Visa U.S.A Cardholder Information Security Program (CISP)
Payment Application Best Practices

This document is to be used to verify that a payment application has been validated against Visa U.S.A. Payment Application Best Practices and to create the Report on Validation.

Please note that payment application validation is voluntary by software vendors[1] and NOT a requirement by Visa U.S.A at this time. Visa USA reserves the right to make payment application validation a requirement, based on payment industry needs, and as needed to support Cardholder Information Security Program (CISP) compliance of payment application users.

Secure payment applications, when implemented in a CISP-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data or CVV2, and the damaging fraud resulting from these breaches.

The requirements for Payment Application Best Practices validation are derived from the Payment Card Industry (PCI) Data Security Standard and the PCI Security Audit Procedures. These documents, which can be found at www.visa.com/cisp, detail what is required to be CISP compliant (and therefore what a payment application should do to facilitate a merchant's CISP compliance) and should be used as a reference for CISP standards.

Validated applications must be capable of being implemented in a CISP-compliant manner. Software vendors are expected to provide product documentation to instruct their customers on secure product implementation. This documentation should clearly delineate vendor and customer responsibilities for meeting CISP requirements. It should detail the responsibilities of the customer to enable security settings within their own network, such as password security, which may not controlled by the application but are required for CISP compliance.

Assessors: contact Visa at cisp@visa.com for approval before proceeding with a Payment Application Best Practices audit. Visa will not accept audits without this pre-approval.

Visa Requirements:

1. A Visa-approved security assessor must perform the payment application validation. For the Qualified CISP Security Assessor List, visit www.visa.com/cisp.
2. The security assessor must utilize the testing procedures documented in this Payment Application Best Practices document.
3. The security assessor or software vendor must deliver the Report on Validation in a secure manner to Visa.
4. Once compliant, Visa will list the software vendor on www.visa.com/cisp **for one year only**. The expiration date will be determined by the date that Visa approves the Report on Validation. Visa will send an acceptance letter to software vendors indicating

[1] Software vendors are developers of applications specifically for credit card transactions. Examples are point-of-sale (POS) and shopping cart products.

© 2005 Visa U.S.A. Inc.

approval of the report. Software vendors must have software re-validated by a Visa-approved security assessor, if they wish to be "active" on the Visa website. Visa will remove the software vendor's listing from the website if subsequent reports are not received by the due date.

Note: Visa does NOT require re-validation, if no major upgrade or product version change has been made to the payment application. Visa will require a letter from the software vendor prior to the expiration date indicating no changes to the payment application. In addition, for any changes to the reviewed version, Visa will require the vendor to submit a description of such changes.

Prerequisites

The software vendor must have a working, semi-production laboratory where the validation process is to occur. The laboratory must include the following:

- Common implementation of the payment application to be tested.
- Implementation of security devices. At a minimum, the following must be running per CISP requirements: firewall or traffic filtering devices, Network Address Translators (NAT), Port Address Translators (PAT), anti-virus software and encryption.
- Establishment of CISP compliant operating systems and applications necessary to run the software.

Note: Alternatively, the software vendor may elect to have the validation performed at the security assessor's laboratory, provided that the assessor's laboratory meets the above requirements.

Scope of payment application validation

Include all systems where the application is implemented. For example, a standard implementation of software vendor's payment application might be installed in a client/server environment within a retail storefront, and back office or corporate network. The laboratory must simulate this type of implementation.

Report on Validation

The Report on Validation must be securely distributed to Visa. Visa will classify the Report as "Visa Secret."[2]

[2] This classification applies to the most sensitive business information, which is intended only for use within Visa.

© 2005 Visa U.S.A. Inc.

Note: Visa will NOT list a software vendor as compliant if the report has outstanding items. Visa highly recommends that software vendor implement all the items (exceptions will be made for encryption of data at rest) listed on the Payment Application Best Practices prior to having their application validated.

Visa will additionally recognize those software vendors with payment applications that provide strong encryption, such as 3DES or AES.

