

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

This guide is designed to assist an independent third-party security firm verify that a select merchant or service provider is in compliance with Visa U.S.A. Cardholder Information Security Program (CISP). Should you have any questions about the following guidelines, contact Visa for clarification before proceeding with the audit or visit <http://www.usa.visa.com/cisp> for more information.

Security Assessment Process

Objectives

1. Protect Visa cardholder information from unauthorized access by verifying that an entity has correctly implemented information security controls.
2. Reduce fraud associated with unauthorized access to Visa cardholder information.
3. Measure a merchant or service provider's level of compliance with the CISP.
4. Identify security issues that could lead to the compromise of Visa cardholder information.

Scope of Assessment

The following will help to assist merchants, service providers and security assessors in determining the scope of the audit.

E-Commerce Environment

CISP validation must be performed on the **e-commerce environment**. The e-commerce environment is defined as any system(s) or system component(s) where Visa cardholder data is retained, stored, or transmitted during the length of the transaction authorization and settlement lifecycle. Refer to sampling note for a list of some of the systems that may be included.

Outsourcing

For those entities that outsource the handling/storing of Visa cardholder data to third-party service providers, the Report On Compliance must document the role of each service provider as it relates to the CISP. Additionally, merchants and service providers must contractually require all associated third parties with access to cardholder data to adhere to CISP data security requirements. Refer to CISP Requirement 11.7 for details.

Sampling

To test the systems within the e-commerce environment, the assessor is to perform sampling. This sample must be representative of all of the types of systems and operating systems in the e-commerce environment. *Each of the three types of samples below need only be chosen once, and then can be re-used whenever referenced in this document.*

Sampling Note: *This document contains numerous references to samples used for testing. These samples are defined here for ease of reference as follows:*

- **Firewalls/routers:** *sample of firewall and router components used to transmit cardholder data. Sample used in Testing Procedures 1, 2, 6, 7, 8, 9.*
- **Database servers:** *sample of database machines that store cardholder data. Sample used in Testing Procedures 2, 3, 5, 6, 7, 8, 9.*
- **Other critical servers:** *sample of all other servers used to process, store, or transmit cardholder data, or which support critical infrastructure for that environment (e.g., web servers, application servers, data transfer servers, data normalization servers, domain name servers (DNS)). Sample used in Testing Procedures 2, 5, 6, 7, 8, 9.*

These samples need only be chosen once and can be re-used as referenced in this document. The samples should be a representative selection of the population, and include a variety of operating systems, functions, and applications, as applicable to the area being reviewed. For example, the reviewer could choose a Sun server running Apache WWW, a NT server running Oracle, a data transfer server running HP-UX, a Linux Server 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.).

Roles and Responsibilities

Within the security assessment process, the following players have major roles and responsibilities:

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Visa

- Develop CISP requirements and Security Audit Procedures (SAP)¹ for assessment of select merchant and service provider environment.
- Review completed Report On Compliance (ROC) and respond to merchant or service provider with a letter of acceptance.
- Follow-up with merchant or service provider and security firm to correct any non-compliance issues and subsequently get into full compliance.
- A list of service providers who have completed the program will be provided to Acquirers.

Acquirer

- Be primary link between Visa and merchant.
- Hold financial responsibility in the Visa system for ensuring merchant's compliance with CISP and other Operating Regulations.
- Follow-up with merchant to correct any non-compliance issues and subsequently get into full compliance.

Select Merchant

- Comply with all provisions of CISP.
- Contractually require all associated third parties with access to cardholder data to adhere to CISP.
- Engage an independent security firm to validate CISP compliance.
- Provide necessary documentation that a security firm requires in order to perform the security assessment process. As part of the security assessment process, the security firm collects information about the organization, contracts, documented security policies and procedures. Note that providing these items in a timely manner helps keep assessment fee at a reasonable level.
- Ensure staff that manages the merchant's security-related functions are available for the security firm during the assessment process.
- Promptly correct any identified security deficiencies.

Service Provider

- Comply with all provisions of CISP.
- Contractually require all associated third parties with access to cardholder data to adhere to CISP.
- Engage an independent security firm to validate CISP compliance.
- Provide necessary documentation that a security firm requires in order to perform the security assessment process. As part of the security assessment process, the security firm collects information about the organization, contracts, documented security policies and procedures. Note that providing these items in a timely manner helps keep assessment fee at a reasonable level.
- Ensure staff that manages the service provider's security-related functions are available for the security firm during the assessment process.
- Promptly correct any identified security deficiencies.

Independent Security Firm

- Conduct an onsite security assessment review based on Visa U.S.A. CISP and SAP.
- Preview the scope of the assessment with merchant or service provider. Typically Visa expects these examinations to include the following:
 1. Gather documentation before interviews, observations and test are to begin.

¹ Visa's testing procedure to validate compliance with the CISP.

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

2. Based on merchant or service provider's environment and Visa's requirements, determine the scope of the assessment. This should also include timeframe of the assessment.
3. If access to a secured environment is necessary during the assessment, security firm must obtain approval from data owner.
4. Schedule interviews with merchant or service provider's staff. Interviewees typically include the individuals who are responsible for contract administration or legal department staff, human resources, information security, network security, physical security, and staff with access to Visa cardholder data.
5. Perform physical examination of technical parameter settings and review supporting documentation.
6. All security firms must describe outline findings utilizing Visa's Report On Compliance (ROC) template below.
7. Follow-up and Consultation – Security Firm must provide consultation to the merchant or service provider to ensure entity fully understands the Report On Compliance report and findings.

Report On Compliance

The Report On Compliance (ROC) must be distributed to Visa, merchant and Acquirer or service provider and is a condition of ongoing Visa card acceptance. Visa will classify the Report as "Visa Secret."² All independent security firms must apply the following report content and format when completing the Report On Compliance (ROC):

1. Executive Summary

Include the following:

- Describe nature of business
- Environment in which the assessment was focused (i.e., client's Internet access points, internal corporate network). **Visa USA requires an assessment to be performed on *selected systems that handle and/or store cardholder information*.**
- Any service provider relationships
- Any wholly-owned entities that require compliance with CISP
- Any international entities that require compliance with CISP
- Any wireless LANs and/or wireless POS terminals

2. Description of Scope of Work and Approach Taken

- Describe the depth to which assessment was performed and a high-level overview of the methodology.
- Timeframe of assessment
- Any specific requests beyond the scope of the Visa Security Audit Procedures (SAP), such as vulnerability scans, penetration test and/or application code review that may have been performed.

3. Findings and Observations

- Describe tests performed other than Visa Security Audit Procedures (SAP) for the requirements.
- Independent security firms must utilize the template beginning on page 5 to provide detailed report findings on each requirements and sub-requirements.

4. Contact Information and Report Date

- Include select merchant or service provider security contact details
- Include professional services firm contact details

² This classification applies to the most sensitive business information, which is intended for use within Visa. Its unauthorized disclosure could seriously and adversely impact Visa, its employees, member banks, business partners, and/or the Brand.

