Payment Card Industry (PCI)

Payment Application Data Security Standard

Summary of Changes from *Payment Application Best Practices v1.4*

Version 1.1

April 2008

Payment Application Data Security Standard Version 1.1

Summary of Changes from *Payment Application Best Practices v1.4*

Old Requirement	New Requirement	Change	Type [i]
General	N/A	▪ Changed "Payment Application Best Practices" to "Payment Application Data Security Standard." ▪ Changed "PABP" to "PA-DSS." ▪ Changed "Qualified Payment Application Security Company/Professional" to "Payment Application–Qualified Security Assessor." ▪ Changed "QPASC" or "QPASP" to "PA-QSA." ▪ Changed "merchant" references to "customer." ▪ Changed all references to the application, software, etc. to "payment application."	N/A
General	N/A	**Relationship between PCI DSS and PA-DSS**: Added second paragraph to further explain relationship.	Explanatory
General	N/A	**Scope of PA-DSS**: Added wording to clarify what types of applications PA-DSS applies to, what is and what is not a payment application, and to provide more detailed scoping information.	Explanatory
General	N/A	**Data Retention Requirements:** Renamed section to "PCI DSS Applicability Information" and moved section further into document.	N/A
General	N/A	**PA-DSS Applicability to Hardware Terminals**: New section added to explain that hardware terminals meeting specified criteria do not need to undergo a PA-DSS review.	Explanatory
General	N/A	**Responsible Parties—PA DSS**: New section added to explain the PA-DSS responsibilities of: ▪ Software vendors ▪ Customers (merchants, service providers, and others who buy or receive third-party payment applications) ▪ Resellers & Integrators (entities that sell, install, and/or service payment applications on behalf of software vendors or others) ▪ PCI SSC ▪ Payment brands	Explanatory
General	N/A	***PA-DSS Implementation Guide*:** Added note at end of section to reference new Appendix A covering responsibilities for implementing controls specified in the *PA-DSS Implementation Guide*.	Explanatory

Old Requirement	New Requirement	Change	Type [i]
General	N/A	**Payment Application Qualified Security Assessor (PA-QSA) Requirements**: Deleted bullets specific to Visa's compliance process.	Clarification
General	N/A	**Testing Laboratory**: Deleted most of this section and refer instead to new *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment*.	Clarification
General	N/A	**PCI DSS Applicability Information**: Renamed and moved previous PABP section "Data Retention Requirements."	N/A
General	N/A	**Instructions and Content for Report on Compliance**: Deleted or replaced content specific to Visa's compliance process. Reordered listed items and enhanced requested report content.	Clarification
General	N/A	**Re-Validation**: Deleted whole section since this item is now covered in the PA-DSS Program Guide	Clarification
General	N/A	**Definitions**: Deleted section.	Clarification
General	N/A	**PA-DSS Completion Steps**: Added section to provide guidance to PA-QSA on steps to finalize review and submit documentation to PCI SSC.	Enhancement
General	N/A	**PA-DSS Program Guide**: Added section to refer to and summarize contents of the PA-DSS Program Guide.	Enhancement
1.1.1 1.1.2 1.1.3	1.1.1 1.1.2 1.1.3	**Testing Procedures**: Changed procedure to require use of forensic tools and/or methods to examine all output to look for sensitive authentication data. Added "Non-volatile memory, including non-volatile cache" to list of items to be examined by forensic tools and/or methods.	Enhancement
1.1.4	1.1.4	**Requirement and Testing Procedure**: Added explanation that deletion should occur in accordance with industry-accepted standards for secure deletion. Require use of forensic tools or methods to verify that the secure wipe tool or procedure provided by the vendor securely removes data.	Enhancement
1.1.5	2.7	**Requirement and Testing Procedure**: Moved to 2.7.	Clarification
1.1.6	1.1.5	**Requirement and Testing Procedure**: Clarified that requirement refers to sensitive authentication data used for debugging or troubleshooting purposes. Minor change to clarify that in addition to resellers and integrators, customers should also be addressed by the *PA-DSS Implementation Guide.*	Clarification