All assessors MUST apply the following report content and format when completing the Report on Validation:

1. Executive Summary
   Include the following:
   - Software vendor name
   - Software vendor contact information
   - Software vendor mailing address
   - Assessor name and contact information
   - Product Name
   - Product Version (if applicable)
   - Operating system with which the payment application was tested. Include other applications required by the payment application.
   - Database software used or supported by the application.
   - Brief description of the payment application/family of products (2-3 sentences)
   - Brief description of the software vendor or assessor's laboratory (2-3 sentences)
   - A network diagram of a typical implementation of the software (not necessarily a specific implementation at a merchant's site) that includes, at high-level, connections into and out of a merchant's network and the implementation components within the merchant's network.
   - Describe the typical merchant that this product is sold to (e.g., large, small, if industry-specific, Internet, brick-and-mortar, etc.)

2. Description of Scope of Validation and Approach Taken
   - Describe scope of review as defined at Scope of payment application validation, above.
   - Timeframe of validation
   - List of documentation reviewed

3. Findings and Observations

© 2005 Visa U.S.A. Inc.

- All assessors must utilize the following template to provide detailed report descriptions and findings on each Best Practices
- Describe tests performed other than those included in the testing procedures column.

4. Contact Information and Report Date
   - Software vendor contact information (include URL, phone number and email address)
   - Assessor contact information (include phone number and email address)
   - Date of report

Definitions
For the purpose of the Validation Procedures and Reporting the following definitions will be used:

- **Best Practices** – Recommended practices for software vendor to create secure payment applications to help their customers comply with CISP.
- **Testing Procedures** – A process to be followed by an independent security audit firm to address individual Best Practices and testing considerations
- **In Place -** Please provide a brief description of Best Practices found to be in place. If a Best Practice is **Not Applicable** to the software, please explain why and define where this control should be implemented (e.g. this server-based control is the customers' responsibility).
- **Not In Place –** Please provide a brief description of Best Practices that are not in place.
- **Target Date/Comments** – For those Best Practices "Not In Place" include a target date that the application vendor expects to have "In Place." Any additional notes or comments may be included here as well.

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
1. Do not retain full magnetic stripe or CVV2 data.				
1.1 Do not store sensitive authentication data subsequent to authorization (not even if encrypted): PCI Data Security Standard 3.2 (A)	**1.1** If sensitive authentication data (see 1.1.1 – 1.1.3 below) is received and erased, obtain and review methodology for erasing the data to determine the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps:			
1.1.1 Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.) PCI Data Security Standard 3.2.1 (A) *Subsequent to authorization,* ***service codes, discretionary data/CVV, and Visa reserved values*** *must be removed; however, account number, expiration date, and name may be extracted and retained.*	**1.1.1** Examine the following files created by the application, and verify that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Debug logs • Audit logs • Database schemas and tables			
1.1.2 Do not store the card-validation code (Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data)). PCI Data Security Standard 3.2.2 (A)	**1.1.2** Examine the following files created by the application and verify that the three-digit or four-digit card-validation code printed on the signature panel (CVV2/CVC2 data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Debug logs • Audit logs • Database schemas and tables			

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
1.1.3 Do not store the PIN Verification Value (PVV) PCI Data Security Standard 3.2.3 (A) *PIN blocks must never be retained, even if encrypted, after transaction authorization.*	**1.1.3.a** Examine the following files created by the application, and verify that the PIN Verification Value (PVV data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Debug logs • Audit logs • Database schemas and tables **1.1.3.b** Examine bulleted items above to verify PIN blocks are not present.			
2. Protect stored data				
2.1 Mask account numbers when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Note that this does not apply to those employees and other parties with a specific need to see full credit card numbers.* PCI Data Security Standard 3.3 *(A)*	**2.1** Review displays of credit card data, including POS devices, screens, logs, receipts, etc., to determine that credit card numbers are masked when displayed.			

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
2.2 Render sensitive cardholder data unreadable anywhere it is stored, (including data on portable media, in logs, and data received from or stored by wireless networks). *The MINIMUM account information that needs to be rendered unreadable is the payment card account number* PCI Data Security Standard 3.4 (A) *Data should be rendered unreadable anywhere cardholder data is stored, even outside the payment application.*	**2.2** Verify that cardholder data is encrypted with strong encryption (at least 128-bit), such as Triple-DES or AES, anywhere it is stored (including databases, removable media, and logs), in accordance with PCI Data Security Standard 3.4.			
2.3 Application should protect encryption keys against disclosure and misuse. PCI Data Security Standard 3.5 (A)	**2.3** Verify the application protects encryption keys against disclosure and misuse, per PCI Data Security Standard 3.5.			
2.4 Application should implement key management processes and procedures. PCI Data Security Standard 3.6 **(A)**	**2.4** Verify the application implements key management techniques, per PCI Data Security Standard 3.6.			
3. Provide secure password features.				