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Definitions

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

- **Requirements** – The Cardholder Information Security Program requirements by which an assessment firm and Visa will validate a merchant or service provider’s CISP compliance.
- **Best Practices** - Recommended processes for an entity to use, in addition to or to enhance required processes. Best practices may become required processes at the discretion of the Security Assessor or Visa, depending on other controls in place and the risk level of the business process.
- **Testing Procedure** – A process to be followed by an independent security audit firm to address individual requirements and testing considerations.
- **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.
- **Target Date/ Comments** –For those controls “Not In Place” include a target date that the merchant or service provider expects to have controls “In Place”. Any additional notes or comments may be included here as well.

Requirements	Best Practices	Testing Procedures	In Place	Not In Place	Target Date/ Comments
Requirement 1: Install and maintain a working firewall to protect data					
1.1 Establish a formal process for approving all external network connections.	<p>A separate DMZ segment may be used for VISA cardholder information.</p> <p>Cardholder information should not be stored longer than is necessary on front-end systems.</p> <p>The DMZ should not be able to talk directly to trusted network. Transactions that need to move from DMZ to internal network should be batched in DMZ and then pulled by internal network from DMZ.</p> <p>Consider network encryption (SSL) between front-end systems and</p>	<p>1.1 Verify that a process requiring written approval for all new network connections is included in a firewall administration policy, and that the firewall administration policy exists, is documented and implemented, and requires the bulleted items below. Verify existence of these items:</p> <ul style="list-style-type: none"> • A current network diagram that documents all connections to Visa cardholder data • Existence of a firewall at each Internet connection and between any DMZ and the Intranet • Description of groups, roles, and responsibilities for logical management of network components • A documented list of services / ports necessary for the business • Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN • Periodic review of firewall/router rule sets • Management approval for external network connections and all other changes to the firewall configuration • Configuration standards for firewalls and routers, including testing of all changes prior to implementation. 			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirements	Best Practices	Testing Procedures	In Place	Not In Place	Target Date/ Comments
<p>1.2 Build a firewall that will:</p> <p><i>Note: Any business protocols outside of the scope of the CISP requirements must be justified and documented in your company policy.</i></p>	<p>back-end databases. This Best Practice may become a requirement at the discretion of the Security Assessor or Visa if the examined entity relies heavily on compensating controls to meet CISP requirements, or engages in more risky business processes (such as processes which recognize the customer, and on subsequent visits, populate transactions with cardholder data when a password is entered).</p> <p>For best-practice security configurations, consider</p>	<p>1.2 Verify firewall/router configurations by reviewing a sample of firewalls/routers (Sampling Note, page 1), for those implemented 1) between the Internet and the DMZ and 2) between the DMZ and the internal network. For example, 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. Inspect network diagrams, firewall rule sets, router configuration settings, etc., as follows:</p>			
<p>1.2.1 Deny all traffic from “untrusted” networks/hosts, except for:</p> <ul style="list-style-type: none"> ▪ Web protocols – The Visa system only allows 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. 	<p>For best-practice security configurations, consider</p>	<p>1.2.1 To determine that inbound and outbound traffic is acceptable and documented, verify that traffic is limited to:</p> <ul style="list-style-type: none"> ▪ Web protocols (HTTP, HTTPS) ▪ System administration/remote access protocols (VPN, SSH) ▪ Other allowed traffic required by the business and documented in the firewall policy. 			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirements	Best Practices	Testing Procedures	In Place	Not In Place	Target Date/ Comments
<p>1.2.2 Restrict connections between publicly accessible servers and any component storing cardholder data. The firewall configuration must deny all traffic except for protocols required by the business.</p>	<p>The Center for Internet Security's benchmark and scoring tool for Cisco IOS routers (www.cisecurity.org), as well as a Top 20 Scanner scan for the FBI/SANS Top 20 Vulnerabilities at (Scanner at www.cisecurity.org, vulnerabilities at www.sans.org/top20)</p>	<p>1.2.2 To determine that connections are restricted between publicly accessible servers and components storing cardholder data, verify the following:</p> <ul style="list-style-type: none"> ▪ Inbound Internet traffic is limited to IP addresses within the DMZ ▪ Inbound and outbound Internet traffic is limited to ports 80 and 443 ▪ Internal addresses cannot pass from the Internet into the DMZ ▪ Only established connections are allowed in, and only if they are associated with a previously established session (run NMAP 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) ▪ Outbound traffic is limited to that which is necessary for the Visa cardholder environment ▪ Running configuration files (e.g., those used for normal running of the routers) and start-up configuration files (those used when machines are re-booted) have the same secure configurations. ▪ All other inbound and outbound traffic not covered in 1.2.1 above is specifically denied. 			
<p>1.2.3 Prohibit an external network direct public access to any system component that is storing cardholder information (i.e., databases).</p>		<p>1.2.3 To determine that direct access between external public networks and components storing cardholder data are prohibited, perform the following, <i>specifically</i> for the firewall/router configuration implemented between the DMZ and the internal network:</p> <ul style="list-style-type: none"> ▪ Verify there is no direct route inbound or outbound for Internet traffic ▪ Verify that internal outbound traffic from cardholder applications can only access IP addresses within the Visa DMZ. 			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirements	Best Practices	Testing Procedures	In Place	Not In Place	Target Date/ Comments
1.3 Implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet. Use technologies such as Port Address Translation (PAT) or Network Address Translation (NAT).		1.3 For firewall components reviewed in 1.2, above, verify that NAT or other technology is used for IP masquerading to restrict broadcast of IP addresses from the internal network to the Internet.			
1.4 Implement 2-factor authentication for remote access to the network. Use technologies such as RADIUS or TACACS with tokens.		1.4 To verify that 2-factor authentication is in place for remote network access, observe an administrator while they connect remotely and verify that both a password and an additional authentication item (Smart card or token PIN, etc.) are requested.			
1.5 Ensure your firewall and router platform:		1.5 <i>Processes in place for Operating System hardening, including for firewalls and routers, are validated under Requirement 8, Testing Procedure 8.2.3.</i>			
1.5.1 Conforms to your organization's system configuration standards.					
1.5.2 Is restricted to only one application or primary function per server.					
1.5.3 Meets or exceeds the minimum hardware and software requirements.					
1.6 Monitor your firewall Central Processing Unit (CPU) load and up/down status with reasonable regularity (at least every 15 minutes).		1.6 Verify that the processes used to ensure continual firewall redundancy and availability include checking for load and up/down status at least every 15 minutes.			
		<i>Processes in place to encrypt non-console administrative access to firewalls and operating systems are validated under Requirement 4, Testing Procedure 4.4.</i> <i>Administrative access controls for network components are validated under Requirement 6, Testing Procedure 6.1.</i>			
Requirement 2: Keep security patches up-to-date.					
2.1 Make sure all "systems and software" have the latest vendor-supplied security patches: <i>Note: "Systems and software" include, but are not limited to: servers, routers, switches, firewalls, operating systems, applications, databases, etc.</i>	Each vendor typically lists recommended security patches on their web site. For example, Microsoft is at www.microsoft.com/security underneath the security bulletins section and Sun	2.1 Using the sample firewalls/routers, database servers, and other critical servers (Sampling Note on page 1), perform the following for each system selected			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirements	Best Practices	Testing Procedures	In Place	Not In Place	Target Date/ Comments
2.1.1 Keep up with vendor changes and enhancements to security patches	<p>is at www.sun.com/bigadmin/patches</p> <p>Production data (including cardholder data) should not be used for testing.</p>	2.1.1 Compare the list of security patches installed on each system to the vendor security patch list to verify that current vendor patches are currently installed.			
2.1.2 Install new/modified security patches within one month of release.		2.1.2 Examine policies related to security patch installation to verify that it is policy to install new security patches within 30 days.			
