Visa U.S.A. Cardholder Information Security Program

Self-Assessment Questionnaire

for

Level 3 Merchants

Table of Contents

Who Should Complete This Self-Assessment Questionnaire

Level 3 Merchants should complete this questionnaire.

Merchants	Qualification
Level 1	Stores, processes or transmits more than 6 million transactions
Level 2	Stores, processes or transmits between 500 thousand and 6 million transactions
Level 3	Stores, processes or transmits fewer than 500 thousand transactions
Service Providers	**Qualification**
Level 1	All VisaNet Processors (Member and Nonmember) and all Payment Gateways
Level 2	Any Service Providers that is not in Level 1 and stores, processes, or transmits more than 1 million Visa accounts/transactions annually
Level 3	Any Service Providers that is not in Level 1 and stores, processes, or transmits less than 1 million Visa accounts/transactions annually

How to Complete the Questionnaire

The questionnaire is divided into six sections. Each section focuses on a specific area of security, based on the requirements included in this document. Within each section, symbols identify individual questions indicating the criticality of each requirement.

This Symbol…	Identifies …
R	A critical security **R**equirement. If this requirement is not followed, cardholder data may be at risk.
BP	A security **B**est **P**ractice. Visa recommends this practice to reduce the risk that cardholder data will be compromised.

Rating Each Section

After completing each section of the assessment, users should fill in the rating boxes as follows:

In each section IF…	THEN, the section rating is …
ALL questions identified with R or BP are answered with “yes”	**Green** - The merchant or service provider is compliant with the self-assessment portion of the CISP assessment.
ALL questions identified with R are answered with “yes” but some questions identified with BP are answered with “no”	**Yellow** – Although the merchant or service provider has achieved compliance with the self-assessment portion of the CISP assessment, there are security risks that need examination.
ANY questions identified with R are answered with “no”	**Red** – The merchant or service provider is not considered compliant. To reach compliance, the risk(s) must be resolved and the self-assessment must be retaken to demonstrate compliance.

Rating the Entire Assessment

After completing the entire assessment, users should determine their overall rating as follows:

IF…	THEN the overall rating is…
All sections register a "Green" rating	Green
One or more sections register a "Yellow" rating	Yellow
One or more sections register a "Red" rating	Red

Questionnaire and Scan Reporting

Level 3 Merchants must submit the completed self-assessment questionnaire to their Acquirer. Acquirers may also require System Perimeter Scans. If System Perimeter Scans are required, Level 3 Merchants should submit the scan results to their Acquirer.

The following must be included with the self-assessment questionnaire:

Organization Information

CORPORATE NAME: DBA(S):

CONTACT NAME:

PHONE: E-MAIL:

APPROXIMATE NUMBER OF VISA TRANSACTIONS/ACCOUNTS HANDLED PER YEAR:

PLEASE INCLUDE A BRIEF DESCRIPTION OF YOUR BUSINESS.
Please explain your business' role in the payment flow. How and in what capacity does your business store, process and/or transmit cardholder data?

PLEASE CIRCLE ALL THAT APPLY TO YOUR MANAGEMENT OF CARDHOLDER INFORMATION:

My servers at my site Co-located at a data center Hosted by another company

NAMES OF ALL THIRD PARTY SERVICE PROVIDERS (i.e. Processor, Web Hosting, Shopping Cart, Payment Gateway, Co-Location, Data Storage, Point of Sale Software):

Questionnaire Ratings			
Section 1:	Green	Yellow	Red
Section 2:	Green	Yellow	Red
Section 3:	Green	Yellow	Red
Section 4:	Green	Yellow	Red
Section 5:	Green	Yellow	Red
Section 6:	Green	Yellow	Red
Overall Rating:	Green	Yellow	Red

System Perimeter Scan Results (If required by Level 3 Merchant Acquirer)

Visa does not require submission of detailed scan results. However, detailed quarterly scan results must be available to Visa upon request.