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
3.1 Application should require a unique username and complex password for all administrative access and access to cardholder data. PCI Data Security Standard 8.1 and 8.2 (A) *Note: These password controls are not intended to apply to POS access for employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for POS access by employees with administrative capabilities, or for server access controlled by the application.*	**3.1** Test the application to verify that usernames and passwords are required for administrative access and access to cardholder data. **3.1.b** Test the application to verify the application does not use (or require the use of) default administrative accounts for other necessary software (e.g., the application should not use the administrative account for database software) **3.1.c** Examine CISP Implementation Documentation (B) created by vendor to verify customers are advised against using administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database). Documentation should advise customers to assign a strong password to these default accounts (even though they won't be used), and then disable or do not use the accounts. Documentation should also advise customers to assign strong application and system passwords whenever possible.			
3.2 Access to PCs, servers, and databases with payment applications should require a unique username and complex password.	**3.2** Examine CISP Implementation Documentation (B) created by vendor to verify customers are advised to control access, via unique username and CISP-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.			
3.3 Encrypt application passwords. PCI Data Security Standard 8.4 (A)	**3.3** Examine application password files to verify that passwords are encrypted.			

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
3.4 Application should allow complex passwords. PCI Data Security Standard 8.5 (A)	**3.4.a** Test the application to verify that complex passwords are allowed (e.g., no shared accounts or passwords, passwords changed every 90 days, password length of at least 7 characters long, passwords with both numeric and alphabetic characters, special characters are accepted, password history is maintained, etc.), per PCI Data Security Standard 8.5.8 through 8.5.15). **3.4.b** Examine CISP Implementation Documentation (B) created by vendor to verify customers are advised how to create CISP-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15.			
4. Log application activity				
4.1 Application should log all access by individual users (especially those with administrative privileges), and be able to link those activities to individual users. PCI Data Security Standard 10.1 (A)	**4.1** Examine application settings to verify that application audit trails are automatically enabled or are available to be enabled by customers.			
4.2 Application should implement an automated audit trail to track and monitor access. PCI Data Security Standard 10.2 and 10.3 (A)	**4.2.a** Examine application log parameters and verify that logs contain the data required in PCI Data Security Standard 10.2 and 10.3. (A) **4.2.b** If application log settings are configurable by the customer or customers are responsible for implementing logging, examine CISP Implementation Documentation (B) prepared by the vendor to verify that customers are instructed on how to set CISP-compliant log settings, per PCI Data Security Standard 10.2 and 10.3.			

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
5. Develop secure applications				
5.1 Develop web (Internet-based) software and web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. See www.owasp.org—*"The Ten Most Critical Web Application Security Vulnerabilities."* Cover prevention of common coding vulnerabilities in software development processes, to include: PCI Data Security Standard 6.5 (A)	**5.1** Obtain and examine software development processes. Verify the process includes training in secure coding techniques for developers, and is based on guidance such as the OWASP guidelines. Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques. Alternatively, verify that an external code review or application penetration test was done based on OWASP guidelines (or similar secure coding guidance), and that all coding vulnerabilities were corrected and re-evaluated. For web-based (Internet) applications, determine that processes are in place to determine that applications are not vulnerable to the following:			
5.1.1 Unvalidated input.	**5.1.1** Unvalidated input.			
5.1.2 Broken access control (e.g., malicious use of user IDs).	**5.1.2** Broken access control (e.g., malicious use of user IDs).			
5.1.3 Broken authentication and session management (use of account credentials and session cookies).	**5.1.3** Broken authentication and session management (use of account credentials and session cookies).			
5.1.4 Cross-site scripting (XSS) attacks.	**5.1.4** Cross-site scripting (XSS) attacks.			
5.1.5 Buffer overflows.	**5.1.5** Buffer overflows.			
5.1.6 Injection flaws (e.g., SQL injection).	**5.1.6** Injection flaws (e.g., SQL injection).			
5.1.7 Improper error handling	**5.1.7** Improper error handling			
5.1.8 Insecure storage	**5.1.8** Insecure storage			
5.1.9 Insecure configuration management.	**5.1.9** Insecure configuration management.			

