



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

---

This document is to be used for payment application vendors to validate that the payment application complies with the Visa U.S.A. Payment Application Best Practices (PABP) and to create the Report on Validation.

## **Relationship between PCI DSS and PABP**

The requirements for the PABP are derived from the Payment Card Industry Data Security Standard (PCI DSS) and the PCI DSS Security Audit Procedures. These documents, which can be found at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org), detail what is required to be PCI DSS compliant (and therefore what a payment application must support to facilitate an application user's PCI DSS compliance) and should be used as a reference for the PCI DSS and supporting documentation.

Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

## **Scope of PABP**

The PABP applies to software vendors who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement. The PABP does not apply to payment software developed by merchants and agents if used only in-house (not sold to a third party), since this in-house developed payment software would be covered as part of the merchant's or agent's normal PCI DSS compliance.

NOTE: All validated payment application products must be general releases and not beta versions.

## **Data Retention Requirements**

The following table (from the PCI DSS) illustrates commonly used elements of cardholder data and sensitive authentication data, whether storage of that data is permitted or prohibited, and whether this data needs to be protected. This table is not meant to be exhaustive; its sole purpose is to illustrate the different type of requirements that apply to each data element.

The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and the PABP. If PAN is not stored, processed, or transmitted, PCI DSS and PABP do not apply.

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|                                 | Data Element                 | Storage Permitted | Protection Required | PCI DSS REQ. 3.4 |
|---------------------------------|------------------------------|-------------------|---------------------|------------------|
| Cardholder Data                 | Primary Account Number (PAN) | YES               | YES                 | YES              |
|                                 | Cardholder Name*             | YES               | YES*                | NO               |
|                                 | Service Code*                | YES               | YES*                | NO               |
|                                 | Expiration Date*             | YES               | YES*                | NO               |
| Sensitive Authentication Data** | Full Magnetic Stripe         | NO                | N/A                 | N/A              |
|                                 | CVC2/CVV2/CID                | NO                | N/A                 | N/A              |
|                                 | PIN / PIN Block              | NO                | N/A                 | N/A              |

\* These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.

\*\* Do not store sensitive authentication data subsequent to authorization (not even if encrypted).

### **PABP Implementation Guide**

Validated applications must be capable of being implemented in a PCI DSS-compliant manner. Software vendors are required to provide a PABP Implementation Guide to instruct their customers and resellers/integrators on secure product implementation, to document the secure configuration specifics mentioned throughout this document, and to clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements. It should detail how the customer and/or reseller/integrator should enable security settings within the customer's network, (for example, the PABP Implementation Guide should cover responsibilities and basic features of PCI DSS password security even if this is not controlled by the application, so that the customer or reseller /integrator understands how to implement secure passwords for PCI DSS compliance).

Payment applications, when implemented according to the PABP Implementation Guide, and when implemented into a PCI DSS compliant environment, should facilitate and support customers' PCI DSS compliance.

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

### Qualified Payment Application Security Professional (QPASP) Requirements

- Only Qualified Payment Application Security Professionals (QPASP) employed by Qualified Payment Application Security Companies (QPASC) are allowed to perform PABP audits. Please refer to the Qualified Payment Application Security Company (QPASC) list at [www.visa.com/cisp](http://www.visa.com/cisp) for more information.
- The QPASP must utilize the testing procedures documented in this Payment Application Best Practices document.
- Both QPASP and software vendor must complete and sign the Confirmation of Report Accuracy letters (available at [www.visa.com/cisp](http://www.visa.com/cisp)) and submit to Visa USA in a secure manner along with the Report on Validation.
- Once compliant, Visa will include the software vendor and product version in the Validated Payment Application List at [www.visa.com/cisp](http://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 approval of the report. Software vendors must re-validate their application for PABP compliance utilizing a QPASP if they wish to be “active” on the Visa website. Otherwise, Visa will remove the software vendor’s listing from the website if re-validation is not received by the due date (please refer to Re-Validation section).

### Testing Laboratory

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

- ❑ All common implementations (including region/country specific versions) of the payment application to be tested.
- ❑ Implementation of security devices. At a minimum, the following must be running per PCI DSS requirements: firewall or traffic filtering devices, Network Address Translators (NAT), Port Address Translators (PAT), anti-virus software and encryption.
- ❑ Establishment of PCI DSS compliant operating systems and applications necessary to run the software.

The laboratory implementation must include all systems where the application is implemented. For example, a standard implementation of software vendor’s payment application might include a client/server environment within a retail storefront, and back office or corporate network. The laboratory must simulate the total implementation. It is required that the laboratory is capable of simulating and validating all functions of the software, to include generation of all error conditions and log entries.