2.2 Test all security patches before they are deployed.		2.2 Verify the following with the system administrator: <ul style="list-style-type: none"> ▪ Patches are tested in a test environment before being deployed into production. ▪ The test environment is separate from the production environment. ▪ Test procedures are documented. 			
2.3 Follow change control procedures for system and software configuration.		<p>2.3.a Verify that company change-control procedures used to implement security patches and software modifications require the following:</p> <ul style="list-style-type: none"> ▪ Documentation of customer impact ▪ Management sign-off by appropriate parties ▪ Specification of an implementation window ▪ Testing that verifies operational functionality ▪ Back-out procedures. <p>2.3.b Select one web server, one firewall, and one router from sample firewalls/routers, database servers, and other critical servers (Sampling Note on page 1). To verify that change-control procedures are followed, find the three most recent security related updates (e.g., application of security patches) for each system, and trace those updates back to related change control documentation. Verify that this documentation is completed in accordance with company procedures.</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirement 3: Protect stored data					
<p>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.</p>	<p>Not encrypting VISA Cardholder data within the database will require further precautions be taken to ensure confidentiality and integrity of VISA data that is exported out of the database into bulk copies, dumps of the database and backup media.</p> <p><i>Note: If encryption techniques cannot be used, account information must be isolated from the Internet in a separate database that is not resident on systems directly connected to the Internet. Ideally, the database should be resident on back-end computers behind an internal firewall (not in the DMZ). One acceptable practice would be to separate account information from sales data on the Web server and to store the account</i></p>	<p>3.1 Verify that the company has policies and procedures for data retention and disposal, and that these policies and procedures include the following</p> <ul style="list-style-type: none"> ▪ Legal, regulatory, and business requirements for data retention, including specific requirements for retention of VISA cardholder information (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 critical servers and directories that store cardholder data, including database servers, transfer directories and bulk data copy directories used to transfer data between servers, and directories used to normalize data between server transfers. ▪ Performance of an audit, at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements. <p><i>Refer to Requirements 12.6 through 12.10 for storage, maintenance, and destruction requirements for physical media.</i></p>			
<p>3.2 Properly dispose of cardholder information at the end of the required storage retention period.</p>		<p>3.2 Verify that cardholder information is disposed of in accordance with company policies examined in Testing Procedures 3.1, above.</p>			
<p>3.3 Perform a quarterly inventory audit to verify if any stored cardholder information exceeds your retention requirements.</p>		<p>3.3 Verify that, at least quarterly, an audit is performed to ensure no cardholder data exceeds business retention requirements.</p>			
<p>3.4 Do not store Card Verification Value 2 (CVV2) data subsequent to a transaction authorization.</p>		<p>3.4 Review several database schemas from the sample of database servers (Sampling Note, page 1) and verify that fields do not contain CVV2 data.</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>3.5 Implement a mechanism to segregate each merchant's stored cardholder data. <i>This requirement applies to entities that process and/or store cardholder data for multiple merchants. Entities that only store and/or process cardholder data for a single merchant do not need to comply with this requirement.</i></p>	<p><i>information on the mainframe, off-line, or in a secure zone.</i></p> <p>Key Storage and Key Management</p> <ul style="list-style-type: none"> ▪ Do not store private keys or server certificate files in a public place ▪ The best key management is fully automated. 	<p>3.5 Verify, by discussions with database administrators and via inspection of database schemas examined in Testing Procedure 3.4, above, that stored cardholder data is segregated in one of the following ways:</p> <ul style="list-style-type: none"> ▪ In a separate table or database for each merchant, or ▪ Physically or logically isolated between merchant systems. <p><i>If merchant data is not segregated, confirm and document use of adequate compensating controls as documented in Attachment B to the CISP Requirements.</i></p> <p><i>This testing procedure is only for entities that process and/or store cardholder data for multiple merchants.</i></p>			
<p>3.6 Encrypt all passwords</p>	<ul style="list-style-type: none"> ▪ Hardware encryption is more secure than software encryption, especially those that erase the encryption key if the device is tampered with. 	<p>3.6 For critical servers in the cardholder environment, examine password files to verify that passwords are unreadable. Include password files for firewalls, routers, operating systems, applications, databases, and web servers.</p>			
<p>3.7 Render unreadable stored cardholder data by using any of the following approaches:</p> <ul style="list-style-type: none"> ▪ One-way ciphers (hashed indexes), such as SHA-1, but not MD5 ▪ Truncation ▪ Simple ciphers ▪ Index tokens and PADs, with the PADs being securely stored ▪ Strong cryptography, such as Triple-DES, with associated key management processes and procedures. 	<p>Software products may be used depending on circumstances, but hardware devices are preferred.</p> <ul style="list-style-type: none"> ▪ Keys should be randomly generated by an automatic process, where every key is equally likely to be chosen. If keys must be easy-to-remember, make them obscure. ▪ Consider split responsibility for keys such that it requires 2 or 3 people, each knowing only their part of the key, to 	<p>3.7.a Document information about the cryptographic system used to protect stored data, including the vendor, type of cryptographic system, and the encryption algorithms. Verify that data is encrypted using one of the following algorithms:</p> <ul style="list-style-type: none"> • One-way ciphers (hashed indexes), such as SHA-1, but not MD5 • Truncation • Simple ciphers • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES, with associated key management processes and procedures. <p><i>If cardholder data is not encrypted, confirm and document use of adequate compensating controls as documented in Attachment A to the CISP Requirements.</i></p> <p>3.7.b Examine several tables from the sample of database servers (Sampling Note, page 1) to verify the data is encrypted (i.e., not stored in plain text).</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>3.8 Implement a cryptographic solution that:</p>	<p>reconstruct the whole key.</p>	<p>3.8 Review vendor and company documentation for the cryptographic solution to verify existence of documentation and that the solution in place includes the following:</p>			
<p>3.8.1 Is isolated so that secret data cannot be disclosed.</p>	<ul style="list-style-type: none"> ▪ Key-encryption keys should be used to encrypt keys prior to distribution – distribute key-encrypting keys manually and securely. 	<p>3.8.1 Physical or logical isolation to protect secret data.</p>			
<p>3.8.2 Conforms to applicable international and national standards, as well as all legal and regulatory controls.</p>		<p>3.8.2 Adherence to international and national standards as well as legal and regulatory controls.</p>			
<p>3.8.3 Uses only crypto devices that meet the approval standards and policies of your organization.</p>	<ul style="list-style-type: none"> ▪ Use hardware systems with anti-tamper enclosures to store keys, if possible. 	<p>3.8.3 Existence of, and adherence to, organization’s approval standards and policies for use of crypto devices.</p>			
<p>3.9 Protect encryption keys against both disclosure and misuse:</p>	<p>Ideally, a key should never appear unencrypted outside the encryption device.</p>	<p>3.9 Verify that processes to protect encryption keys against disclosure and misuse include the following:</p>			
<p>3.9.1 Restrict access to keys to the fewest number of custodians necessary.</p>	<p>Store keys used to encrypt keys separately from keys used to encrypt data.</p>	<p>3.9.1 Access to cryptographic keys is restricted to very few custodians.</p>			
<p>3.9.2 Store keys securely in the fewest possible locations and forms.</p>	<p>No encryption key should be used for an indefinite period – it should expire automatically.</p>	<p>3.9.2 Storage of cryptographic keys in encrypted format and storage of key-encrypting keys separately from data-encrypting keys.</p>			
<p>3.9.3 Limit the risks associated with shared symmetric keys; only use them for “one-to-one” communication between two entities.</p>	<p>However, keys used to encrypt data files for storage can’t be changed often.</p>	<p>3.9.3 Shared-symmetric keys are only used for one-to-one communication between two entities.</p>			
<p>3.10 Fully document all key management processes and procedures.</p>	<p>Instead, for example, encrypt each file with a unique file key, and then encrypt all file keys with a key-encryption key. The key-encryption key should then be memorized or stored in a secure location.</p>	<p>3.10 Verify the existence of key management procedures, and that these procedures have provisions for the following:</p> <ul style="list-style-type: none"> • Generation of strong keys • Secure key distribution • Secure key storage • Periodic key changes • Destruction of old keys. <p><i>See related Key Management Best Practices at left.</i></p>			
<p>➡ Refer to Attachments A & B to the CISP Requirements: Encrypt Stored Data and Data Segregation Mechanisms for further details.</p>					

