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

Media Contacts

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

PCI SECURITY STANDARDS COUNCIL PUBLISHES THIRD-PARTY SECURITY ASSURANCE GUIDANCE

—PCI Special Interest Group guidance provides merchants with payment security best practices for working with third-party providers—

WAKEFIELD, Mass., 7 August 2014 — Businesses are rapidly adopting a third-party operations model that can put payment data at risk. Today, the PCI Security Standards Council, an open global forum for the development of payment card security standards, published guidance to help organizations and their business partners reduce this risk by better understanding their respective roles in securing card data. Developed by a PCI Special Interest Group (SIG) including merchants, banks and third-party service providers, the information supplement provides recommendations for meeting PCI Data Security Standard (PCI DSS) requirement 12.8 to ensure payment data and systems entrusted to third parties are maintained in a secure and compliant manner.

Breach reports continue to highlight security vulnerabilities introduced by third parties as a leading cause of data compromise. According to a 2013 study[1] by the Ponemon Institute, the leading mistake organizations make when entrusting sensitive and confidential consumer information to third-party vendors is not applying the same level of rigor to information security in vendor networks as they do in their own.

Per PCI DSS Requirement 12.8, if a merchant or entity shares cardholder data with a third-party service provider, certain requirements apply to ensure continued protection of this data will be enforced by such providers. The *Third-Party Security Assurance Information Supplement* focuses on helping organizations and their business partners achieve this by implementing a robust third-party assurance program. Produced with the expertise and real-world experience of more than 160 organizations involved in the Special Interest Group, the guidance includes practical recommendations on how to:

- Conduct due diligence and risk assessment when engaging third party service providers to help organizations understand the services provided and how PCI DSS requirements will be met for those services.
- Implement a consistent process for engaging third-parties that includes setting expectations, establishing a communication plan, and mapping third-party services and responsibilities to applicable PCI DSS requirements.

[1] Securing Outsourced Consumer Data, Ponemon Institute, February 2013

- Develop appropriate agreements, policies and procedures with third-party service providers that include considerations for the most common issues that arise in this type of relationship.
- Implement an ongoing process for maintaining and managing third-party relationships throughout the lifetime of the engagement, including the development of a robust monitoring program.

The guidance includes high-level suggestions and discussion points for clarifying how responsibilities for PCI DSS requirements may be shared between an entity and its third-party service provider, as well as a sample PCI DSS responsibility matrix that can assist in determining who will be responsible for each specific control area.

PCI Special Interest Groups are PCI community-selected and developed initiatives that provide additional guidance and clarifications or improvements to the PCI Standards and supporting programs. As part of its initial proposal, the group also made specific recommendations that were incorporated into PCI DSS requirements 12.8 and 12.9 in version 3.0 of the standard.

“One of the big focus areas in PCI DSS 3.0 is security as a shared responsibility,” said Bob Russo, PCI SSC General Manager. “This guidance is an excellent companion document to the standard in helping merchants and their business partners work together to protect consumers’ valuable payment information.”

The *Third-Party Security Assurance Information Supplement* is available on the PCI SSC website at: https://www.pcisecuritystandards.org/security_standards/documents.php.
As with all PCI Council information supplements, the guidance provided in this document is supplemental and does not supersede or replace any PCI DSS requirements.

To learn more about the Third-Party Security Assurance guidance and to participate in the 2015 SIG selection process, register to attend the PCI Community Meetings: http://community.pcisecuritystandards.org/

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, JCB International, MasterCard 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