Confirmation of passing scan(s) must be provided as follows:

- For Level 1 Merchants and Level 1 & 2 Service Providers, confirmation of passing scan(s) must be submitted to Visa with the Report On Compliance on an annual basis.
- For all Merchants, confirmation of passing scan(s) must be submitted to the merchant's Acquirer on a quarterly basis.
- For Level 3 Service Providers, confirmation of passing scan(s) must be submitted to Visa with the self-assessment questionnaire on an annual basis.

An entity will obtain a passing grade if there are no URGENT, CRITICAL, or HIGH-risk vulnerabilities identified.

The scan results must be accompanied by the following information:

BRIEFLY DESCRIBE YOUR NETWORK TOPOLOGY OR INCLUDE A HIGH-LEVEL NETWORK DIAGRAM. FOR EXAMPLE, THIS MAY INCLUDE THE FOLLOWING:

- Connections to the Internet indicating devices to be scanned
- All systems that store, process or transmit cardholder data
- All physical locations (provide a separate map for each location if necessary)
- Brief description of any mechanisms used for securing these systems (internal or external firewalls, antivirus, IDS, etc.)

□ Check here to indicate that all *Company Name* 's external IP addresses have been provided to the scan vendor to be scanned.

Questionnaire

Section 1: Security Management

		Description	Response	
1.1	BP	Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	□ Yes	□ No
1.2	BP	Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	□ Yes	□ No
1.3	BP	Is there an up-to-date information security awareness and training program in place for all system users?	□ Yes	□ No
1.4	BP	Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	□ Yes	□ No
1.5	R	Have the roles and responsibilities for information security been clearly defined within the company?	□ Yes	□ No
1.6	BP	Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	□ Yes	□ No
1.7	R	Is sensitive cardholder data securely disposed of when no longer needed?	□ Yes	□ No

Section 2: Access Control

		Description	Response	
2.1	R	Are all access control logs regularly reviewed and do they contain both successful and unsuccessful login attempts, access to audit logs, and root/administration access?	☐ Yes	☐ No
2.2	R	Does access control for customers require username and password authentication?	☐ Yes	☐ No
2.3	R	Does each non-consumer user have an individual username and password that is not shared with any other user?	☐ Yes	☐ No
2.4	BP	Are non-consumer users who have access to cardholder data in payment processing platforms required to use Secure ID card or some other two-factor or token base authentication method?	☐ Yes	☐ No
2.5	R	Is access to payment card account numbers restricted for users on a need-to-know basis?	☐ Yes	☐ No
2.6	R	Are maintenance accounts and remote support access controls enabled only during the time needed?	☐ Yes	☐ No
2.7	R	Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords?	☐ Yes	☐ No
2.8	R	Are non-consumer users required to change their passwords on a pre-defined regular basis?	☐ Yes	☐ No
2.9	R	Are all passwords on network devices and systems encrypted?	☐ Yes	☐ No
2.10	R	Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?	☐ Yes	☐ No
2.11	R	Are privileged and administrative accounts strictly controlled?	☐ Yes	☐ No
2.12	BP	Are password-protected screen-savers used on systems and consoles that provide access to cardholder data and critical systems?	☐ Yes	☐ No
2.13	R	When an employee leaves the company, are that employee’s user account and password immediately revoked?	☐ Yes	☐ No
2.14	R	Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?	☐ Yes	☐ No
2.15	R	Are accounts that are not used for a lengthy amount of time (“sleeping” accounts) automatically disabled in the system after a pre-defined period?	☐ Yes	☐ No
2.16	R	Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?	☐ Yes	☐ No

