



# Payment Card Industry (PCI) Data Security Standard

---

## Requirements and Security Assessment Procedures

Version 1.2.1

July 2009

This Abbreviated Document provided by:



[www.DCRS.com](http://www.DCRS.com)

2605 METRO BOULEVARD • ST. LOUIS MO 63043  
314.739.6666 • 800.231.0166

## Introduction and PCI Data Security Standard Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. This document, *PCI Data Security Standard Requirements and Security Assessment Procedures*, uses as its foundation the 12 PCI DSS requirements, and combines them with corresponding testing procedures into a security assessment tool. It is designed for use by assessors conducting onsite reviews for merchants and service providers who must validate compliance with the PCI DSS. Below is a high-level overview of the 12 PCI DSS requirements. The next several pages provide background about preparing for, conducting, and reporting a PCI DSS assessment, whereas the Detailed PCI DSS Requirements begin on page 13.

### PCI Data Security Standard – High-Level Overview

#### 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

For the COMPLETE VERSION of this DOCUMENT titled:

# **Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures**

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download.html](https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html)

## **About the PCI Data Security Standard (PCI DSS)**

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

## **List of Validated Payment Applications**

The specific versions of the applications identified on the following List of Validated Payment Applications (Application List) have been assessed for compliance with the Payment Application Data Security Standard (PA-DSS).

[https://www.pcisecuritystandards.org/security\\_standards/vpa/](https://www.pcisecuritystandards.org/security_standards/vpa/)

## **Prioritized Approach for DSS 1.2**

The Prioritized Approach provides guidance that will help merchants identify how to reduce risk to card holder data as early on as possible in their compliance journey. The tool groups together the requirements of PCI DSS 1.2 into six key milestones for merchants to consider in their card data security strategy.

<https://www.pcisecuritystandards.org/education/prioritized.shtml>