI Data Security Standard requirements relevant to the business relationship between the organization and the 3rd party are included in the contract. Specifically verify the following information is included in the contract:			
12.8.1 Acknowledgement that the 3rd party is responsible for security of cardholder data in their possession.	**12.8.1** Contract provisions include acknowledgement by the 3rd party of their responsibility for securing cardholder data.			

Maintain an Information Security Policy

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 uses specifically required by law.	**12.8.2** Contract provisions include ownership and acceptable uses of cardholder data.			
12.8.3 Business continuity in the event of a major disruption, disaster or failure.	**12.8.3** Contract provisions include appropriate business continuity provided by the 3rd party such that the 3rd party's services will be available in the event of a major disruption 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 Data Security Standards for protecting cardholder data.	**12.8.4** Contract provisions allow for audits by Visa or Visa-approved entities in the event of a cardholder data compromise.			
12.8.5 Termination provision that ensures that 3rd party will continue to treat cardholder data as confidential.	**12.8.5** Contract provisions require continued security of cardholder data during and after contract terminations.			

Maintain an Information Security Policy

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain the Incident Response Plan and related procedures, examine the documents and perform the following:			
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 (e.g., informing Acquirers and credit card associations).	**12.9.1** Verify that the Incident Response Plan and related procedures includes: • Roles, responsibilities, and communication strategies in the event of a compromise • Coverage and responses for all critical system components • Notification, at a minimum, of credit card associations and Acquirers • Strategy for business continuity post compromise • Reference or inclusion of incident response procedures from card associations. • Analysis of legal requirements for reporting compromises (e.g., per California bill 1386, notification of affected consumers is a requirement in the event of an actual or suspected compromise, for any business with California residents in their database).			
12.9.2 Test the plan at least annually.	**12.9.2** Testing of the plan at least annually			
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to compromise alerts.	**12.9.3** Verify via observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.			
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	**12.9.4** Verify via observation and review of policies, that staff with security breach responsibilities are periodically trained..			

Maintain an Information Security Policy

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	**12.9.5** Verify via observation and review of processes, that monitoring and responding to alerts from security systems is included in the Incident Response Plan.			
12.9.6 Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.9.6** Verify via observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			