Media Contacts

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

Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SECURITY STANDARDS COUNCIL PUBLISHES CARD PRODUCTION SECURITY REQUIREMENTS

— New PCI Standard for card vendors to improve the secure manufacture, production and delivery of payment cards—

WAKEFIELD, Mass., 09 May 2013 — Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards announced the publication of a standard for secure payment card production.

The standard consists of two sets of requirements: *PCI Card Production Physical Security Requirements* and *PCI Card Production Logical Security Requirements*. Together, these documents provide card vendors with a comprehensive source of information describing the security requirements to follow for card production activities including card manufacture, chip embedding, magnet-stripe encoding, embossing, card personalization, chip initialization, chip personalization.

Formerly managed as separate requirements by each payment card brand, the Council aligned these requirements and solicited feedback from the PCI community to produce one set of criteria recognized across the industry. The resulting standard is designed to secure the components and sensitive data involved in the production of payment cards and protect against the fraudulent use of card materials. It's broken down into two core areas:

- **Physical security requirements** – for all card vendors, these requirements address the presence, movement, and accountability of a card, including tangible features such as the security of the premises, personnel access to secure areas, and CCTV surveillance.

- **Logical security requirements** – for card personalization vendors, these requirements address threats to the confidentiality of personalization data during data transfer, access, storage, and destruction; and all aspects associated with cryptographic key management, including the protection of issuer keys used in the personalization process.

These security requirements are available for immediate download at: https://www.pcisecuritystandards.org/security_standards/documents.php. Vendors should work

with the individual card brands to confirm timing for when future security reviews must be performed against the new PCI Card Production Security Requirements.

In line with other PCI Standards, the requirements will be updated on a three-year lifecycle, based on feedback from the PCI community.

“There are a lot of pieces involved in securely producing payment cards, from design all the way through delivery,” said Bob Russo, general manager, PCI Security Standards Council. “The publication of these requirements gives card vendors one set of criteria to follow, and as we’ve seen with our other standards, will help drive improved security across the payments chain.”

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