Old Requirement	New Requirement	Change	Type [i]
New	2.1	**New Requirement**: Added 2.1 for vendor to provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period.	Enhancement
2.1	2.2	Requirement numbering change	N/A
2.2	2.3	Requirement numbering change	N/A
2.3	2.4	**Requirements**: Clarified that example provided should be "local user account databases."	Clarification
2.4	2.5	Requirement numbering change	N/A
2.5	2.6	Requirement numbering change	N/A
1.1.5	2.7	**Requirement and Testing Procedure**: Moved former requirement 1.1.5 to new requirement 2.7. Added explanation that deletion should occur in accordance with industry-accepted standards for secure deletion. Added test that requires use of forensic tools or methods to verify that the secure wipe tool or procedure provided by the vendor securely removes cryptographic material.	Clarification & Enhancement
3 (all)	3 (all)	**Requirements and Testing Procedures**: Changed all references to "strong" or "complex" passwords to "secure authentication" to include other forms of authentication (tokens, biometrics, etc.).	Clarification
3.1	3.1	**Requirement**: Added clarification that this requirement applies to the application as it is provided from the vendor (out-of-the-box installation), and that vendor must advise customers that changes may result in non-compliance with PCI DSS.	Clarification
3.3	3.3	**Requirement**: Wording changed to match related PCI DSS v1.1 Requirement 8.4, which requires that passwords be encrypted during both transmission and storage.	Clarification
4.1	4.1	**Requirement**: Added clarification that this requirement applies to the application as it is provided from the vendor (out-of-the-box installation).	Clarification
4.2	4.2	**Testing Procedures**: Added bullet for *PA-DSS Implementation Guide,* stating that content should include instructions that disabling of the logs should not be done.	Clarification
5.1 5.2	5.2 5.1	**Requirements & Testing Procedures**: For clarity, reversed the order of these two requirements—5.2 (SDLC) became 5.1, and 5.1 (OWASP) became 5.2.	Clarification

Old Requirement	New Requirement	Change	Type [i]
5.2.1	5.1.1	**Requirements & Testing Procedures**: Added 5.1.1.1–5.1.1.5, to specify items to be included in the testing process for security patches and system software and configuration changes.	Enhancement
5.2.2-5.2.6	5.1.2-5.1.6	Requirement numbering changes	N/A
5.2.7	5.1.7	**Testing Procedures**: Added an alternate option to Test 5.1.7.a, for use of a code analysis tool for security vulnerabilities. Added Test 5.1.7.c to verify that a documented code review/analysis process is followed and that process contains key steps. Also added Test 5.1.7.d to confirm that vendor's applications are reviewed by an organization that specializes in application security or that a tool is used that analyzes code for security vulnerabilities.	Enhancement
5.1	5.2	**Requirements & Testing Procedures**: Added clarification that requirement applies to all web applications, whether internal, external, or administrative applications. Removed requirement to "Review custom code to identify coding vulnerabilities" since this is also covered by new 5.1.7.	Clarification
5.1	5.2.b	**Testing Procedures**: Moved last part of former 5.1 test procedure to new Test 5.2.b. Also, changed 5.2.b to require the assessor to attempt to exploit vulnerabilities in 5.2.1–5.2.10, rather than to review vendor processes.	Enhancement
5.1.1 – 5.1.10	5.2.1 – 5.2.10	**Requirements & Testing Procedures**: Changed each to match new *Open Web Application Security Project Guide* (new "Top Ten").	Clarification
5.3.4	5.3.4	**Requirements & Testing Procedures**: Added product de-installation in addition to back-out for changes.	Clarification
5.4	5.4	**Requirement**: Changed "Disable" to "The payment application must not use or require the use of" in relation to insecure services and protocols	Clarification
5.5	N/A	**Requirements & Testing Procedures**: This requirement, which maps to PCI DSS Requirement 6.6, was deleted since the implementation of this requirement is the responsibility of the customer, and not the software vendor.	Clarification
6.1 6.2	6.2 6.1	**Requirement & Testing Procedures**: For clarity, reversed the order of these two requirements—6.2 became 6.1, and 6.1 became 6.2.	Clarification