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks.					
4.1 Use encryption techniques such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC), etc., to make sensitive data impossible to read during transmission.	Consider network encryption (SSL) between front-end systems and back-end database. This Best Practice may become a requirement at the discretion of the Security Assessor or Visa if the examined entity relies heavily on compensating controls to meet CISP requirements, or engages in more risky business processes (such as recognizing the customer, and on subsequent visits, populating the transactions with cardholder data when a password is entered).	4.1 Verify the use of encryption (e.g., SSL) wherever cardholder data is transmitted or received over the Internet by performing the following: <ul style="list-style-type: none"> For SSL implementations, verify that HTTPS appears as a part of the browser Universal Record Locator (URL) during a transaction, and that no cardholder data was required when HTTPS did not appear in the URL. Select a sample of transactions as they are received from a cardholder or merchant, and observe the transactions as they occur to verify that cardholder data is encrypted during transit. 			
4.2 Never send cardholder information via unencrypted e-mail.		4.2 To verify that cardholder data is not sent via unencrypted email, perform the following: <ul style="list-style-type: none"> Verify existence of a policy stating that VISA cardholder information is not to be sent via unencrypted emails. Verify that email encryption software is provided to employees, and that its use is strongly encouraged. 			
4.3 Implement strong cryptography and appropriate key controls to safeguard data during transmission.		4.3 Verify that at least 128 bit encryption is used during data transmission.			
4.4 Encrypt non-console administrative access. Use technologies such as SSH or VPN.		4.4 For the samples of firewalls/routers database servers, and other critical servers (Sampling Note, pg.1), verify that non-console administrative access is encrypted by: <ul style="list-style-type: none"> Observing administrators as they log on and determining that SSH (or other encryption method) is invoked before the administrator's password is requested. Reviewing services and parameter files to determine that telnet and other remote login commands are not available for use. 			
➡ Refer to CISP Requirement 3.0 for specific actions related to cryptographic solutions and key management.					
Requirement 5: Use and regularly update anti-virus software or programs.					
5.1 Deploy anti-virus mechanisms on all systems.	Use anti-virus mechanisms on all Microsoft OS and Mail gateways involved in	5.1 For the samples of database and other critical servers (Sampling Note, page 1) verify that anti-virus software is installed on the systems.			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>5.2 Keep all anti-virus mechanisms current and actively running. Make sure they are capable of generating audit logs.</p>	<p>the transmission or storage of VISA cardholder data.</p> <p>Anti-virus logs should be kept for a minimum of 6 months or a period equal to your company's standard retention policy.</p>	<p>5.2 To verify that anti-virus software is current, actively running, and capable of generating logs, perform the following:</p> <ul style="list-style-type: none"> • 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 available and enabled and that the logs are being retained in accordance with the company's retention policy. 			
Requirement 6: Restrict access to data by business need-to-know.					
<p>6.1 Develop a data control policy. Limit access to computing resources and cardholder information to only those individuals whose job requires such access.</p>		<p>6.1 Using the sampled firewalls/routers, database servers, and other critical servers (Sampling Note, page 1), obtain-a list of all User IDs and their associated access rights, and perform the following:</p> <ul style="list-style-type: none"> ▪ Confirm via discussions with the security manager that access rights assigned to privileged User IDs are restricted to least privileges necessary to perform the job. ▪ Confirm via examination of authorization forms that all administrators are authorized and have active accounts. ▪ Select a sample of general users and confirm via examination of authorization forms that those users are authorized and have active accounts. 			
<p>6.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know.</p>		<p>6.2 Verify there is a written procedure for data control, and that it includes the following:</p> <ul style="list-style-type: none"> ▪ Coverage of all production operating systems, network components, databases, and applications. ▪ Assignment of privileges to individuals based on job classification and function. ▪ Requirement for an authorization form that is signed by management and specifies required privileges. 			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirement 7: Assign a unique ID to each person with computer access.					
<p>7.1 Uniquely identify all users before allowing them to access system resources or cardholder information.</p>	<p>Authentication must clearly establish a user's unique identity.</p> <p>An internal employee transfer may result in the employee no longer needing access to cardholder data.</p>	<p>7.1 For the samples of firewalls/routers, database servers, and other critical servers (Sampling Note, page 1), review user ID listings and verify the following:</p> <ul style="list-style-type: none"> • Generic ID's are not used except in emergency situations. • Shared IDs for system administration activities and other critical functions do not exist. 			
<p>7.2 Employ at least one of the methods below to authenticate all internal and external users:</p> <ul style="list-style-type: none"> ▪ Unique user name and password ▪ Token devices (i.e., Secured, certificates, or public key) ▪ Biometrics 	<p>Repeated system access attempts could mean someone is trying to establish a false identity for illegal system access or use a valid identity in an unauthorized manner.</p>	<p>7.2 To verify that users are authenticated using unique ID and password for access to the cardholder environment, perform the following:</p> <ul style="list-style-type: none"> • Document the authentication method(s) used. • For each type of authentication method used and once for each type of server (e.g., firewall, database, application, Web, etc.), perform or observe a test authentication to verify authentication is working as expected. For example, if one factor authentication (user ID and password) is employed, perform a test logon to verify that a user ID and password are required to authenticate access. If SecurID authentication is used, perform a test logon to verify that token pin is required to authenticate access. 			
<p>7.3 Ensure proper user authentication and password management for non-consumer users:</p>		<p>7.3 Verify, via review of procedures and discussions that procedures exist for adding, deleting, and modifying user IDs and access credentials. Perform the following:</p>			
<p>7.3.1 Control the addition, deletion, and modification of user IDs, credentials, or other identifier objects.</p>		<p>7.3.1 Select a sample of user IDs from sampled firewalls/routers, database servers, and other critical servers (Sampling Note, page 1), and trace those IDs to the authorization forms. Verify the IDs are implemented in accordance with the authorization form (e.g., with privileges as specified, all signatures obtained, etc.).</p>			
<p>7.3.2 Immediately revoke accesses of terminated users.</p>		<p>7.3.2 Select a sample of employees terminated in the last 6 months, and verify that their IDs have been inactivated or removed.</p>			
<p>7.3.3 Distribute password procedures and policies to all users who have access to cardholder information.</p>		<p>7.3.3 Select a sample of employees with access to cardholder data, and ask them about their awareness of password procedures.</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

7.3.4 Do not permit group passwords.		7.3.4 Review password procedures to verify that group passwords are explicitly prohibited. Interview system administrators to verify that group passwords are not given out even if requested.			
7.3.5 Change user passwords at least every 90 days.		7.3.5 Inspect system configuration settings to verify that user passwords are required to change at least every 90 days. (In Windows NT, the password maximum age should be set to 90, or in UNIX, the password change interval setting should be set to 90.)			
7.3.6 Require a minimum password length of at least 7 characters.		7.3.6 Inspect system configuration settings to verify that passwords are required to be at least 7 characters long. (In Windows 2000, Minimum Password Length is set in Account Policy).			
7.3.7 Use passwords containing both numeric and alphabetic characters.		7.3.7 Inspect system configuration settings to verify that passwords are required to contain both numeric and alphabetic characters. (In Windows 2000, the password complexity option is enabled in Account Policy).			
7.3.8 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.		7.3.8 Inspect system configuration settings to verify that new passwords cannot be the same as the 4 previously used passwords. (In Windows NT, the password history setting is set to '4'.)			
7.3.9 Monitor system access attempts. Limit "repeated" attempts by locking out the user ID after a specific number of tries. (The maximum number for system access attempts must not exceed six.)		7.3.9 Inspect system configuration settings to verify that a user's account is locked out after 6 invalid logon attempts. (In Windows 2000, Account Lockout Policy is set in Account Policy).			
7.3.10 Set the lockout duration to "forever" until administrator enables the user ID.		7.3.10 Inspect system configuration settings to verify that that once a user account is locked out, it remains locked until a system administrator resets the account. (In Windows 2000, the Account Lockout Duration, Account Lockout Threshold, and 'Reset Account Lockout After' settings should be set appropriately.)			
7.3.11 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.		7.3.11 Inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes. (In Windows 2000; the setting is at "Amount of idle time required before disconnecting session" feature in security options within Group Policy.)			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>7.3.12 Authenticate all access to any database containing cardholder information. This includes access attempts made by applications, administrators, and all other users.</p>		<p>7.3.12 Verify that all database access is authenticated, including that for individuals, applications, and administrators. Also verify that direct SQL queries to the database are prohibited.</p>			
Requirement 8: Do not use vendor-supplied defaults for system passwords and other security parameters					
<p>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.).</p>	<p>Vendor-supplied passwords are well known and easily obtained from vendors or the Internet.</p> <p>There are many good sources for security configuration standards, which include discussion of risky services and features, and proper security parameter settings. The Center for Internet Security (www.cisecurity.org) has numerous free benchmarks (best-practice security configurations) and scoring tools for Windows NT and 2000, Solaris, and others (Apache and IIS are in draft form), as well as a Top 20 Scanner to scan for the FBI/SANS Top 20 Vulnerabilities (Scanner at www.cisecurity.org, vulnerabilities at www.sans.org/top20)</p>	<p>8.1 To verify that default accounts and passwords have been changed, use the samples of firewalls/routers, database servers, and other critical servers (Sampling Note, page 1), and attempt to logon (with system administrator help) to the devices using default vendor-supplied accounts and passwords (e.g., for the Microsoft SQL server, the default password for the SA account is blank. Use vendor manuals and sources on the Internet to find more vendor-supplied accounts/passwords.)</p>			
<p>8.2 Develop system configuration standards for all “networks components”. Make sure these standards address all known security vulnerabilities and industry best practices.</p> <p><i>Note: “Network components” include, but are not limited to servers, switches, firewalls, etc.</i></p>		<p>8.2 Evaluate the organization’s system configuration standards for network components and critical servers. Verify each item below is included in the standard, and via discussions with the relevant administrator, verify that each item is included when new systems are configured. Also perform additional steps as follows:</p>			
<p>8.2.1 Implement only one application or primary function per network component (i.e., one application per server).</p>		<p>8.2.1 Only one application or primary function is implemented per server.</p>			
<p>8.2.2 Make sure each network component contains the minimum hardware and software it needs to prevent misuse.</p>		<p>8.2.2 Each component contains the minimum hardware and software needed to prevent misuse.</p>			
<p>8.2.3 Disable all unnecessary services.</p>		<p>8.2.3 All unnecessary services are disabled (necessary ones are documented). Obtain and inspect a list of enabled system services/daemons from a subset of the total sample. Verify that the list of enabled services does not contain unnecessary services and that any potentially dangerous ones are justified and documented (e.g. FTP and telnet).</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>8.2.4 Configure system security parameters to prevent misuse.</p>	<p>Also consider SANS at www.sans.org for training, publications, links to other sites, etc..</p>	<p>8.2.4 System security parameters are configured to prevent misuse. Verify that system administrators and/or security managers have knowledge of common security parameter settings for their operating systems, database servers, and Web servers. Review system configuration standards and verify inclusion of these parameters settings. Select a small sub-sample from the samples of database and other critical servers, and verify that several of the most risky parameters are set appropriately.</p>			
<p>8.2.5 Remove all unnecessary functionality, e.g., drivers, features, subsystems, file systems, etc.</p>		<p>8.2.5 All unnecessary functionality (e.g., drivers, features, subsystems, file systems, etc.) is removed. Verify necessary functions are documented and are the only ones present on the sub-sample of machines used above.</p>			
<p>8.2.6 Enable the audit subsystem in support of Requirement 9.</p>		<p>8.2.6 Audit capabilities are enabled on firewalls, routers, database servers, and other critical servers.</p>			
<p>8.2.7 Configure the networking subsystems to protect against known attacks.</p>		<p>8.2.7 Systems are configured to protect against known attacks.</p>			
<p>8.3 Establish a process to identify newly discovered security vulnerabilities. Update your standards to address new vulnerability issues.</p>		<p>8.3 Review processes in place to identify new security vulnerabilities, and verify that the process includes updates to the system configuration standards reviewed in 8.2 above as new vulnerability issues are found.</p>			
<p>Requirement 9: Track all user access to data by a unique ID</p>					
<p>9.1 Establish a process for linking all data access activities (especially those with root or administrative privileges) to an individual user or system.</p>	<p>Audit trail files should not be able to be deleted for at least 6 months. No one should be able to delete the files from their original location. Copy the files to a location for retention, and the authorized administrator can delete from there as necessary.</p>	<p>9.1 Verify, via observation and discussions with the system administrator, that audit trails are enabled and active.</p>			
<p>9.2 Implement automated audit trails to reconstruct the following events:</p>		<p>9.2 Confirm through inquiry and via cursory review of audit logs for the samples of firewalls/routers, database servers, and other critical servers (Sampling Note, page 1), that audit trails record the following types of events:</p>			
<p>9.2.1 All accesses to cardholder data</p>		<p>9.2.1 Access to cardholder data</p>			
<p>9.2.2 All actions taken by any individual with root or administrative privileges</p>		<p>9.2.2 Actions taken by any individual with root or administrative privileges</p>			
<p>9.2.3 Access to all audit trails</p>		<p>9.2.3 Access to all audit trails</p>			
<p>9.2.4 Invalid logical access attempts</p>		<p>9.2.4 Invalid logical access attempts</p>			
<p>9.2.5 Use of identification and authentication mechanisms</p>		<p>9.2.5 Use of identification and authentication mechanisms</p>			
<p>9.2.6 Initialization of the audit logs</p>		<p>9.2.6 Initialization of audit logs</p>			
<p>9.2.7 Deletion of objects</p>		<p>9.2.7 Deletion of objects</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