Note: Alternatively, the software vendor may elect to have the validation performed at the QPASC’s laboratory provided that the above requirements are met.

### Instructions and Content for Report on Validation

This document is to be used by QPASPs as the template for creating the Report on Validation and must be submitted to Visa securely. All software vendors and product versions which have validated full compliance with PABP will be included on the list of validated payment applications published at [www.visa.com/cisp](http://www.visa.com/cisp). No software vendor and product version will be included until *all* PABP controls are validated to be in place.

All QPASPs must follow the instructions for report content and format when completing a Report on Validation.

## 1. Executive Summary

Include the following:

- Software vendor name
- Software vendor contact information
- Software vendor mailing address
- QPASP name and contact information
- Product Name
- Product Version (if applicable)
- List of resellers and/or integrators for this product
- 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 QPASC'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, including implementation of POS devices, systems, databases, and web servers as applicable
- Describe/diagram each piece of the communication link, including 1) LAN, WAN or internet, 2) host to host software communication, and 3) within host where software is deployed (e.g. how two different processes communicate with each other on the same host)
- All flows of cardholder data
- All payment application related software components, including third party software dependencies
- End to end authentication, including application authentication mechanism, authentication database, and security of data storage
- Describe the typical merchant that this product is sold to (for example, large, small, if industry-specific, Internet, brick-and-mortar) and vendor's customer's base. (e.g. market segment, big customer names).

## 2. Description of Scope of Validation and Approach Taken

- Describe scope of review as defined at Scope of assessment, above
- Describe region/country specific implementations covered
- Timeframe of validation
- List of documentation reviewed

## 3. Findings and Observations

- All QPASP's must use the following template to provide detailed report descriptions and findings
- 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)
- QPASP contact information (include phone number and email address)



## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

- Date of report

### Re-Validation

*No change* - Visa does NOT currently require re-validation for previously validated product versions if *no* changes were made to the compliant payment application version. However, Visa will require a Confirmation of Report Accuracy from the software vendor prior to the expiration date indicating that *no* changes were made to the validated payment application.

*Changes made but does not affect any of the 14 PABP requirements* - If changes were made to a previously validated payment application version but does not impact the compliance of any of the 14 PABP requirements, Visa will require the software vendor to submit a description of each change in addition to a Confirmation of Letter Accuracy indicating so.

*Major changes and product version upgrade* – Changes made to a previously validated payment application version which impact any of the 14 PABP requirements will require a completely new and separate PABP validation performed by a QPASP. All PABP validation requirements apply.

### Definitions

The following definitions pertain to the Validation Procedures and Reporting:

- **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.