Section 3: Operational Security

		Description	Response	
3.1	R	Are security incidents reported to the person responsible for security investigation?	☐ Yes	☐ No
3.2	BP	Is a penetration test performed on critical infrastructure at least annually?	☐ Yes	☐ No
3.3	R	Are audit logs regularly reviewed, backed up, secured, and retained for at least six months on all critical systems?	☐ Yes	☐ No
3.4	R	Are account numbers sanitized before being logged in the audit log?	☐ Yes	☐ No
3.5	R	Is encryption used in the transmission of account numbers via e-mail?	☐ Yes	☐ No
3.6	R	Are secure, encrypted communications used for remote administration of production systems and applications?	☐ Yes	☐ No
3.7	R	If the network is remotely accessed by employees, administrators, or third parties, is remote access control software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on?		
3.8	R	Are vendor default security settings changed on production systems before taking the system into production?	☐ Yes	☐ No
3.9	R	Are all production systems hardened by removing all unnecessary tools and services installed by the default configuration?	☐ Yes	☐ No
3.10	R	Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	☐ Yes	☐ No
3.11	R	Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?	☐ Yes	☐ No
3.12	R	Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?	☐ Yes	☐ No
3.13	R	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?	☐ Yes	☐ No
3.14	BP	Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?	☐ Yes	☐ No
3.15	R	Are all critical system clocks and times synchronized, and do logs include data and time stamp?	☐ Yes	☐ No

Section 4: Application and System Development

		Description	Response	
4.1	R	Were the Open Web Application Security Project group (www.owasp.org) guidelines taken into account in the development of Web applications?	☐ Yes	☐ No
4.2	R	If production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage?	☐ Yes	☐ No
4.3	R	Are all but the last four digits of the account number masked when displaying cardholder data?	☐ Yes	☐ No
4.4	R	Are account numbers in databases and in backup media stored securely—for example, by means of encryption or truncation?	☐ Yes	☐ No
4.5	R	Is it prohibited to store CVC2/CVV2 or magnetic stripe data in the database, log files, or point-of-sale products?	☐ Yes	☐ No
4.6	BP	Is sensitive cardholder data stored in databases encrypted with sufficient-strength keys, such as 128-bit triple DES or other strong algorithms based on industry standards?	☐ Yes	☐ No
4.7	R	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	☐ Yes	☐ No
4.8	R	When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?	☐ Yes	☐ No
4.9	R	Are cookies secured or encrypted?	☐ Yes	☐ No

Section 5: Network Security

		Description	Response	
5.1	R	Are the router and firewall configurations secured and do they conform to documented security standards?	☐ Yes	☐ No
5.2	R	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	☐ Yes	☐ No
5.3	R	If routers and other network devices are configured remotely, is a secure communications protocol used to protect the communication channel from eavesdropping?	☐ Yes	☐ No
5.4	R	Are routers configured to drop any unauthorized packets?	☐ Yes	☐ No
5.5	R	Are the router logs regularly reviewed for unauthorized traffic?	☐ Yes	☐ No
5.6	R	Are routers configured to prevent remote probing?	☐ Yes	☐ No
5.7	R	Is a firewall used to protect the network and limit traffic required for business?	☐ Yes	☐ No
5.8	R	Are firewall logs regularly reviewed?	☐ Yes	☐ No
5.9	R	Are Web servers located on a public reachable network segment (DMZ) separated from the internal network by a firewall?	☐ Yes	☐ No
5.10	R	Is payment card account information stored in a database located on the internal network and protected by a firewall?	☐ Yes	☐ No
5.11	R	Is the firewall configured to translate the IP addresses used on the Internet to different internal IP addresses (for example, using network address translation [NAT])?	☐ Yes	☐ No
5.12	R	Do the network router and firewall configurations prevent network-mapping from the outside (such as ping or trace route)?	☐ Yes	☐ No
5.13	R	Are all Internet-accessible hosts (for example, the firewall, the Web server, and the router) updated and patched for security vulnerabilities?	☐ Yes	☐ No
5.14	R	Are transmissions of sensitive cardholder data encrypted through the use of SSL or other industry acceptable methods?	☐ Yes	☐ No
5.15	R	If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?	☐ Yes	☐ No
5.16	R	If wireless access is used, is the communication encrypted?	☐ Yes	☐ No
5.17	R	If wireless access is used, is the access to the network limited to authorized devices?	☐ Yes	☐ No
5.18	BP	Are modems configured to allow only dial-out connections?	☐ Yes	☐ No

Section 6: Physical Security

		Description	Response	
6.1	R	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?	□ Yes	□ No
6.2	R	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?	□ Yes	□ No
6.3	R	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?	□ Yes	□ No
6.4	R	Is all cardholder data printed on paper or received by fax adequately protected against unauthorized access?	□ Yes	□ No

This concludes the questionnaire.

