

What is PCI?

PCI Overview

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That's why Visa USA has instituted the **Cardholder Information Security Program (CISP)**. Mandated since June 2001, CISP is intended to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard.

In 2004, the CISP requirements were incorporated into an industry standard known as Payment Card Industry (**PCI**) Data Security Standard resulting from a cooperative effort between Visa and MasterCard to create common industry security requirements. Visa USA maintains CISP as the managing program for data security compliance endorsing the PCI Data Security Standard.

Effective September 7, 2006, the PCI Security Standards Council ("PCI SSC") owns, maintains and distributes the PCI Data Security Standard (DSS) and all its supporting documents. Visa USA, however, continues to manage all CISP compliance enforcement and validation initiatives.

[PCI Requirements](#)

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

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 network

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