9.2.8 Actions taken in response to the compromise of cryptographic keys		9.2.8 Compromise of cryptographic keys			
9.2.9 Changes in the custody of keys and devices or media holding keys		9.2.9 Changes in the custody of keys and devices or media holding keys			
9.2.10 All encryption key management operations		9.2.10 All encryption key management operations			
9.3 Record the following audit trail entries for each event:		9.3 Confirm through inquiry and observation that the audit trail minimally captures the following information:			
9.3.1 User identification		9.3.1 User identification			
9.3.2 Type of event		9.3.2 Type of event			
9.3.3 Date and time		9.3.3 Date and time stamp			
9.3.4 Success or failure indication		9.3.4 Success or failure indication			
9.3.5 Origination of event		9.3.5 Origination of event			
9.3.6 Identity or name of affected data, system component, or resource		9.3.6 Identity or name of affected data, system component, or resources			
9.4 Secure audit trails so they cannot be altered in any way.		9.4 Verify the following via discussions with the system administrator and cursory review of file permissions: <ul style="list-style-type: none"> ▪ Only individuals who have a job-related need can view audit trail files ▪ No one has the ability to change or delete current audit trail files. 			
9.5 Review security, firewall, and server logs at least daily.		9.5 Verify that processes are in place to review security logs at least daily, and that follow-up to exceptions is specified.			
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 six months or more.)		9.6 Verify that audit log retention policies exist and are implemented, and include log retention for at least 6 months. For the samples of firewall/routers/ database servers, and other critical servers (Sampling Note, page 1), verify that audit logs are available online or on tape for the period of time specified in the policy.			
Requirement 10: Regularly test security systems and processes.					
10.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts.	Custom code should be reviewed for security concerns before being place into production. These code reviewers	10.1 Confirm through inquiry that periodic security testing of the devices within the VISA cardholder environment occurs.			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>10.2 Run internal and external network vulnerability scans at least monthly and after any change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades).</p>	<p>should be knowledgeable about secure coding techniques as well as things that developers should avoid doing to develop secure applications. Consider sources such as The Open Web Application Security Project at www.owasp.org.</p>	<p>10.2 Inspect output from the most recent network, host, and application vulnerability scans to verify that periodic security testing of the devices within the VISA cardholder environment occurs. Confirm that high level risks identified in the scans are accompanied by remediation plans which:</p> <ul style="list-style-type: none"> • Outline how and when the risk will be addressed • Specify who has ownership of the system at risk. 			
<p>10.3 Before promoting custom application code to the production site, review it carefully to identify any potential coding vulnerability.</p>	<p>Do not display whole credit card numbers on any Web pages – just show the last 4 digits.</p>	<p>10.3 Confirm that written policies dictates that code reviews are required, are to be performed by individuals other than the originating author of the code (e.g., developer), and that those performing the code reviews have knowledge of secure coding techniques. Confirm that such code reviews are occurring after code changes.</p>			
<p>10.4 Perform penetration testing on network infrastructure and applications at least once a year and after any “significant” infrastructure and application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment, etc.).</p>	<p>Per VISA regulations, Incident Response and Disaster Recovery procedures should include the following:</p>	<p>10.4 Verify that penetration testing is performed on network infrastructure and applications at least annually and after any significant changes to the environment.</p>			
<p>10.5 Use network intrusion detection systems to monitor all network traffic and alert personnel to suspected compromises.</p> <ul style="list-style-type: none"> ▪ Designate specific personnel to be available on a 24/7 basis to respond to unexpected compromise alerts. 	<ul style="list-style-type: none"> ▪ Immediately notify VISA U.S.A. Fraud Control, through the merchant bank or processor, of any suspected or confirmed loss or theft of material or records that contain account information. 	<p>10.5 Verify the use of network intrusion detection products to monitor and alert personnel of suspected compromises, and confirm existence of related policies and procedures.</p> <ul style="list-style-type: none"> ▪ Via observation and review of policies, confirm the existence of 24/7 incident response and monitoring coverage. 			
<p>10.6 Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files.</p>	<ul style="list-style-type: none"> ▪ Demonstrate the ability to prevent future loss or theft of account or transaction information; and 	<p>10.6 Verify the use of file integrity monitoring products, and confirm existence of related policies and procedures.</p>			
<p>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.</p>	<ul style="list-style-type: none"> ▪ Allow VISA U.S.A. or an independent third 	<p>10.6.1 Verify via observation and review of policies, existence of 24/7 response for critical system or file changes.</p>			
<p>10.6.2 Perform critical files comparisons at least daily (or more frequently if the process can be automated).</p>		<p>10.6.2 Verify that critical file comparisons are performed at least daily.</p>			
<p>10.7 Be prepared to respond immediately to a system failure:</p>		<p>10.7 Verify the existence of a Disaster Recovery Plan and related procedures, and that the plan includes:</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