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
5.2 Develop software applications based on industry best practices and include information security throughout the software development life cycle. Include the following: PCI Data Security Standard 6.3 (A)	**5.2** Obtain and review written software development processes to confirm they are based on industry standards and that security is included throughout the life cycle. From review of written software development processes, inquiry of software developers, and review of relevant data (network configuration documentation, production and test data, etc.), determine the following:			
5.2.1 Testing of all security patches and system and software configuration changes before deployment. PCI Data Security Standard 6.3.1 **(A)**	**5.2.1** All changes (including patches) are tested before being deployed.			
5.2.2 Removal of non-essential (test, development, etc.) application accounts, usernames, and passwords before applications are released to customers. PCI Data Security Standard 6.3.5 and 6.3.6 (A)	**5.2.2** Non-essential application accounts, usernames, and passwords are removed before application is released to customers.			
5.2.3 Removal of unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, unencrypted FTP, and others). These services and protocols should not be used or required by the application. PCI Data Security Standard 2.2.2 (A)	**5.2.3** Review system services, daemons, and protocols enabled or required by the application. Verify that unnecessary and insecure services or protocols are not enabled by default or required by the application (e.g., FTP is not enabled, or is encrypted via SSH or other technology).			
5.2.4 Review of custom code prior to release to production or customers, to identify any potential coding vulnerability. PCI Data Security Standard 6.3.7 **(A)**	**5.2.4.a** Confirm the vendor performs code reviews, and that individuals other than the originating author of the code perform the reviews. **5.2.4.b** Confirm that code reviews occur for new code as well as for code changes.			

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
6. Protect wireless transmissions				
6.1 Wireless transmissions of cardholder data should be encrypted, over both public and private networks. Encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless LAN. Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes. PCI Data Security Standard 4.1.1 (A)	**6.1.a** For wireless payment applications (including those connected to cardholder environments), verify that: • Appropriate encryption methodologies are in use for any wireless transmissions, such as: VPN, SSL/TLS at 128 bit, WEP (Wired Equivalency Protocol) at 128 bits, and/or WPA. • If WEP is used and the key rotation process is manual, verify processes are in place to rotate shared WEP keys at least quarterly and whenever key personnel leave. • If WEP is used, verify that another methodology is in use, in addition to WEP, to protect the data. • For automated key rotation processes, verify that keys change every 10-30 minutes. **6.1.b** If customer could implement the payment application into a wireless environment, examine CISP Implementation Documentation (B) prepared by vendor to verify customers are instructed on CISP- compliant wireless settings, per PCI Data Security Standard 1.3.9, 2.1.1 and 4.4.(A)			
6.2 If wireless technology is used within the payment environment, it should be implemented securely. PCI Data Security Standard 1.3.9 & 2.1.1 (A)	**6.2** For wireless payment applications (including those connected to cardholder environments), verify that the wireless technology has been implemented securely with a firewall configuration and that wireless vendor defaults have been changed per PCI Data Security Standard 1.3.9 and 2.1.1			

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
7. Test applications to address vulnerabilities.				
7.1 Software developers should establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet), test their applications for vulnerabilities, and for timely development and deployment of security patches and upgrades. Updates and patches should be delivered in a secure manner with a known chain-of-trust. Any underlying software or systems that are provided along with the payment application (e.g., web servers) should be included in this process. PCI Data Security Standard 6.2 (A)	**7.1** Obtain and examine development processes. Verify the process includes: • Using outside sources for security vulnerability information • Testing of applications for new vulnerabilities, • Delivery of patches and updates in a secure manner with a known chain-of-trust, and • Timely development and deployment of patches to customers. Also verify that all software provided with the payment application (e.g., web servers) is included in this process.			
8. Facilitate secure network implementation				
8.1 The payment application should be able to be implemented into a secure network environment. Application should not interfere with use of network address translation (NAT), port address translation (PAT), traffic filtering network devices, anti-virus protection, patch or update installation, or use of encryption. PCI Data Security Standard 1, 3, 4, and 5 (A)	**8.1** Test the application in a lab to obtain evidence that it can run in a network with NAT, PAT, traffic-filtering devices, anti-virus software, and encryption. Verify that the application does not inhibit installation of patches or updates to other components in the environment.			
9. Cardholder data must never be stored on a server connected to the Internet				

