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

PCI SECURITY STANDARDS COUNCIL RELEASES UPDATED PCI DSS WIRELESS GUIDELINES

—Guidance now aligned with PCI DSS 2.0; recommendations on Bluetooth and rogue wireless access points added -

WAKEFIELD, Mass., August 26, 2011 —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 published an update to the *PCI DSS Wireless Guidelines Information Supplement*, providing organizations with the current PCI DSS considerations for implementing wireless technology securely in payments environments.

A product of collaboration with the Council's Wireless Special Interest Group – comprised of more than 40 participants from POS vendors and network security companies to acquiring banks and large merchants - the wireless guidelines were first published in 2009 to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless and to provide practical methods and concepts for deployment of secure wireless in payment card transaction environments.

With the release of PCI DSS version 2.0, the Wireless SIG chaired by Doug Manchester, director, product security, VeriFone, and its Bluetooth sub-group, led by Tim Cormier, director of POS systems, Ingenico, worked with the Council to update and align the language in the information supplement with the newest version of the Standard.

—more—

In response to feedback from the PCI community on areas needing additional clarification, the group also added guidance specific to Bluetooth technologies and rogue wireless access points, including:

- Additional considerations for Bluetooth technology within the cardholder data environment (CDE)
- Recommended methods for testing and detecting rogue wireless access points per PCI DSS requirement 11.1

By identifying some of the key PCI DSS requirements related to wireless and providing recommendations for its use in a PCI DSS compliant manner, the information supplement helps organizations evaluate the potential impact of wireless technology on their cardholder data environment (CDE) before implementation. The guidance emphasizes that PCI DSS requirements must be individually evaluated for each environment.

“Wireless networks continue to be an easy target for data compromise, especially as new devices are added to these environments” said Bob Russo, general manager of the PCI Security Standards Council. “This resource remains an important tool for understanding how to secure your payment card data when using wireless technologies.”

Recommendations on the use of technologies in relation to the PCI Standards are issued as separate guidance on an ongoing basis throughout the standards lifecycle. These documents do not introduce additional requirements to the PCI Standards, nor are they an endorsement of one technology over another.

The PCI DSS Wireless Guidelines information supplement can be accessed here: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guideline_with_WiFi_and_Bluetooth_082211.pdf

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 related 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 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: http://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

###