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements  | Testing Procedures  | In Place | Not In Place | Target Date / Comments |
|--|---|----------|--------------|------------------------|
| <b>1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data.</b>  |   |          |              |                        |
| <p><b>1.1</b> Do not store sensitive authentication data subsequent to authorization (even if encrypted):</p> <p>Sensitive authentication data includes the data as cited in the following requirements 1.1.1 through 1.1.3:</p> <p><u>PCI Data Security Standard 3.2</u></p>  | <p><b>1.1</b> If sensitive authentication data (see 1.1.1 – 1.1.3 below) is received and deleted, obtain and review methodology for deleting the data to determine that the data is unrecoverable.</p> <p>For each item of sensitive authentication data below, perform the following steps after completing numerous test transactions that simulate all functions of the software, to include generation of error conditions and log entries:</p>   |          |              |                        |
| <p><b>1.1.1</b> Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.</p> <p><i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i></p> <p><i>Note: See PCI DSS Glossary for additional information.</i></p> <p><u>PCI Data Security Standard 3.2.1</u></p> | <p><b>1.1.1</b> Examine the following files created by the application and verify that the full contents of any track from the magnetic stripe on the back of the card are not stored under any circumstance:</p> <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• Transaction logs</li> <li>• History files</li> <li>• Trace files</li> <li>• Debugging and error logs</li> <li>• Audit logs</li> <li>• Database schemas and tables</li> <li>• Database contents</li> </ul> |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements   | Testing Procedures   | In Place | Not In Place | Target Date / Comments |
|---|--|----------|--------------|------------------------|
| <p><b>1.1.2</b> Do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions..</p> <p><i>Note: See PCI DSS Glossary for additional information.</i></p> <p><u>PCI Data Security Standard 3.2.2</u></p> | <p><b>1.1.2</b> Examine the following files created by the application and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:</p> <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• Transaction logs</li> <li>• History files</li> <li>• Trace files</li> <li>• Debugging and error logs</li> <li>• Audit logs</li> <li>• Database schemas and tables</li> <li>• Database contents</li> </ul> |          |              |                        |
| <p><b>1.1.3</b> Do not store the personal identification number (PIN) or the encrypted PIN block.</p> <p><u>PCI Data Security Standard 3.2.3</u></p> <p><i>PIN blocks must never be retained (even if encrypted) after transaction authorization.</i></p>   | <p><b>1.1.3.</b> Examine the following files created by the application, and verify that PINs and encrypted PIN blocks are not stored under any circumstance:</p> <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• Transaction logs</li> <li>• History files</li> <li>• Trace files</li> <li>• Debugging and error logs</li> <li>• Audit logs</li> <li>• Database schemas and tables</li> <li>• Database contents</li> </ul>  |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements  | Testing Procedures   | In Place | Not In Place | Target Date / Comments |
|--|--|----------|--------------|------------------------|
| <p><b>1.1.4</b> Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the software.</p> <p><u>PCI Data Security Standard 3.2</u></p>                                      | <p><b>1.1.4.a</b>, Review the <u>PABP Implementation Guide</u> prepared by the vendor and verify the documentation includes the following instructions for merchants and resellers/integrators:</p> <ul style="list-style-type: none"> <li>• that historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the software)</li> <li>• how to remove historical data</li> <li>• that such removal is absolutely necessary for PCI compliance</li> </ul> |          |              |                        |
|  | <p><b>1.1.4.b</b> Verify the vendor provides a secure wipe tool or procedure to remove the data.</p>   |          |              |                        |
|  | <p><b>1.1.4.c</b> Verify the secure wipe tool or procedure securely removes the data.</p>  |          |              |                        |
| <p><b>1.1.5</b> Securely delete any cryptographic key material or cryptogram stored by previous versions of the software. This could be cryptographic keys used for computation or verification of cardholder data or sensitive authentication data.</p> | <p><b>1.1.5.a</b> Review the <u>PABP Implementation Guide</u> prepared by the vendor and verify the documentation includes the following instructions for merchants and resellers/integrators:</p> <ul style="list-style-type: none"> <li>• that cryptographic material must be removed</li> <li>• how to remove cryptographic material</li> <li>• that such removal is absolutely necessary for PCI compliance</li> </ul>   |          |              |                        |
|  | <p><b>1.1.5.b</b> Verify vendor provides a secure wipe tool or procedure to remove cryptographic material.</p>   |          |              |                        |
|  | <p><b>1.1.5.c</b> Verify the secure wipe tool or procedure securely removes the cryptographic material.</p>  |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements   | Testing Procedures   | In Place | Not In Place | Target Date / Comments |
|---|--|----------|--------------|------------------------|
| <p><b>1.1.6</b> Securely delete any log files, debugging files, and other data sources received from customers for debugging or troubleshooting purposes, to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.</p> <p><u>PCI Data Security Standard 3.2</u></p> | <p><b>1.1.6.a</b> Examine the software vendor's procedures for troubleshooting customers' problems and verify the procedures include:</p> <ul style="list-style-type: none"> <li>• Collection of sensitive authentication data only when needed to solve a specific problem</li> <li>• Storage of such data in a specific, known location with limited access</li> <li>• Collection of only a limited amount of data needed to solve a specific problem</li> <li>• Encryption of sensitive authentication data while stored</li> <li>• Secure deletion of such data immediately after use.</li> </ul>  |          |              |                        |
|   | <p><b>1.1.6.b</b> Select a sample of recent troubleshooting requests from customers, and verify each event followed the procedure examined at 1.1.6.a.</p>   |          |              |                        |
|   | <p><b>1.1.6.c</b> Review the <u>PABP Implementation Guide</u> prepared by the vendor and verify the documentation includes the following instructions for resellers/integrators:</p> <ul style="list-style-type: none"> <li>• resellers/integrators must collect sensitive authentication only when needed to solve a specific problem</li> <li>• Resellers/integrators must store such data only in specific, known locations with limited access</li> <li>• Resellers/integrators must collect only the limited amount of data needed to solve a specific problem</li> <li>• Resellers/integrators must encrypt sensitive authentication data while stored</li> <li>• Resellers/integrators must securely delete such data immediately after use.</li> </ul> |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements   | Testing Procedures   | In Place | Not In Place | Target Date / Comments |
|---|--|----------|--------------|------------------------|
| <b>2. Protect stored cardholder data</b>  |  |          |              |                        |
| <p><b>2.1</b> Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).</p> <p><i>Note: This requirement does not apply to those employees and other parties with a specific need to see full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).</i></p> <p><u>PCI Data Security Standard 3.3</u></p> | <p><b>2.1</b> Review displays of credit card data, including but not limited to POS devices, screens, logs, and receipts, to determine that credit card numbers are masked when displaying cardholder data, except for those with a specific need to see full credit card numbers.</p> |          |              |                        |
| <p><b>2.2</b> Render PAN, at a minimum, unreadable anywhere it is stored, (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:</p> <ul style="list-style-type: none"> <li>• Strong one-way hash functions (hashed indexes)</li> <li>• Truncation</li> <li>• Index tokens and pads (pads must be</li> </ul>  | <p><b>2.2.a</b> Verify that the PAN is rendered unreadable anywhere it is stored, in accordance with PCI Data Security Standard 3.4.</p>   |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements  | Testing Procedures  | In Place | Not In Place | Target Date / Comments |
|--|---|----------|--------------|------------------------|
| <p>securely stored)</p> <ul style="list-style-type: none"> <li>Strong cryptography with associated key management processes and procedures.</li> </ul> <p>The MINIMUM account information that needs to be rendered unreadable is the PAN.</p> <p><u>PCI Data Security Standard 3.4</u></p> <p><i>The PAN must be rendered unreadable anywhere it is stored, even outside the payment application.</i></p> | <p><b>2.2.b</b> If the software vendor stores the PAN for any reason (for example, because log files, debugging files, and other data sources are received from customers for debugging or troubleshooting purposes), verify that the PAN is rendered unreadable in accordance with PCI Data Security Standard 3.4.</p> |          |              |                        |
| <p><b>2.3</b> If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (e.g. not using local system accounts). Decryption keys cannot be tied to local user accounts.</p> <p><u>PCI Data Security Standard 3.4.1</u></p>  | <p><b>2.3</b> If disk encryption is used, verify that it is implemented in accordance with PCI Data Security Standard 3.4.1.a through 3.4.1.c</p>   |          |              |                        |
| <p><b>2.4</b> Application must protect encryption keys used for encryption of cardholder data against disclosure and misuse.</p> <p><u>PCI Data Security Standard 3.5</u></p>  | <p><b>2.4</b> Verify the application protects encryption keys against disclosure and misuse, per PCI Data Security Standard 3.5.</p>  |          |              |                        |
| <p><b>2.5</b> Application must implement key management processes and procedures for keys used for encryption of cardholder data.</p> <p><u>PCI Data Security Standard 3.6</u></p>   | <p><b>2.5</b> Verify the application implements key management techniques, per PCI Data Security Standard 3.6.</p>  |          |              |                        |