Appendix A: Detailed CISP Requirements

Requirement 1: Install and maintain a working firewall to protect data. *(Importance: 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 a formal process for approving all external network connections.

1.2 Build a firewall that will:

1.2.1 Deny all traffic from "untrusted" networks/hosts, **except for**:

- Web protocols –HTTP – port 80 and Secure Sockets Layer (SSL) – typically port 443.
- System administration protocols (e.g., Secure Shell (SSH) or Virtual Private Network (VPN).
- Other protocols required by the business (e.g., ISO 8583).

1.2.2 Restrict connections between publicly accessible servers and any component storing cardholder data, including any connections from wireless networks. The firewall configuration must deny all traffic **except for** protocols required by the business.

1.2.3 Prohibit an external network direct public access to any system component that is storing cardholder information (i.e., databases).

1.3 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).

1.4 Monitor your firewall Central Processing Unit (CPU) load and up/down status with reasonable regularity (at least every 15 minutes).

Requirement 2: Keep security patches up-to-date. *(Importance: Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. These vulnerabilities are fixed via security patches from vendors, and all systems need to have current software patches to protect systems against exploitation by employees, external hackers, and viruses.)*

2.1 Make sure all systems and software have the latest vendor-supplied security patches.

2.1.1 Keep up with vendor changes and enhancements to security patches.

2.1.2 Install new/modified security patches within one month of release.

2.2 Test all security patches before they are deployed.

2.3 Follow change control procedures for system and software configuration.

Requirement 3: Protect Stored Data *(Importance: 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.)*

3.1 Keep cardholder information storage to a minimum. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.

3.2 Verify that cardholder information is disposed of in accordance with company policies.

3.3 Do not store sensitive authentication data (including Magnetic Stripe (CVV) data, CVV2 data, PINs, and Verified by Visa passwords) subsequent to a transaction authorization.

3.4 Encrypt all passwords

3.5 Mask account numbers when displayed to customers or other external parties.

3.6 Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media and in logs) 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 or AES with associated key management processes and procedures.

The MINIMUM account information that needs to be encrypted is the payment card account number. Magnetic Stripe data (Track 1 & Track 2/CVV) and CVV2 data must not be retained in any zone.

Payment card account numbers must NEVER be stored on a server connected to the Internet (i.e. in the DMZ).

3.7 Implement a cryptographic solution that is isolated so that secret data cannot be disclosed.

3.8 Protect encryption keys against both disclosure and misuse:

3.8.1 Restrict access to keys to the fewest number of custodians necessary.

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

3.9 Fully document all key management processes and procedures.

Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks. *(Importance: Sensitive information should 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. Sensitive information includes credit card numbers and passwords.)*

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

4.2 Never send cardholder information via unencrypted e-mail.

4.3 Encrypt non-console administrative access. Use technologies such as SSH or VPN.

Requirement 5: Use and regularly update anti-virus software or programs. (*Importance: Many vulnerabilities and malicious viruses enter the network via employees' email activities. Anti-virus software should be used on all email systems and desktops to protect all systems from such malicious software)*

5.1 Deploy anti-virus mechanisms on all Windows-based systems.

5.2 Keep all anti-virus mechanisms current and actively running. Make sure they are capable of generating audit logs.

Requirement 6: Restrict access to data by business need-to-know. (*Importance: This ensures critical data can only be accessed in an authorized manner.)*

6.1 Develop a data control policy. Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

6.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know.

Requirement 7: Assign a unique ID to each person with computer access*. (Importance: This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.)*

7.1 Uniquely identify all users before allowing them to access system resources or cardholder information.

7.2 Employ at least one of the methods below to authenticate all internal users:

- Unique user name and password
- Token devices (i.e., Secured, certificates, or public key)
- Biometrics

7.3 Implement two-factor authentication for remote access to the network. Use technologies such as RADIUS or TACACS with tokens.

