Overview of the PCI DSS Wireless Guideline Information Supplement

The near ubiquity of wireless networks makes them a top priority for organizations that store, process or transmit cardholder data. In response, the PCI Security Standards Council Special Interest Group Implementation Team has published an information supplement called *PCI DSS Wireless Guideline*. The goal of this document is to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and provide practical methods and concepts for deployment of secure wireless in payment card transaction environments. It is also intended for assessors who audit PCI DSS compliance. This At-a-Glance is a summary of the 32-page Guideline.

### Wireless Requirements for Compliance with PCI DSS

The wireless requirements for PCI DSS relate to whether or not the technology is part of the Cardholder Data Environment (CDE). The CDE is the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment. The illustration above is an example of wireless in a retail CDE. PCI DSS Wireless Guideline addresses these requirements from two perspectives related to the CDE:

- **Generally applicable wireless requirements.** These are requirements that all organizations should have in place to protect their networks from attacks via rogue or unknown wireless access points and clients. They apply to organizations regardless of whether the wireless technology is part of the CDE or not. As a result, these requirements are generally applicable to organizations that wish to comply with PCI DSS.

- **Requirements applicable for in scope wireless networks.** These are requirements that all organizations that transmit payment card information over wireless technology should have in place to protect those systems. They are specific to the usage of wireless technology that is in scope for PCI DSS compliance, namely the Cardholder Data Environment. These requirements apply in addition to the universally applicable set of requirements.

### Using the PCI DSS Wireless Guideline

Download the Guideline.

The Guideline provides specific recommendations for the contents outlined on the back side of this At-a-Glance, left sidebar. The adjacent diagram provides a step-by-step decision process for complying with PCI DSS wireless requirements. Please see the Guideline for details, including authority documents and external references, glossary of acronyms, and a PCI DSS v1.2 cross reference.
GUIDELINE CONTENTS

1. Overview

2. Wireless operational guide for complying with PCI DSS
   - Defining the Cardholder Data Environment (CDE)

3. Applicable requirements pertaining to wireless for all networks
   - Maintain a hardware inventory
   - Wireless scanning to look for rogue APs
   - Segmenting wireless networks

4. Applicable requirements for in scope wireless networks
   - Physical security of wireless devices
   - Changing the default settings of the APs
   - Wireless intrusion prevention and access logging
   - Strong wireless authentication and encryption
   - Use of strong cryptography on transmission of cardholder data over wireless
   - Development and enforcement of wireless usage policies

5. Authority documents and external references

6. Glossary of acronyms

7. PCI DSS v1.2 Cross Reference

---

Decision Process for PCI DSS Wireless Compliance

Comply with PCI DSS Wireless Requirements

Is there any wireless deployed?

Is wireless segmented out of PCI scope?

Change defaults on wireless APs, controllers and devices (PCI DSS Req. 2.1.1)

Enable 802.11i security on wireless LAN (PCI DSS Req. 4.1.1)

Physically secure wireless devices (PCI DSS Req. 9.1.3)

Log wireless access centrally (PCI DSS Req. 10.5.4)

Monitor for wireless intrusion attempts and alert personnel to potential risks and attacks (PCI DSS Req. 1.4)

Develop usage policies for wireless access (PCI DSS Req. 12.3)

Check for and remove unauthorized wireless devices in CDE periodically (PCI DSS Req. 11.1 & 12.9)

Install strong access controls (e.g. stateful firewalls) between wireless and CDE (PCI DSS Req. 1.2.3)

Generate audit report to prove that default keys, passwords, vendor defaults, SNMP strings, etc. have been changed

A centralized management system to configure and manage 802.11i authentication and encryption is recommended

Generate a wireless audit report that proves that unencrypted access to CDE does not occur

Have quarterly reports showing periodic wireless scans of all CDE with rogue wireless devices eliminated

Document access control rules and prove that wireless traffic does not enter CDE using log monitoring

Binary Decision: Is wireless deployed?

NO

YES

NO

YES

© 2009 PCI Security Standards Council LLC. The intent of this document is to provide supplemental information. Information provided here does not replace or supersede wireless requirements in the PCI Data Security Standard. Special interest groups are made up of Participating Organization, Qualified Security Assessor, and Approved Scanning Vendor subject matter experts.