### 3. Provide secure password features.

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements  | Testing Procedures   | In Place | Not In Place | Target Date / Comments |
|--|--|----------|--------------|------------------------|
| <p><b>3.1</b> Application must require unique usernames and complex passwords for all administrative access and for all access to cardholder data.</p> <p><u>PCI Data Security Standard 8.1 and 8.2</u></p> <p><i>Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.</i></p> | <p><b>3.1</b> Test the application to verify that unique usernames and complex passwords are required for all administrative access and for all access to cardholder data, in accordance with PCI DSS requirement 8.1, 8.2, and 8.5all.</p>  |          |              |                        |
|  | <p><b>3.1.b</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 must not use the administrative account for database software)</p>   |          |              |                        |
|  | <p><b>3.1.c</b> Examine <u>PABP Implementation Guide</u> created by vendor to verify the following:</p> <ul style="list-style-type: none"> <li>• Customers and resellers/integrators are advised against using administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database).</li> <li>• Customers and resellers/integrators are advised to assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts.</li> <li>• Customers and resellers/integrators are advised to assign strong application and system passwords whenever possible.</li> <li>• Customers and resellers/integrators are advised how to create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15</li> </ul> |          |              |                        |
| <p><b>3.2</b> Access to PCs, servers, and databases with payment applications must require a unique username and complex password.</p> <p><u>PCI Data Security Standard 8.1 and 8.2</u></p>  | <p><b>3.2</b> Examine <u>PABP Implementation Guide</u> created by vendor to verify customers and resellers/integrators are advised to control access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.</p>   |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements  | Testing Procedures   | In Place | Not In Place | Target Date / Comments |
|--|--|----------|--------------|------------------------|
| <p><b>3.3</b> Encrypt application passwords.<br/><u>PCI Data Security Standard 8.4</u></p>   | <p><b>3.3</b> Examine application password files to verify that passwords are encrypted.</p>   |          |              |                        |
| <p><b>4. Log application activity</b></p>  |  |          |              |                        |
| <p><b>4.1</b> Application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users.<br/><u>PCI Data Security Standard 10.1</u></p> | <p><b>4.1</b> Examine application settings to verify that application audit trails are automatically enabled or are available to be enabled by customers.</p>  |          |              |                        |
| <p><b>4.2</b> Application must implement an automated audit trail to track and monitor access.<br/><u>PCI Data Security Standard 10.2 and 10.3</u></p>   | <p><b>4.2.a</b> Examine application log parameters and verify that logs contain the data required in PCI Data Security Standard 10.2 and 10.3.</p> <p><b>4.2.b</b> If application log settings are configurable by the customer and resellers/integrators, or customers or resellers/integrators are responsible for implementing logging, examine <u>PABP Implementation Guide</u> prepared by the vendor to verify that customers are instructed on how to set PCI DSS-compliant log settings, per PCI Data Security Standard 10.2 and 10.3.</p> |          |              |                        |
| <p><b>5. Develop secure applications</b></p>   |  |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