10.7.1 Create a business and disaster recovery plan that involves a crisis-management team who can handle all mission-critical decisions, if possible together during a moment of crisis.	party acceptable to VISA to verify that ability by conducting a security review. A strong incident response capability includes active monitoring where individuals are watching screens for alerts or receive pages vs. passive monitoring where individuals receive emails that are inspected at a later time.	10.7.1 A crisis-management team to handle all important decisions.			
10.7.2 Test the plan at least annually.		10.7.2 Testing of the plan at least annually.			
10.7.3 Provide adequate training to staff with operational business and recovery plan execution responsibilities.		10.7.3 Training for staff with execution responsibilities			
10.8 Be prepared to respond immediately to a system breach.		10.8 Verify the existence of an Incident Response Plan and related procedures, and that the plan includes:			
10.8.1 Create a plan that designates roles and responsibilities in the event of system compromise. Make sure the plan addresses security communication/contract strategies (e.g., informing Visa, law enforcement, internal parties, etc.).		10.8.1 Roles, responsibilities, and communication strategies in the event of a compromise. (Visa, law enforcement, and internal parties should all be detailed in the list of those to receive communication in the event of a compromise.)			
10.8.2 Test the plan at least annually.		10.8.2 Testing of the plan at least annually.			
10.8.3 Provide appropriate training to staff with security breach response responsibilities.		10.8.3 Training for staff with security breach responsibilities			
10.9 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.		10.9 Review policies and procedures for backups, as well as supporting documentation (backup tape logs, etc.) to verify that backups are performed in accordance with the following: <ul style="list-style-type: none"> ▪ Full backups are performed nightly, or full backups are performed weekly with nightly incremental backups. ▪ Backup media are stored and transported in a physically secure, fireproof, offsite location. ▪ Backup media are available within a reasonable time (e.g., 4 hours) of a request by an authorized administrator. 			
Requirement 11: Maintain a policy that addresses information security for employees and contractors.					
11.1 Establish and publish a security policy that:	Educate employees and contractors about their cardholder information security responsibilities through posters, letters,	11.1 Review the information security policy, verify the policy is published, and verify that:			
11.1.1 Addresses all CISP requirements		11.1.1 The policy addresses all CISP requirements			
11.1.2 Reflects your organization's business objectives and risk control standards		11.1.2 The information security policy reflects the organization's business objectives.			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

11.2 Develop daily operational security procedures that are consistent with CISP requirements.	memos, meetings, promotions, etc.	11.2 Review the daily operational security procedures. Verify they are consistent with CISP, and include administrative and technical procedures for each of the CISP requirements.			
11.3 Make sure your security policy and procedures clearly define information security responsibilities for all employees and contractors.	A formalized, documented, enforceable agreement must be maintained between the select merchant or service provider as keeper of cardholder data and any 3 rd parties with access to the data. This agreement may be addressed by various means, such as within the provisions of the contracts between these entities, an addendum to a current contract, or an entirely new contract.	11.3 Verify that information security policies clearly define information security responsibilities for both employees and contractors.			
11.4 Assign to an individual or team the following information security management responsibilities:		11.4 Verify that the following information security responsibilities are specifically and formally assigned:			
11.4.1 Establish, document, and distribute security policies and procedures.		11.4.1 Creating and distributing security policies and procedures.			
11.4.2 Monitor and analyze security alerts and information and distribute to appropriate personnel.		11.4.2 Monitoring and analyzing security alerts, and distributing information 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.		11.4.3 Creating and distributing security incident response and escalation procedures.			
11.4.4 Administer user account and authentication management, including additions, deletions, and modifications resulting from user changes and terminations.	This agreement can be customized to cover the areas relevant to the business performed by the 3rd party.	11.4.4 Administering user account and authentication management.			
11.4.5 Monitor and control all access to data.	In the example of an offsite media storage company, such relevant areas would include contacting the select merchant or service provider if there is any compromise to their data, conducting background checks on all personnel with access to such data, supporting critical information retrieval in the event of a disaster at the	11.4.5 Monitoring and controlling all access to data.			
11.5 Make all employees aware of the importance of cardholder information security:		11.5 Verify the existence of a security awareness program, and that it contains the following components:			
11.5.1 Educate employees through posters, letters, memos, meetings, promotions, etc.		11.5.1 Multiple methods of communicating awareness (posters, letters, meetings, etc.).			
11.5.2 Require employees to acknowledge in writing they have read and understood your company's security policy and procedures.		11.5.2 Requirement for employees to acknowledge in writing that they have read and understood the company's information security policy.			
11.6 Screen all potential employees to minimize the risk of attacks from internal sources.		11.6 Verify that background checks are performed on all potential employees including pre-employment, criminal, credit history, and reference checks.			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>11.7 Contractually require all associated third parties with access to cardholder data to adhere to CISP data security requirements. At a minimum, the agreement should address:</p>	<p>event of a disaster at the select merchant's or service provider's facilities, and using disaster recovery and business continuity controls at the offsite media storage company. Many CISP controls would not be relevant to an offsite</p>	<p>11.7 Review any 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 CISP requirements that are relevant to the business relationship between the organization and the 3rd party are included in the contract (see further explanations in the Best Practices column). Specifically verify that contracts address:</p>			
<p>11.7.1 Security provisions outlined in the CISP, and any fines and penalties as specified by Visa for a lack of compliance with those provisions.</p>	<p>storage facility (as part of a CISP review), but those that are relevant to the security and availability of cardholder data should be in the agreement.</p>	<p>11.7.1 CISP security requirements and any related fines and penalties</p>			
<p>11.7.2 Ownership by Visa, Acquirer, and Merchants of cardholder information and that it 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.</p>	<p>Another example would be if the 3rd party had an electronic connection to the select merchant or service provider, then their firewall administration, etc. would become part of the agreement.</p>	<p>11.7.2 Ownership and acceptable uses of cardholder information.</p>			
<p>11.7.3 Business continuity in the event of a major disruption, disaster or failure.</p>	<p>Consider 3rd party relationships in which VISA cardholder information is processed or transmitted to/from an international entity that is not subject to VISA U.S.A. CISP. These entities are subject to VISA International Account Information Security (AIS).</p>	<p>11.7.3 Business continuity provided by the 3rd party.</p>			
<p>11.7.4 Audit provisions that ensure that Visa, or a Visa 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 Visa CISP standards for protecting cardholder data.</p>		<p>11.7.4 Audit provisions for Visa or Visa-approved entities in the event of a cardholder data compromise.</p>			
<p>11.7.5 Third party termination clauses to address compliance with CISP and security of cardholder information during contract terminations and related data transfers.</p>		<p>11.7.5 Security of cardholder information during 3rd party contract terminations.</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Requirement 12: Restrict physical access to cardholder data					
<p>12.1 Use appropriate facility entry controls to limit physical access to systems that store or process cardholder data.</p>		<p>12.1 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:</p> <ul style="list-style-type: none"> ▪ Verify that video cameras are present in the data centers to monitor systems storing cardholder data. ▪ Observe that consoles for 3 randomly selected systems that store and/or transmit cardholder data are “locked” to prevent unauthorized use. ▪ Verify 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. 			
<p>12.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.</p> <p><i>Note: Unless otherwise indicated, “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 less than three hours.</i></p>		<p>12.2 Procedures to help distinguish between employees and visitors are reviewed at 12.3.2 below.</p>			
<p>12.3 Make sure all visitors are:</p>		<p>12.3 Verify the following employee/visitor controls are present:</p>			
<p>12.3.1 Authorized before entering areas where cardholder data is processed or maintained.</p>		<p>12.3.1 Verify the use of ID badges within the company. Verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.</p>			
<p>12.3.2 Given a physical token (e.g., badge or access device) that identifies them as non-employees containing a fixed expiration date.</p>		<p>12.3.2 Observe people within the facility to verify that: 1) ID badges clearly distinguish employees from visitors/outside and 2) visitor badges contain a fixed expiration date.</p>			
<p>12.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.</p>		<p>12.3.3 Verify that visitors are asked to surrender their ID badge upon departure or expiration date.</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>12.4 Use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months.</p>		<p>12.4 Verify that a visitor log is in use for physical access to the facility as well as computer rooms and data centers where cardholder information is stored or transmitted. Confirm the log contains the visitors name, the firm represented, and the employee authorizing physical access, and is retained for at least 3 months.</p>			
<p>12.5 Restrict and/or monitor closely visitor access to areas where cardholder information is processed or maintained.</p>		<p>12.5 Restrictions and monitoring for visitor access to restricted areas are reviewed at 12.1.1, 12.3.2, and 12.4.</p>			
<p>12.6 Physically secure all paper and electronic media (e.g., computer, networking, and communications hardware, telecommunication lines, etc.) that contain cardholder information.</p>		<p>12.6 Review the procedures and processes in place for protecting all paper and electronic media that contains cardholder data. Verify that, in addition to paper and electronic media in computer rooms and data centers, the process includes controls for paper, CDs and disks in employee desks and open workspaces, and PC hard drives.</p>			
<p>12.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information:</p>		<p>12.7 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:</p>			
<p>12.7.1 Label the media as “confidential”.</p>		<p>12.7.1 All media should be labeled as “confidential”.</p>			
<p>12.7.2 Send the media via secured courier or a delivery mechanism that can be accurately tracked.</p>		<p>12.7.2 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.</p>			
<p>12.8 Ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals).</p>		<p>12.8 Select a recent sample of 3 days of offsite media tracking logs (see 12.7a above) and verify the presence in the logs of tracking details and proper management authorization.</p>			
<p>12.9 Maintain strict control over the storage and accessibility of media that contains cardholder information:</p>		<p>12.9 Verify that a policy exists to control storage and maintenance of hardcopy and electronic media, and that this policy requires periodic media inventories. Verify related processes by performing the following:</p>			
<p>12.9.1 Properly inventory all media and make sure it is securely stored.</p>		<p>12.9.1 Review supporting documentation to verify that periodic media inventories are performed</p>			
<p>12.9.2 Implement data retention and disposal policies and procedures for all media containing cardholder information.</p>		<p>12.9.2 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.</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

