Security Standards Council

Payment Card Industry
Security Standards Council, LLC

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

Media Contacts

Laura K. Johnson
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org

PCI SECURITY STANDARDS COUNCIL RELEASES VERSION 2.0 OF THE PCI DATA SECURITY STANDARD AND PAYMENT APPLICATION DATA SECURITY STANDARD

—Feedback from global stakeholders shapes revisions; new standards and website ease implementation for merchants—

WAKEFIELD, Mass., October 28, 2010 — The PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), today released version 2.0 of the PCI DSS and PA-DSS. Reflecting input from the Council's global stakeholders, this latest version is designed to provide greater clarity and flexibility to facilitate improved understanding of the requirements and eased implementation for merchants. Version 2.0 becomes effective on January 1, 2011.

The updated standards were the main topic of discussion at the Council's Annual Community Meetings in Orlando, Florida and Barcelona, Spain where, in the last stage of the lifecycle process, stakeholders had the opportunity for final review of the standards. More than 1,500 people from 600 organizations around the world participated in these gatherings, adding to the thousands of pieces of feedback the Council received from merchants, banks, processors and the PCI community throughout the development process.

A summary of changes to the standards was shared with the market prior to the release, highlighting the main types of revisions that include clarifications, additional guidance and evolving requirements.

Version 2.0 does not introduce any new major requirements. The majority of changes are modifications to the language, which clarify the meaning of the requirements and

—more—

make understanding and adoption easier for merchants. Key revisions serve to reinforce the need for a thorough scoping exercise prior to assessment in order to understand where cardholder data resides; promote more effective log management in securing cardholder data; allow organizations to adopt a risk-based approach when assessing and prioritizing vulnerabilities that is based on their specific business circumstances; and accommodate the unique environments of small merchants to simplify their compliance efforts.

The standards, detailed summary of changes and supporting documentation can be found at https://www.pcisecuritystandards.org/security_standards/documents.php.

“The nature of the changes is a testament to the strength and growing global maturity of the standards as a framework for securing cardholder data,” said Bob Russo, general manager of the Council. “I want to thank each and every individual and organization who contributed to the development of these standards. It’s their input that’s critical in making the PCI Security Standards an excellent baseline for protecting payment card data.”

In addition to the standards documents, the Council has also launched a new website with updated materials and navigational tools aimed at providing its diverse stakeholders with the targeted information they need to understand the standards and how to apply them in their organizations. As part of a broader initiative to help small merchants develop their PCI security programs, it also includes a dedicated site for this key group with resources to address their unique environments.

The release of version 2.0 begins the new three year lifecycle for standards development, which streamlines the development process by aligning DSS, PA-DSS and PTS on a similar three year schedule. The lifecycle also allows for minor revisions or errata to be issued throughout the cycle as necessary.

The new standards are effective January 1, 2011, but validation against the previous version of the standard (1.2.1) will be allowed until December 31, 2011. This gives stakeholders more time to understand and implement the new versions of the standards as well as provide feedback throughout the process. However, the Council encourages organizations to transition to the updated version as soon as possible. From January 1, 2012 and moving forward, all assessments must be under version 2.0 of the standards.

The Council also invites Participating Organizations and the public to a webinar that covers the updated standards in greater depth, followed by a Q&A session with representatives from the Council's Technical Working Group. Registration details can be found here:

November 9, 3:00 p.m. ET / noon PT (Participating Organizations only)
November 11, 11:00 a.m. ET / 8:00 a.m. PT (Participating Organizations only)
November 16, 3:00 p.m. ET / noon PT
November 18, 11:00 a.m. ET / 8:00 a.m. PT

For More Information:
For more information on the PCI Security Standards Council and how to become a Participating Organization, please visit www.pcisecuritystandards.org or contact the PCI SSC Secretariat at secretariat@pcisecuritystandards.org.

About the PCI Security Standards Council
The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the PCI Data Security Standard (DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors and other vendors are encouraged to join as participating organizations.

###