| PABP Requirements  | Testing Procedures  | In Place | Not In Place | Target Date / Comments |
|--|---|----------|--------------|------------------------|
| <p><b>5.1</b> Develop all web applications based on secure coding guidelines such as the <i>Open Web Application Security Project</i> guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include:</p> <p><u>PCI Data Security Standard 6.5</u></p> | <p><b>5.1</b> Obtain and review software development processes for any web-based applications. Verify the process includes training in secure coding techniques for developers, and is based on guidance such as the OWASP guidelines (<a href="http://www.owasp.org">http://www.owasp.org</a>). Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques. For any web-based applications, verify that processes are in place to confirm that applications are not vulnerable to the following:</p> |          |              |                        |
| <b>5.1.1</b> Unvalidated input.  | <b>5.1.1</b> Unvalidated input.   |          |              |                        |
| <b>5.1.2</b> Broken access control (e.g., malicious use of user IDs).  | <b>5.1.2</b> Broken access control (e.g., malicious use of user IDs).   |          |              |                        |
| <b>5.1.3</b> Broken authentication and session management (use of account credentials and session cookies).  | <b>5.1.3</b> Broken authentication and session management (use of account credentials and session cookies).   |          |              |                        |
| <b>5.1.4</b> Cross-site scripting (XSS) attacks.   | <b>5.1.4</b> Cross-site scripting (XSS) attacks.  |          |              |                        |
| <b>5.1.5</b> Buffer overflows.   | <b>5.1.5</b> Buffer overflows.  |          |              |                        |
| <b>5.1.6</b> Injection flaws (e.g., SQL injection).  | <b>5.1.6</b> Injection flaws (e.g., SQL injection).   |          |              |                        |
| <b>5.1.7</b> Improper error handling   | <b>5.1.7</b> Improper error handling  |          |              |                        |
| <b>5.1.8</b> Insecure storage  | <b>5.1.8</b> Insecure storage   |          |              |                        |
| <b>5.1.9</b> Insecure configuration management.  | <b>5.1.9</b> Insecure configuration management.   |          |              |                        |
| <p><b>5.2</b> Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.</p> <p><u>PCI Data Security Standard 6.3</u></p>   | <p><b>5.2</b> Obtain and examine written software development processes to verify that they are based on industry standards and that security is included throughout the life cycle. From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:</p>   |          |              |                        |
| <b>5.2.1</b> Testing of all security patches and system and software configuration changes before deployment   | <b>5.2.1</b> All changes (including patches) are tested before being deployed.  |          |              |                        |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|   |  |  |  |  |
|---|--|--|--|--|
| <p><b>5.2.2</b> Separate development, test, and production environments</p>   | <p><b>5.2.2</b> The test/development environments are separate from the production environment, with access control in place to enforce the separation</p>   |  |  |  |
| <p><b>5.2.3</b> Separation of duties between development, test, and production environments</p>   | <p><b>5.2.3</b> There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment</p>   |  |  |  |
| <p><b>5.2.4</b> Live PANs are not used for testing or development</p>   | <p><b>5.2.4</b> Live PANs are not used for testing and development, or are sanitized before use</p>  |  |  |  |
| <p><b>5.2.5</b> Removal of test data and accounts before production systems become active.</p>  | <p><b>5.2.5</b> Test data and accounts are removed before a production system becomes active</p>   |  |  |  |
| <p><b>5.2.6</b> Removal of custom application accounts, usernames, and passwords before applications are released to customers.</p>   | <p><b>5.2.6</b> Custom application accounts, usernames, and passwords are removed before application is released to customers.</p>   |  |  |  |
| <p><b>5.2.7</b> Review of custom code prior to release to customers, to identify any potential coding vulnerability.</p>  | <p><b>5.2.7.a</b> Confirm the vendor performs code reviews, and that individuals other than the originating author of the code perform the reviews..</p>   |  |  |  |
|   | <p><b>5.2.7.b</b> Confirm that code reviews occur for new code as well as for code changes</p>   |  |  |  |
| <p><b>5.3</b> Software vendor must follow change control procedures for all product software configuration changes. The procedures must include the following:<br/><br/><u>PCI Data Security Standard 6.4</u></p> | <p><b>5.3.a</b> Obtain and examine the vendor's change-control procedures for software modifications, and verify that the procedures require items 5.3.1 – 5.3.4 below</p>   |  |  |  |
|   | <p><b>5.3.b</b> Examine recent software changes, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:</p> |  |  |  |
| <p><b>5.3.1</b> Documentation of impact</p>   | <p><b>5.3.1</b> Verify that documentation of customer impact is included in the change control documentation for each change</p>   |  |  |  |
| <p><b>5.3.2</b> Management sign-off by appropriate parties</p>  | <p><b>5.3.2</b> Verify that management sign-off by appropriate parties is present for each change</p>  |  |  |  |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|   |  |  |  |  |
|---|--|--|--|--|
| <p><b>5.3.3</b> Testing of operational functionality</p>  | <p><b>5.3.3</b> Verify that operational functionality testing was performed for each change</p>  |  |  |  |
| <p><b>5.3.4</b> Back-out procedures</p>   | <p><b>5.3.4</b> Verify that back-out procedures are prepared for each change</p>   |  |  |  |
| <p><b>5.4</b> Disable or remove unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, unencrypted FTP, and others). These services and protocols must not be used or required by the application.</p> <p><u>PCI Data Security Standard 2.2.2</u></p>  | <p><b>5.4</b> Examine 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 (for example, FTP is not enabled, or is encrypted via SSH or other technology).</p>   |  |  |  |
| <p><b>5.5</b> Ensure that all web-facing applications are protected against known attacks by either of the following methods:</p> <ul style="list-style-type: none"> <li>• Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security</li> <li>• Installing an application-layer firewall in front of web-facing applications</li> </ul> <p><u>PCI Data Security Standard 6.6</u></p> <p><i>Note: For PCI DSS, this method is considered a best practice until June 30, 2008, after which it becomes a requirement.</i></p> | <p><b>5.5</b> For web-based applications, ensure that one of the following methods are in place as follows.</p> <ul style="list-style-type: none"> <li>• Verify that custom application code is periodically reviewed by an organization that specializes in application security; that all coding vulnerabilities were corrected; and that the application was re-evaluated after the corrections</li> <li>• Verify that an application-layer firewall is in place in front of web-facing applications to detect and prevent web-based attacks</li> </ul> |  |  |  |