<p>➔ Refer to CISP Requirement 3.0 for specific actions and timeframes related to cardholder information retention and disposal.</p>		<p><i>Data retention and destruction procedures reviewed in 12.10 below and at Testing Procedure 3.1.</i></p>			
<p>12.10 Destroy media containing cardholder information when it is no longer needed for business or legal reasons:</p>		<p>12.10 Verify that a policy exists for periodic media destruction, especially with respect to cardholder data. Verify that the procedure requires the following:</p>			
<p>12.10.1 Shred or incinerate hardcopy materials</p>		<p>12.10.1 Shredding or incineration of hardcopy materials.</p>			
<p>12.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.</p>		<p>12.10.2 Destruction of electronic media beyond recovery by using a military wipe program to delete files, degaussing, or otherwise physically destroying the media.</p>			

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Attachment A

Visa USA Cardholder Information Security Program Requirement #3: "Protect stored data"

Encryption Clarification

As merchants and service providers work to ensure compliance with the "Digital Dozen," Visa has been made aware of the need to further clarify the requirement to encrypt stored data.

The intent of the requirement is to protect stored cardholder information. While strong encryption (PGP or Triple-DES and associated key management practices and procedures) may be the implied recommendation, Visa is aware that this technique may not be achievable in some environments, and that acceptable alternatives, including other encryption or storage mechanisms that achieve this same objective, need to be articulated.

Baseline Clarifications

- The MINIMUM account information that needs to be encrypted is the Visa account number and expiration date. *(Note that CVV2 data must not be retained in any zone.)*
- The term "encryption" refers to any of several techniques used to render account information unreadable.
- Account numbers must NEVER be stored in the clear on the same webserver that is connected to the Internet (i.e., in the DMZ).

Acceptable Practices

For account information accessible from the Internet, any of the following approaches are being used to secure the account number and expiration date:

- One-way ciphers (hashed indexes), such as SHA-1, but not MD5
- Truncation
- Simple ciphers
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as PGP or Triple-DES, with associated key management processes and procedures

If encryption techniques cannot be used, account information must be isolated from the Internet in a separate database not resident on systems directly connected to the Internet. Ideally, the database should be resident on back-end computers behind an internal firewall (not in the DMZ.) One acceptable practice would be to separate account information from sales data on the Web server and to store the account information on the mainframe, off-line, or in a secure zone.

Visa U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting

Attachment B

Visa USA Cardholder Information Security Program Requirement #3: "Protect stored data"

Data Segregation Mechanisms

As service providers work to ensure compliance with the Visa U.S.A. Cardholder Information Security Program (CISP), Visa has been made aware of the need to further clarify the sub-requirement to *segregate merchants' stored data*.

The intent of this sub-requirement is to mitigate the risk in the event an entity is compromised. A service provider environment hosts numerous customer data.

An attack on one customer is an attack on all. By separating one customer's data from another, the number of credit cards that a hacker could potentially compromise in an attack is limited. This document will discuss best practices in Internet commerce security and Visa's recommendations for segregating merchant information.

Internet Commerce:

At a minimum, all service providers must implement the following practices for their e-commerce environment:

- Implement multiple layers of firewall (i.e., separate external and internal network).
- The database that stores merchant and cardholder information must not reside on the same network segment as the web servers (i.e., DMZ). This database must be placed in a secured zone.
- To further protect merchant and cardholder information, we recommend implementing additional databases to push sensitive information from the main database (i.e., account numbers and expiration date) onto this database. This database must be placed in a secured zone.
- All CISP requirements must be implemented on these systems.

Additionally, these guidelines should be followed to protect merchant and cardholder information, whether or not physical or logical segregation is implemented.

- Access to data should be restricted by business need-to-know. Apply the principle of "least privilege" restricting data based on a user's need to know. For systems with multiple users, a mechanism should be established that restricts access based on a users need to know.
- Avoid direct access to tables. Use stored procedures, and views to provide a shield between the site and actual cardholder information.
- A web-application that accesses a database SHOULD NOT use an administrative account, which can read and write all data and make changes to the database schema. The account should be limited to only the access rights and privileges needed to perform the functions of the site.
- Each e-Commerce entity should have a separate database account with access limited to that e-Commerce entity's cardholder data.
- The web-application should not store the credentials for e-Commerce entities with database accounts. The e-Commerce entity would provide the credentials that would then be passed through to the database.

Segregation of Merchant information:

Physical separation of data is the strongest segregation mechanism for securing stored data, however if you cannot accomplish physical segregation, at a minimum there should be a logical separation of data.

- 1) Physical data segregation. Practices include:
 - Completely separate network for each merchant.
 - If separate network cannot be met, implement separate backend servers that store merchant information.
- 2) Logical data separation. Practices include:
 - Use separate merchant tables to store cardholder information. A service provider storing cardholder data for multiple e-Commerce entities should separate each e-Commerce entity's cardholder data and separate cardholder lookup or transactional tables.