7.4 Ensure proper user authentication and password management for non-consumer users:

7.4.1 Control the addition, deletion, and modification of user IDs, credentials, or other identifier objects.
7.4.2 Immediately revoke accesses of terminated users.
7.4.3 Remove inactive user accounts at least every 90 days.
7.4.4 Distribute password procedures and policies to all users who have access to cardholder information.
7.4.5 Do not permit group passwords.
7.4.6 Change user passwords at least every 90 days.
7.4.7 Require a minimum password length of at least seven characters.
7.4.8 Use passwords containing both numeric and alphabetic characters.
7.4.9 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.
7.4.10 Monitor system access attempts. Limit repeated attempts by locking out the user ID after not more than six attempts.
7.4.11 Set the lockout duration to thirty minutes or until administrator enables the user ID.
7.4.12 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.
7.4.13 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.

Requirement 8: Do not use vendor-supplied defaults for system passwords and other security parameters*.* *(Importance: 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.)*

8.1 Always change the vendor-supplied defaults **before** you install a system on the network (i.e., passwords, SNMP community strings, unnecessary accounts, etc.).

8.2 Develop system configuration standards for all networks components. Make sure these standards address all known security vulnerabilities and industry best practices.
8.2.1 Implement only one application or primary function per network component (i.e., one application per server).
8.2.2 Disable all unnecessary services
8.2.3 Configure system security parameters to prevent misuse.
8.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (e.g., unnecessary web servers).
Network components include, but are not limited to servers, routers, switches, and firewalls.

8.3 Encrypt internal non-console administrative access. Use technologies such as SSH or VPN.

8.4 Establish a process to identify newly discovered security vulnerabilities. Update your standards to address new vulnerability issues.

Requirement 9: Track all user access to data by a unique ID. *(Importance: 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.)*

9.1 Establish a process for linking all data access activities (especially those with root or administrative privileges) to an individual user or system.

9.2 Implement automated audit trails to reconstruct the following events:
9.2.1 All accesses to cardholder data
9.2.2 All actions taken by any individual with root or administrative privileges
9.2.3 Access to all audit trails
9.2.4 Invalid logical access attempts
9.2 5 Use of identification and authentication mechanisms
9.2.6 Initialization of the audit logs
9.2.7 Creation and deletion of system level objects

9.3 Record the following audit trail entries for each event:
9.3.1 User identification
9.3.2 Type of event
9.3.3 Date and time
9.3.4 Success or failure indication
9.3.5 Origination of event
9.3.6 Identity or name of affected data, system component, or resource

9.4 Secure audit trails so they cannot be altered in any way.

9.5 Review security, firewall, and server logs at least daily.

9.6 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 2 years or more.

Requirement 10: Regularly test security systems and processes. *(Importance: 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. Additionally, elements a company relies on during an emergency, such as disaster recovery plans and incident response plans, should be tested to ensure they work as expected.)*

10.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts.

10.2 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).

10.3 Software and application development is based on industry best practices and information security is included throughout the software development life cycle.

10.3.1 Before promoting custom application code to the production site, review it carefully to identify any potential coding vulnerability.

10.3.2 Development of web software and applications is based on the Open Web Application Security Project guidelines (www.owasp.org).

10.4 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, etc.).

10.5 Use network intrusion detection systems to monitor all network traffic and alert personnel to suspected compromises.

10.5.1 Designate specific personnel to be available on a 24/7 basis to respond to compromise alerts.

10.6 Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files.

10.6.1 Designate specific personnel to be available on a 24/7 basis to respond to reports of unauthorized critical system or content file changes.

10.6.2 Perform critical files 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.

10.7 Be prepared to respond immediately to a system breach.

10.7.1 Create an incident response plan to be used in the event of system compromise. Make sure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, roles and responsibilities, and communication and contact strategies (e.g., informing Acquirers and credit card associations.).