**6. Protect wireless transmissions**

|  |  |  |  |  |
|--|--|--|--|--|
| <p><b>6.1 For wireless networks transmitting cardholder data</b>, encrypt the transmissions by using WiFi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.</p> <p>If WEP is used, do the following:</p> <ul style="list-style-type: none"> <li>• Use with a minimum 104-bit encryption key and 24 bit-initialization value.</li> <li>• Use ONLY in conjunction with WiFi Protected Access (WPA or WPA2) technology, VPN, or SSL/TLS.</li> <li>• Rotate shared WEP keys quarterly (or automatically if the technology permits)</li> <li>• Rotate shared WEP keys whenever there are changes in personnel with access to keys.</li> <li>• Restrict access based on media access code (MAC) address.</li> </ul> <p><u>PCI Data Security Standard 4.1.1</u></p> | <p><b>6.1.a</b> For wireless payment applications, and other wireless applications connected to cardholder data environments, verify that appropriate encryption methodologies implemented in accordance with PCI Data Security Standard 4.1.1.a.</p>  |  |  |  |
|  | <p><b>6.1.b</b> If WEP is used, verify it is used in accordance with in PCI Data Security Standard 4.1.1.b.</p>  |  |  |  |
|  | <p><b>6.1.c</b> If customer could implement the payment application into a wireless environment, examine <u>PABP Implementation Guide</u> prepared by vendor to verify customers and resellers/integrators are instructed on PCI DSS-compliant wireless settings, per PCI Data Security Standard 1.3.9, 2.1.1 and 4.1.1.</p> |  |  |  |



# Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|  |  |  |  |  |
|--|--|--|--|--|
| <p><b>6.2</b> If wireless technology is used within the payment environment, it must be implemented securely.</p> <p><u>PCI Data Security Standard 1.3.8 &amp; 2.1.1</u></p> | <p><b>6.2</b> For wireless payment applications, and other wireless applications connected to cardholder data environments, verify that the wireless technology has been protected with a firewall configuration and that wireless vendor defaults have been changed per PCI Data Security Standard 1.3.8 and 2.1.1.</p> |  |  |  |
|--|--|--|--|--|

