

# PCI DSS

From Wikipedia, the free encyclopedia

## Contents

- 1 Introduction to PCI DSS
- 2 The Requirements of the Standard
- 3 PCI Compliance and Wireless LANs
- 4 External links

## Introduction to PCI DSS

**PCI DSS** stands for Payment Card Industry (PCI) Data Security Standard (DSS). It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or they risk losing the ability to process credit card payments.

The PCI DSS reflects the combined interests of VISA, MasterCard, Discover, American Express, and JCB. These five credit card brands have agreed upon a common set of security standards. Prior to this each card brand managed their own set of requirements:

- MasterCard - Site Data Protection (SDP) Program
- VISA - Cardholder Information Security Program (CISP) and Account Information Security (AIS)
- Discover - Discover Information Security and Compliance (DISC)
- American Express - Data Security Operating Policies

Merchants and Service Providers must validate compliance with an audit by a PCI DSS Qualified Security Assessor (QSA) Company.

## The Requirements of the Standard

The current version of the standard (version 1.1, released in September, 2006) specifies 12 requirements for compliance, organized into 6 logically related groups, which are called "control objectives."

The control objectives and their requirements are:

- Build and Maintain a Secure Network
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Use and regularly update anti-virus software
  - Requirement 6: Develop and maintain secure systems and applications

- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security

## PCI Compliance and Wireless LANs

The PCI DSS recognizes wireless LANs as public networks and automatically assumes it will be hacked. It does not matter what encryption is used. PCI DSS also provides two specific security guidelines to prevent breaches coming in from wireless networks used in any environments containing credit card data. They are:

- Firewall segmentation between wireless networks and the POS (point-of-sale) networks or any network that comes in contact with credit card information.
- Use of wireless analyzers (a.k.a. Wireless Intrusion Detection) to detect any unauthorized wireless devices and attacks

## External links

- PCI DSS Standard
- PCI Answers Blog and Forum Different PCI experts demystifying the experience of compliance
- "PCI DSS Made Easy", a whitepaper from GFI
- Experiences and lessons learned with the Payment Card Industry Data Security Standard (PCI DSS)" (english, PDF, 173 kB)
- PCI DSS 101 - An introduction to PCI DSS - what it is, where it came from and why your shop may find it useful, even if you do not process credit card data (English, PowerPoint, 5.2 MB)

Retrieved from "[http://en.wikipedia.org/wiki/PCI\\_DSS](http://en.wikipedia.org/wiki/PCI_DSS)"

Categories: [Payment systems](#) | [Credit cards](#)

---

- This page was last modified 22:59, 29 August 2007.
- All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.)  
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3) tax-deductible nonprofit charity.