10.7.2 Test the plan at least annually.

10.7.3 Provide appropriate training to staff with security breach response responsibilities.

10.8 Make sure media is backed up nightly to adequately facilitate recovery. Store media back-ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.

Requirement 11: Maintain a policy that addresses information security for employees and contractors. *(Importance: 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.)*

11.1 Establish and publish a security policy that:

11.1.1 Addresses all requirements in this specification.

11.1.2 Reflects your organization's business objectives and risk control standards

11.2 Develop daily operational security procedures that are consistent with requirements in this specification.

11.3 Make sure your security policy and procedures clearly define information security responsibilities for all employees and contractors.

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

11.4.1 Establish, document, and distribute security policies and procedures.

11.4.2 Monitor and analyze security alerts and information and distribute to appropriate personnel.

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

11.4.4 Administer user account and authentication management, including additions, deletions, and modifications resulting from user changes and terminations.

11.4.5 Monitor and control all access to data.

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

11.5.1 Educate employees through posters, letters, memos, meetings, promotions, etc.

11.5.2 Require employees to acknowledge in writing they have read and understood your company's security policy and procedures.

11.6 Screen all 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.

11.7 Contractually require all associated 3rd parties with access to cardholder data to adhere to requirements in this specification. At a minimum, the agreement should ensure that 3rd parties are responsible for security of cardholder information, and that 3rd parties are aware of their responsibility for being compliant with requirements in this specification.

Requirement 12: Restrict physical access to cardholder data. *(Importance: Any physical access to data or systems that house cardholder data allows the opportunity to access or access data, or remove systems or hardcopies, and should be appropriately restricted.)*

12.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store or process cardholder data

12.2 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 more than one day.

12.3 Make sure all visitors are:

- **12.3.1** Authorized before entering areas where cardholder data is processed or maintained.
- **12.3.2** Given a physical token (e.g., badge or access device) that identifies them as non-employees containing a fixed expiration date.
- **12.3.3** Asked to surrender the physical token before leaving the facility or at the date of expiration.

12.4 Use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months.

12.5 Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, faxes, etc.) that contain cardholder information.

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

- **12.6.1** Label the media as "confidential".
- **12.6.2** Send the media via secured courier or a delivery mechanism that can be accurately tracked.

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

12.8 Maintain strict control over the storage and accessibility of media that contains cardholder information:

- **12.8.1** Properly inventory all media and make sure it is securely stored.
- **12.8.2** Implement data retention and disposal policies and procedures for all media containing cardholder information.

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

- **12.9.1** Shred or incinerate hardcopy materials
- **12.9.2** Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Appendix B: Glossary

Term	Definition
Access control	Measures that limit access to information or information processing resources to those authorized persons or applications.
Account harvesting	A method to determine existing user accounts based on trial and error. Giving too much information in an error message can disclose information that makes it easier for an attacker to penetrate or compromise the system.
Account number	The payment card number (credit or debit) that identifies the issuer and the particular cardholder account.
Acquirer	A bankcard association member that initiates and maintains relationships with merchants that accept Visa or MasterCard cards.
Asset	Information or information processing resources of an organization.
Audit Log	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Sometimes specifically referred to as a security audit trail.
Authentication	The process of verifying identity of a subject or process.
Authorization	The granting of access or other rights to a user, program, or process
Backup	A duplicate copy of data made for archiving purposes or for protecting against damage or loss.
Cardholder	The customer to whom a card has been issued or the individual authorized to use the card.
Cardholder data	All personally identifiable data about the cardholder and relationship to the Member (i.e., account number, expiration date, data provided by the Member, other electronic data gathered by the merchant/agent, and so on). This term also accounts for other personal insights gathered about the cardholder ‘i.e., addresses, telephone numbers, and so on).
Compromise	An intrusion into a computer system where unauthorized disclosure, modification, or destruction of cardholder data may have occurred.
Console	A screen and keyboard which allows access and control of the server / mainframe in a networked environment.
Consumer	Individual purchasing goods and /or services.
Cookies	A string of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information.
CVC2	3-digit Card Validation Code printed on the back of a MasterCard payment card, used to verify e-commerce transactions.