## 7. Test applications to address vulnerabilities.

|  |  |  |  |  |
|--|--|--|--|--|
| <p><b>7.1</b> Software vendors must establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet), to test their applications for vulnerabilities, and for timely development and deployment of security patches and upgrades. Updates and patches must 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) must</p> | <p><b>7.1.a</b> Obtain and examine development processes to identify new vulnerabilities and implement corrections into software. Verify the processes include:</p> <ul style="list-style-type: none"><li>• Using outside sources for security vulnerability information</li><li>• Testing of applications for new vulnerabilities</li><li>• Delivery of patches and updates in a secure manner with a known chain-of-trust</li><li>• Timely development and deployment of patches to customers.</li></ul> |  |  |  |
|--|--|--|--|--|



## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|   |  |  |  |  |
|---|--|--|--|--|
| <p>be included in this process.<br/><u>PCI Data Security Standard 6.2</u></p> | <p><b>7.1.b</b> Verify that processes to identify new vulnerabilities and implement corrections into software apply to all software provided with the payment application (e.g., web servers).</p> |  |  |  |
|---|--|--|--|--|

### 8. Facilitate secure network implementation

|   |  |  |  |  |
|---|--|--|--|--|
| <p><b>8.1</b> The payment application must be able to be implemented into a secure network environment. Application must 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 encryption.<br/><u>PCI Data Security Standard 1, 3, 4, and 5</u></p> | <p><b>8.1</b> 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.</p> |  |  |  |
|---|--|--|--|--|

### 9. Cardholder data must never be stored on a server connected to the Internet

|  |  |  |  |  |
|--|--|--|--|--|
| <p><b>9.1</b> The payment application must not require that the database server and web server be on the same server, or in the DMZ with the web server.<br/><u>PCI Data Security Standard 1.3 and 1.3.4</u></p> | <p><b>9.1.a</b> 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 must not require that the database server and web server be on the same server, or in the DMZ with the web server).</p> |  |  |  |
|--|--|--|--|--|



## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|  |  |  |  |  |
|--|--|--|--|--|
|  | <p><b>9.1.b</b> If customer could store cardholder data on a server connected to the Internet, examine <u>PABP Implementation Guide</u> prepared by vendor to verify customers and resellers/integrators are told not to store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)</p> |  |  |  |
|--|--|--|--|--|

### 10. Facilitate secure remote software updates

|   |  |  |  |  |
|---|--|--|--|--|
| <p><b>10.1</b> If software updates are delivered via remote access into customers' systems, software vendors must 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 must advise customers to properly configure a personal firewall product to secure "always-on" connections.</p> <p><u>PCI Data Security Standard 1.3.9 and 12.3.9</u></p> | <p><b>10.1</b> If the vendor delivers software and/or updates via remote access to customer networks, examine <u>PABP Implementation Guide</u> prepared by vendor, and verify it contains:</p> <ul style="list-style-type: none"> <li>• Instructions for customers and resellers/integrators regarding secure modem use, per PCI Data Security Standard 12.3.</li> <li>• Recommendation for customers and resellers/integrators to use 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.</li> </ul> |  |  |  |
|---|--|--|--|--|

### 11. Facilitate secure remote access to application

|  |  |  |  |  |
|--|--|--|--|--|
| <p><b>11.1</b> The payment application must not interfere with use of a two-factor authentication mechanism. The application must allow for technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates.</p> <p><u>PCI Data Security Standard 8.3</u></p> | <p><b>11.1</b> Test the application in a lab to obtain evidence that it can run with a two-factor authentication mechanism (the application must not prohibit an organization's ability to implement two-factor authentication).</p> |  |  |  |
|--|--|--|--|--|



# Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|  |   |  |  |  |
|--|---|--|--|--|
| <p><b>11.2</b> Remote access must be authenticated using a two-factor authentication mechanism.<br/><u>PCI Data Security Standard 8.3</u></p>  | <p><b>11.2</b> If the payment application may be accessed remotely, examine <u>PABP Implementation Guide</u> prepared by the software vendor, and verify it contains instructions for customers and resellers/integrators regarding required use of two-factor authentication (username and password and an additional authentication item such as a token or certificate).</p> |  |  |  |
| <p><b>11.3</b> If vendors, resellers/integrators, or customers can access customers' applications remotely, the remote access software must be implemented securely.<br/><u>PCI Data Security Standard 8.3</u></p> | <p><b>11.3.a</b> If the software vendor uses remote access software for remote access to the customers' application, verify that vendor personnel implement and use remote access software security features. See example below at 11.3.b.</p>  |  |  |  |



**Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures**

|  |   |  |  |  |
|--|---|--|--|--|
|  | <p><b>11.3.b</b> If resellers/integrators or customers can use remote access software, examine <u>PABP Implementation Guide</u> prepared by the software vendor, and verify that customers and resellers/integrators are instructed to use and implement remote access software security features. For example:</p> <ul style="list-style-type: none"><li>• Change default settings in the remote access software (for example, change default Passwords and use unique Passwords for each customer)</li><li>• Allow connections only from specific (known) IP/MAC addresses</li><li>• Use strong authentication or complex Passwords for logins</li><li>• Enable encrypted data transmission</li><li>• Enable account lockout after a certain number of failed login attempts</li><li>• Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed</li><li>• Enable the logging function</li><li>• Restrict access to customer Passwords to authorized reseller/integrator personnel</li><li>• Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, 8.5.</li></ul> |  |  |  |
|--|---|--|--|--|

**12. Encrypt sensitive traffic over public networks.**

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|  |  |  |  |  |
|--|--|--|--|--|
| <p><b>12.1</b> Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and, internet protocol security (IPSEC)) to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p><i>Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).</i></p> <p><u>PCI Data Security Standard 4.1</u></p> | <p><b>12.1</b> If the application allows data transmission over the Internet, examine <u>PABP Implementation Guide</u> prepared by the vendor, and verify the vendor recommends use of SSL for secure data transmission in accordance with PCI DSS requirement 4.1.</p>                      |  |  |  |
| <p><b>12.2</b> The application must never send unencrypted PANs by e-mail.</p> <p><u>PCI Data Security Standard 4.2</u></p>  | <p><b>12.2.a</b> If the application allows and/or facilitates sending of PANs by e-mail, verify that an e-mail encryption solution is provided.</p>  |  |  |  |
|  | <p><b>12.2.b</b> If the application allows and/or facilitates the sending of PANs by e-mail, examine the <u>PABP Implementation Guide</u> prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use an email encryption solution.</p> |  |  |  |
| <p><b>13. Encrypt all non-console administrative access.</b></p>   |  |  |  |  |
| <p><b>13.1</b> Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</p> <p><u>PCI Data Security Standard 2.3</u></p> <p><i>Telnet or rlogin must never be used for non-console administrative access.</i></p>  | <p><b>13.1</b> If application or server allows non-console administration, examine the <u>PABP Implementation Guide</u> prepared by vendor, and verify vendor recommends use of SSH, VPN, or SSL/TLS for encryption of non-console administrative access.</p>                                |  |  |  |
| <p><b>14. Maintain instructional documentation and training programs for customers, resellers, and integrators.</b></p>  |  |  |  |  |

## Visa U.S.A. CISP Payment Application Best Practices & Audit Procedures

|   |  |  |  |  |
|---|--|--|--|--|
| <p><b>14.1</b> Develop, maintain, and disseminate a <u>PABP Implementation Guide(s)</u> for customers, resellers, and integrators that accomplishes the following:</p>  | <p><b>14.1</b> Examine the <u>PABP Implementation Guide</u> and related processes, and verify the guide is disseminated to all relevant application users (including customers, resellers, and integrators).</p>               |  |  |  |
| <p><b>14.1.1</b> Addresses all requirements in this document wherever the <u>PABP Implementation Guide</u> is referenced.</p>   | <p><b>14.1.1</b> Verify the <u>PABP Implementation Guide</u> covers all related requirements in this document.</p>   |  |  |  |
| <p><b>14.1.2</b> Includes a review at least annually and updates to keep the documentation current with software changes as well as with changes to the requirements in this document.</p>  | <p><b>14.1.2</b> Verify the <u>PABP Implementation Guide</u> is reviewed on an annual basis and updated for changes to software and for changes to the requirements in this document.</p>                                      |  |  |  |
| <p><b>14.2</b> Develop and implement training and communication programs to ensure software resellers and integrators know how to implement the application software and related systems and networks in a PABP-compliant manner. Update the training on an annual basis and whenever new software versions are released.</p> | <p><b>14.2.a</b> Examine the training materials and communication program for resellers and integrators, and confirm the materials cover all items noted for the <u>PABP Implementation Guide</u> throughout this document</p> |  |  |  |
|   | <p><b>14.2.b</b> Examine the training materials for resellers and integrators and verify the materials are updated on an annual basis and when new software versions are released.</p>   |  |  |  |
|   | <p><b>14.2.c</b> Select a sample of resellers and integrators and interview them to verify they received the training materials.</p>   |  |  |  |