Payment Card Industry (PCI) Data Security Standard

Summary of Changes

Requirement	Change
General	Consistent use of terms cardholder data and sensitive authentication data throughout the standard. Replaced terms like data and information.
General	Replaced vague terms such as periodically, regularly with annually, monthly, quarterly.
General	Consistent use of MUST and SHOULD throughout the document.
General	Removed paragraph at bottom of page 1 "Note that these Payment Card Industry (PCI) Data Security Requirements apply to all Members, merchants, and service providers that store, process or transmit cardholder data."
General	Added a preface and table on page 2 to describe components of cardholder data and sensitive authentication data and clarify the cardholder data environment.
1	Added clarification to description of Requirement 1 (before details of requirement starts)
1.1.3	Replaced Intranet with internal network zone
1.2	Deleted sub-requirements (1.2.1 – 1.2.3) due to confusion, consolidated intent of requirement into 1.2
1.3.2	Deleted requirement and added "inbound and" to 1.3.6 to cover 1.3.2.
2.2	Added wording to state that configuration standards should be consistent with other standards (NIST, SANS, etc.).
2.4 (NEW)	Added hosting provider requirement and Appendix A - PCI DSS Applicability for Hosting Providers, to govern PCI DSS compliance for providers that host merchants and service providers
3	Added clarification to description of Requirement 3 (before details of requirement starts), to include elements of Requirement 3 that are not encryption related (e.g., data retention, masking).
3.2	Added clarifications for storage of track data, and added definition of sensitive authentication data.
3.2.1	Removed "CVV" since this is part of the magnetic stripe and redundant with the already-existing prohibition against storage of magnetic stripe data
3.2.3	1. Removed "PVV" since PVV is part of the magnetic stripe and redundant with 3.2.1. 2. Changed focus of requirement to PINs and encrypted PIN blocks.
3.3	Added wording to note (under requirement) that requirement does not supersede stricter requirements that may be in place for displays of cardholder data (e.g., for POS receipts).
3.4	1. Removed examples of strong cryptography from bullet and instead include examples in the definition of "strong cryptography" in the new Glossary. 2. Added information about how disk encryption should be implemented, if used. 3. Added reference from this requirement to new Appendix A, for those unable to render data unreadable.
4	Added clarification to description of Requirement 4 (before details of requirement starts), that requirement applies to "open, public networks." Clarified the intent of the requirement.
4.1	1. Clarified language 2. Added examples of open, public networks.

4.1.1	1. Added clarifications for wireless requirements to reflect changes in technology. 2. Added more specifics about implementing WEP appropriately. 3. Provided better guidance for key rotation.
5 & 5.1	Added clarification to description of Requirement 5 (before details of requirement starts) and at 5.1 to clarify the types of systems for which anti-virus software is applicable.
5.1.1 (NEW)	New requirement that malicious software, such as spyware and adware, are included in anti-virus software capabilities.
6	Added clarification to description of Requirement 6 (before details of requirement starts) to clarify this requirement .
6.3.4	Changed “real credit cards” to “live PANs.”
6.5	Changed “web software and applications” to “all web applications.”
6.6 (NEW)	1. Added requirement for application code review or application firewall. 2. Added note that this is considered a best practice until June 30, 2008, after which it will be a requirement.
9.5	Changed the wording to better reflect the requirement’s intent.
10.7	Changed wording to clarify intent that audit logs must be retained for at least one year, with a minimum of three months available online.
11.1	Clarified that wireless analyzers should be used periodically, even if wireless is not currently deployed.
11.3	Added 11.3.1 and 11.3.2 to clarify already existing requirement that penetration tests should include both network-layer and application-layer penetration tests.
11.5	Changed the requirement from daily to at least weekly.
12.3.10	Changed focus of requirement to prohibit, via policy, storage of cardholder data, copying etc. during remote access. Formerly required disabling such access.
12.6 & 12.6.1	Changed the wording to better focus on information security awareness. Also, added the phrase “upon hire and at least annually.”
12.8	Shortened and clarified the intent of the legal contract requirement and related sub-requirements.
12.10 (NEW)	Added requirement for a policy to manage connected entities, including maintaining a list, implementing appropriate due diligence, ensuring connected entities are PCI DSS compliant, and having an established process to connect and disconnect entities.
Appendix A (NEW)	Added Appendix A- PCI DSS Applicability for Hosting Providers. Establishes requirements for providers that host merchant and service provider clients.
Appendix B (NEW)	Added Appendix B – Compensating Controls. Defines compensating controls in general and discusses compensating controls when stored cardholder data cannot be rendered unreadable.