Old Requirement	New Requirement	Change	Type [i]
6.2	6.1	**Requirement & Testing Procedures**: Added wording to clarify that if a payment application is designed or bundled with wireless technology, wireless must be configured in accordance with PCI DSS Requirement 2.1.1. Split testing procedures as follows: 6.1.a to verify wireless is configured in accordance with PCI DSS Requirement 2.1.1, and 6.1.b to ensure the implementation guide advises customers and resellers/integrators to install a firewall per PCI DSS Requirement 1.3.8 where wireless is used.	Clarification
6.1	6.2	**Requirement**: Changed wording in requirement to clarify that if a payment application is designed or bundled with wireless technology, and if WEP is used, it must be done in conjunction with secure encryption transmission technology; and removed reference to WPA or WPA2 in WEP bullets.	Clarification
7.1	7.1	**Requirement & Testing Procedures**: Split 7.1 and moved portions into new 7.2. 7.1 now focuses on process to identify and correct software vulnerabilities.	Enhancement
New	7.2	**Requirement & Testing Procedures**: Added to address integrity of code added during patches and software updates. Enhances testing procedures previously in 7.1.	Enhancement
8.1	8.1	**Requirements & Testing Procedures**: Broadened wording to eliminate mention of specific controls or technologies, and to instead state that the application must not interfere with any devices, applications, or configurations required by PCI DSS.	Clarification
9.1	9.1	**Requirement**: Reworded for clarification	Clarification
10.1	10.1	**Requirements & Testing Procedures**: Added “a firewall” as a product that can be used to secure an always-on connection.	Clarification
11.2	11.2	**Requirements**: Added “to the payment application” to clarify that this requirement applies to remote access to the payment application.	Clarification
11.3	11.3	**Requirements & Testing Procedures**: Deleted “software” from requirement and testing procedures to emphasize that all remote-access products need to be implemented securely, not just software products. For 11.3.a, removed reference to 11.3.b and copied remote access security features from 11.3.b.	Clarification

Old Requirement	New Requirement	Change	Type [i]
12.1	12.1	**Requirements & Testing Procedures**: Changed emphasis of requirement to "application must support use of" encrypted transmissions. Also, added wording for "secure encrypted transmission technology" to align with 6.2 above. Added Test 12.1.a to verify that vendor either provides encrypted transmissions technology or specifies use of such technology. Original 12.1.a became 12.1.b.	Clarification
12.2	12.2	**Requirements & Testing Procedures**: Changed emphasis of requirement to all "end-user messaging technologies" (includes instant messaging and chat), rather than just e-mail.	Clarification
14.1.2	14.1.2	**Requirement and Testing Procedure**: Enhanced requirement so that all major and minor payment application changes are documented, and created related new Testing Procedure 14.1.2.a. Original 14.1.2.a became 14.1.2.b	Enhancement
14.2	14.2	**Requirements & Testing Procedures**: Moved last sentence to new Requirement 14.2.1. Added new Test 14.2.1.b for verifying that new documentation is distributed along with new software versions. Added new Test 14.2.1.c for verifying that resellers and integrators are interviewed to verify receipt of training materials.	Enhancement
New	Appendix A (new)	**Appendix A**: Added to summarize and explain the *PA-DSS Implementation Guide* and the responsibilities for implementing the related controls.	Explanatory
New	Appendix B (new)	**Appendix B**: Added for PA-QSAs to use with each PA-DSS assessment, to confirm the status and capabilities of the laboratory environment and processes used to validate the application.	Enhancement

[i] Explanatory: Explanations and/or definitions to increase understanding
Clarification: Clarifies intent of requirement
Enhancements: Changes needed to move program from best practice to more robust industry standard