Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

Security
Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI COUNCIL PUBLISHES PCI DSS AND PA-DSS VERSION 3.0

—Updated standards to help organizations make payment security business-as-usual—

WAKEFIELD, Mass., 07 November 2013 — Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards, published version 3.0 of the PCI Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS). Available now on the PCI SSC website, version 3.0 becomes effective on 01 January 2014.Version 2.0 will remain active until 31 December 2014 to ensure adequate time for organizations to make the transition.

Changes are made to the standards every three years, based on feedback from the Council's global constituents per the PCI DSS and PA-DSS development lifecycle and in response to market needs. Proposed changes for version 3.0 were shared publicly in August, and Participating Organizations and assessors had the opportunity to discuss the draft standards at the 2013 Community Meetings prior to final publication.

Version 3.0 will help organizations make payment security part of their business-as-usual activities by introducing more flexibility, and an increased focus on education, awareness and security as a shared responsibility.

Overall updates include specific recommendations for making PCI DSS part of everyday business processes and best practices for maintaining ongoing PCI DSS compliance; guidance from the Navigating PCI DSS Guide built in to the standard; and enhanced testing procedures to clarify the level of validation expected for each requirement. New requirements include:

PCI DSS

- **Req. 5.1.2** - evaluate evolving malware threats for any systems not considered to be commonly affected
- **Req. 8.2.3** - combined minimum password complexity and strength requirements into one, and increased flexibility for alternatives
- **Req. 8.5.1** - for service providers with remote access to customer premises, use unique authentication credentials for each customer*
- **Req. 8.6** - where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) these must be linked to an individual account and ensure only the intended user can gain access
- **Req. 9.3** - control physical access to sensitive areas for onsite personnel, including a process to authorize access, and revoke access immediately upon termination

- **Req. 9.9** - protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution*
- **Req. 11.3 and 11.3.4** - implement a methodology for penetration testing; if segmentation is used to isolate the cardholder data environment from other networks, perform penetration tests to verify that the segmentation methods are operational and effective*
- **Req. 11.5.1** - implement a process to respond to any alerts generated by the change-detection mechanism
- **Req. 12.8.5** - maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity
- **Req. 12.9** - for service providers, provide the written, agreement/acknowledgment to their customers as specified at requirement 12.8.2*

PA-DSS

- **Req. 5.1.5 –** payment application developers to verify integrity of source code during the development process
- **Req. 5.1.6 –** payment applications to be developed according to industry best practices for secure coding techniques
- **Req. 5.4 -** payment application vendors to incorporate versioning methodology for each payment application
- **Req. 5.5** - payment application vendors to incorporate risk assessment techniques into their software development process
- **Req. 7.3** - application vendor to provide release notes for all application updates
- **Req. 10.2.2 -** vendors with remote access to customer premises (for example, to provide support/maintenance services) use unique authentication credentials for each customer
- **Req. 14.1 –** provide information security and PA-DSS training for vendor personnel with PA-DSS responsibility at least annually

**Indicates future dated requirements that are best practices until 01 July 2015.*

Organizations can access the standards and detailed summary of changes from version 2.0 to version 3.0 at the PCI SSC website:
https://www.pcisecuritystandards.org/security_standards/documents.php

Click here to view an infographic on PCI DSS 3.0.

Supporting documentation including updated Self-Assessment Questionnaires (SAQ), Attestations of Compliance (AOC) and Reporting Templates will be available in early 2014 once version 3.0 is effective.

“Over the course of several years now, the PCI Security Standards Council has done a laudable job at defining and evolving a cohesive set of standards, as well as at listening and adapting over time to the feedback from merchants, banks, payment processors, service providers, and technology providers,” said Derek Brink, vice president and research fellow, Aberdeen Group. “The stakeholders in the payment card community seem to be working to put security and compliance in the right relationship – i.e., that compliance does not drive security; compliance is the result of foundational security practices."

"PCI Standards continue to provide a strong framework for payment card security," said Bob Russo, general manager, PCI SSC. "The core principles at work when we first published PCI DSS are still relevant today. Version 3.0 builds on these to address the feedback we've heard from our community and to help organizations make payment security good business practice – every day, all year round."

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has more than 650 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC