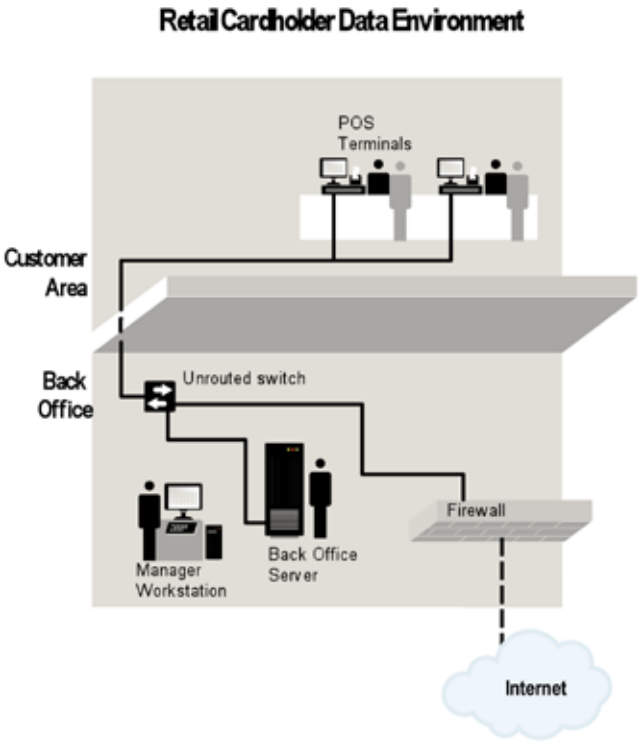
Overview of the PCI DSS Wireless Guideline Information Supplement

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.



HIGHLIGHTS

- Provides guidance for testing or deploying 802.11 Wireless Local Area Networks (WLAN)
- Focuses on suggestions for deploying WLAN in the Cardholder Data Environment
- Includes operational procedures required to make WLAN part of a PCI DSS compliant network

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

Decision Process for PCI DSS Wireless Compliance