Term	Definition
CVV2	3-digit Card Verification Value printed on the back of a Visa payment card, used to verify e-commerce transactions.
Database	A structured format for organizing and maintaining information that can be easily retrieved. A simple example of a database is a table or a spreadsheet.
Default accounts	A system login account that has been predefined in a manufactured system to permit initial access when the system is first put into service.
Default password	The password on system administration or service accounts when a system is shipped from the manufacturer, usually associated with the default account. Default accounts and passwords are published and well-known.
Dual Control	A method of preserving the integrity of a process by requiring that several individuals independently take some action before certain transactions are completed.
DMZ (de-militarized zone)	A network added between a private network and a public network in order to provide an additional layer of security.
Egress	Traffic leaving the network.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption), against unauthorized disclosure.
Firewall	Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.
Host	The main hardware on which software is resident.
Information Security	Protection of information for confidentiality, integrity and availability.
Ingress	Traffic entering the network.
Intrusion detection Systems	An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
IP address	An IP address is a numeric code that uniquely identifies a particular computer on the Internet.
IP Spoofing	A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
ISO 8583	An established standard for communication between financial systems.
Key	In cryptography, a key is a value applied using an algorithm to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.

Term	Definition
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe used for authorization during a card present transaction. Entities may not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/CVV, and Visa reserved values must be purged; however, account number, expiration date, and name may be extracted and retained.
Monitoring	A view of activity on a network.
Network	A network is two or more computers connected to each other so they can share resources.
Network Address Translation (NAT)	The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.
Non consumer users	Any user, excluding consumer customers, that accesses systems, including but not limited to, employees, administrators, and third parties.
Password	A string of characters that serve as an authenticator of the user.
Patch	A quick-repair job for a piece of programming. During a software product's beta test distribution or try-out period and later after the product is formally released, problems will almost invariably be found. A patch is the immediate solution that is provided to users.
Penetration	The successful act of bypassing the security mechanisms of a system.
System Perimeter Scan	A non-intrusive test which involves probing external-facing systems and reporting on the services available to the external network (i.e. services available to the Internet)
Policy	Organizational-level rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.
Procedure	A procedure provides the descriptive narrative on the policy to which it applies. It is the "how to" of the policy. A procedure tells the organization how a policy is to be carried out.
Protocol	An agreed-upon method of communication used within networks. A specification that describes the rules and procedures products should follow to perform activities on a network.
Risk Analysis	Also known as risk assessment, a process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
Router	A router is a piece of hardware or software that connects two or more networks. A router functions as a sorter and interpreter as it looks at addresses and passes bits of information to their proper destinations. Software routers are sometimes referred to as gateways.
Sanitization	To delete sensitive data from a file, a device, or a system; or modify data so that data is useless for attacks.

Term	Definition
Security Officer	The person who takes primary responsibility for the security related affairs of the organization.
Security policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Sensitive cardholder data	Data whose unauthorized disclosure may be used in fraudulent transaction. It includes, the account number, magnetic stripe data, CVC2/CVV2 and expiration date.
Separation of duties	The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.
Server	A computer that acts as a provider of some service to other computers, such as processing communications, file storage, or printing facility.
SQL injection	A form of attack on a database-driven Web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database.
SSL	An established industry standard that encrypts the channel between a web browser and Web server to ensure the privacy and reliability of data transmitted over this channel.
Tamper-resistance	A system is said to be tamper-resistant if it is difficult to modify or subvert, even for an assailant who has physical access to the system.
Threat	A condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.
Token	A device that performs dynamic authentication.
Transaction data	Data related to an electronic payment.
Truncation	The practice of removing a data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits.
Two-factor authentication	Authentication that requires users to produce two credentials - something they have (e.g., smartcards or hardware tokens), and something they know (e.g., a password). In order to access a system, users must produce both factors.
UserID	A character string that is used to uniquely identify each user of a system.
Virus	A program or a string of code that can replicate itself and cause the modification or destruction of software or data.
Vulnerability	A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.