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
9.1 The payment application should not require that the database server and web server be on the same server, or in the DMZ with the web server. PCI Data Security Standard 1.3 and 1.3.5 (A)	**9.1.a** To verify that the application stores cardholder data in the internal network, and never in the DMZ, obtain evidence that the application does not require data storage in the DMZ, and will allow use of a DMZ to separate the Internet from systems storing cardholder data (e.g., application should not require that the database server and web server be on the same server, or in the DMZ with the web server). **9.1.b** If customer could store cardholder data on a server connected to the Internet, examine CISP Implementation Documentation (B): prepared by vendor to verify customers are told not to store cardholder data on Internet-accessible systems (e.g., web server and database server should not be on same server.)			
10. Facilitate secure remote software updates				
10.1 If software updates are delivered via remote access into customers' systems, software vendors should tell customers to turn on modem only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors should advise customers to properly configure a personal firewall product to secure "always-on" connections. PCI Data Security Standard 1.3.10 and 12.3 (A)	**10.1** If the vendor delivers software and/or updates via remote access to customer networks, examine CISP Implementation Documentation (B) prepared by vendor, and verify it contains: • Instructions regarding secure modem use, per PCI Data Security Standard 12.3. • Recommendation for use of a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI Data Security Standard 1.3.10.			
11. Facilitate secure remote access to application				

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
11.1 If employees, administrators, or vendors can access the application remotely, access should be authenticated using a 2-factor authentication mechanism. The application should allow for technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates. PCI Data Security Standard 8.3 (A)	**11.1.a** If customer can access the application remotely, examine CISP Implementation Documentation (B) prepared by the software vendor, and verify it contains instructions regarding secure remote access to the network, including the use of two-factor authentication (username/ password and an additional authentication item such as a token or certificate). **11.1.b** If vendor accesses customers' sites remotely for application support, etc., verify the vendor has processes implemented to: • Restrict access to passwords to authorized vendor personnel, • Protect customers' passwords from unauthorized use, • Establish customer passwords according to Best Practice 3, above, and PCI Data Security Standard 8.1, 8.2, 8.4, 8.5 (or that the vendor provides such instruction to the customer in the CISP Implementation Documentation (B) **11.1.c** If the application requires, or supports use of, a remote access product for remote vendor or customer access (e.g., pcAnywhere), examine CISP Implementation Documentation (B) prepared by the software vendor, and verify that customers are instructed to use and implement all security features of the remote access software. See (E) for more details.			

12. Encrypt sensitive traffic over public networks.

© 2005 Visa U.S.A. Inc.

Best Practices	Testing Procedures	In Place	Not In Place	Target Date / Comments
12.1 Use strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks. PCI Data Security Standard 4.1 [(A)]	**12.1** If the application allows data transmission over the Internet, examine CISP Implementation Documentation [(B)]: prepared by the vendor, and verify the vendor recommends use of SSL for secure data transmission.			
12.2 The application should never send cardholder information via unencrypted e-mail. PCI Data Security Standard 4.2 [(A)]	**12.2.a** If the application allows and/or facilitates sending of email, verify that email encryption features are provided. **12.2.b** If the application allows and/or facilitates the sending of email, examine CISP Implementation Documentation [(B)] prepared by the vendor, and verify the vendor recommends use of email encryption for sending sensitive emails (with cardholder data).			
13. Encrypt all non-console administrative access.				
13. Use technologies such as SSH, or SSL/TLS for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration. PCI Data Security Standard 2.3 [(A)]	**13.** If application or server allows non-console administration, examine CISP Implementation Documentation [(B)]: prepared by vendor, and verify vendor recommends use of SSH or SSL/TLS for secure administrative access.			

[(A)] For references to PCI Data Security Standard, see www.visa.com/cisp
[(B)] For references to CISP Implementation Documentation, Visa suggests vendors document the configuration specifics in this document and strongly advise their customers that the application has to be configured as stated. Vendors may tell customers something similar to "this application, when implemented according to CISP Implementation Documentation, and when implemented into a secure environment, will not keep the customer from being CISP compliant".
[(C)] www.owasp.org, "The Ten Most Critical Web Application Security Vulnerabilities," 2004 Update, January 27, 2004
[(D)] See Visa CISP web site at www.visa.com/cisp for definitions of merchant levels and other program details.

© 2005 Visa U.S.A. Inc.

(E) For example, features like usernames with complex passwords, password protection for dial-in and dial-out files, automatic log off when call is completed, encrypting session traffic, limiting logon attempts, and logging failed attempts are features available in most remote access software, but not enabled by default.

© 2005 Visa U.S.A. Inc.