CSNP
CYBERSECURITY NON-PROFIT

PCI DSS Compliance Guide

A comprehensive framework for protecting payment card data and achieving compliance

FOUNDATION

Understanding PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive security requirements designed to protect cardholder data during payment processing, storage, and transmission.

Developed by major card brands—Visa, Mastercard, American Express, Discover, and JCB—PCI DSS ensures consistent security standards across all payment environments.

Why it matters: Compliance protects your customers, reduces breach risk, avoids costly penalties, and maintains customer trust in your business.

12 Requirements

Organized into six control objectives

Annual Validation

Required for all merchants

Version 4.0

Latest standard with enhanced protections

Merchant Levels and Requirements

PCI DSS categorizes merchants into four levels based on annual transaction volume, determining validation requirements and assessment complexity.

Level 4: Under 20K Transactions

Self-Assessment Questionnaire (SAQ) and network scan by Approved Scanning Vendor (ASV). Ideal starting point for small businesses.

Level 2: 1M-6M Transactions

Annual SAQ and quarterly scans, or onsite assessment if required by acquiring bank. Enhanced validation requirements.

Level 3: 20K-1M Transactions

Annual SAQ completion and quarterly network scans. Most small to medium businesses fall into this category.

Level 1: Over 6M Transactions

Annual Report on Compliance (ROC) by Qualified Security Assessor (QSA) and quarterly network scans. Most stringent requirements.

Self-Assessment Questionnaire (SAQ) Types

Choose the appropriate SAQ based on how your business processes payment card data. Each type addresses specific merchant environments and integration methods.

SAQ A

Card-not-present merchants who outsource all payment processing with no electronic storage, processing, or transmission of cardholder data.

SAQ A-EP

E-commerce merchants who outsource payment processing but have a website that directly impacts security of the payment transaction.

SAQ B

Merchants using imprint machines or standalone dial-out terminals with no electronic cardholder data storage.

SAQ C

Merchants with payment application systems connected to the internet, but no electronic cardholder data storage.

SAQ D

All other merchants and service providers not included in the other SAQ types. Most comprehensive assessment.

REQUIREMENTS 1-2

Build and Maintain a Secure Network

Requirement 1: Install and Maintain Network Security Controls

- Deploy and configure firewalls to protect cardholder data
- Restrict connections between untrusted networks and systems in the cardholder data environment
- Prohibit direct public access between the internet and any system component
- Install perimeter firewalls between wireless networks and cardholder data

Requirement 2: Apply Secure Configurations

- Change all vendor-supplied defaults before installing systems on the network
- Develop configuration standards for all system components
- Remove unnecessary functionality, services, and accounts
- Document and implement security configuration standards

REQUIREMENTS 3-4

Protect Stored Cardholder Data

1

Minimize Data Storage

Keep cardholder data storage to an absolute minimum. Develop and implement data retention and disposal policies. Never store sensitive authentication data after authorization.

2

Render Data Unreadable

Mask PAN when displayed (first six and last four digits maximum). Encrypt cardholder data stored in databases using strong cryptography. Protect encryption keys from disclosure and misuse.

3

Secure Transmission

Use strong cryptography and security protocols (TLS, SSH, IPsec) to safeguard cardholder data during transmission over open, public networks. Never send unprotected PANs by email or messaging.

REQUIREMENTS 5-6

Maintain a Vulnerability Management Program

Requirement 5: Protect from Malicious Software

Deploy and maintain anti-malware solutions on all systems commonly affected by malware. Ensure anti-malware mechanisms are actively running and cannot be disabled by users.

- Keep anti-malware software current through automatic updates
- Perform periodic evaluations to identify and address evolving malware threats
- Generate and review anti-malware logs regularly

Requirement 6: Develop Secure Systems and Software

Establish processes to identify and address security vulnerabilities in systems and applications through regular patching and secure development practices.

01

Identify Vulnerabilities

Monitor security alerts and apply patches

02

Assess Risk

Prioritize based on severity and exposure

03

Remediate

Apply patches within defined timeframes

04

Verify

Confirm successful implementation

REQUIREMENTS 7-8

Implement Strong Access Control Measures

Requirement 7: Restrict Access

Limit access to cardholder data by business need-to-know. Implement role-based access control (RBAC) and assign access based on job classification and function. Deny all access by default.

Requirement 8: Identify Users

Assign a unique ID to each person with computer access. Implement multi-factor authentication for all access to the cardholder data environment. Never use shared accounts or generic IDs.

Effective access control ensures that only authorized individuals can view or modify cardholder data, significantly reducing the risk of insider threats and unauthorized access. Review access rights quarterly and immediately revoke access for terminated employees.

REQUIREMENTS 9-10

Monitor and Test Networks Regularly

Requirement 9: Restrict Physical Access

Use facility entry controls to limit physical access to cardholder data and systems.

- Implement video cameras to monitor sensitive areas
- Restrict physical access to wireless access points and network infrastructure
- Maintain visitor logs and distinguish visitors from onsite personnel
- Physically secure all media containing cardholder data

Requirement 10: Log and Monitor Access

Track and monitor all access to network resources and cardholder data through comprehensive logging.

- Implement automated audit trails for all system components
- Record all user activities, exceptions, and security events
- Review logs daily and retain for at least one year
- Synchronize all critical system clocks using time-synchronization technology

REQUIREMENTS 11-12

Test Security Systems and Maintain Policies

Regular Security Testing

Conduct quarterly internal and external vulnerability scans by ASVs. Perform annual penetration testing and test security controls after significant changes.

Information Security Policy

Maintain and disseminate a comprehensive security policy addressing all PCI DSS requirements. Review annually and update as needed to reflect changes.

Security Awareness

Provide security awareness training for all personnel at hire and annually. Train staff on their specific responsibilities for protecting cardholder data.

Reducing Your PCI DSS Scope

Minimizing the systems and processes that handle cardholder data dramatically simplifies compliance efforts, reduces costs, and lowers security risks.

1

Outsource Payment Processing

Use validated third-party payment processors and point-to-point encryption (P2PE) solutions to keep cardholder data out of your environment entirely. This is the most effective scope reduction strategy.

2

Segment Your Network

Isolate the cardholder data environment (CDE) from other networks using firewalls and network segmentation. Clearly define and document CDE boundaries to limit assessment scope.

3

Use Tokenization

Replace sensitive card data with unique identification symbols (tokens) that retain essential information without compromising security. Tokens are useless if intercepted.

4

Eliminate Unnecessary Storage

Delete stored cardholder data that is no longer needed for business, legal, or regulatory purposes. Implement automated deletion policies and procedures.

Common Compliance Mistakes to Avoid

1

Assuming compliance is one-time

PCI DSS requires continuous compliance, not just passing an annual assessment. Security is an ongoing process requiring regular monitoring, testing, and updates.

2

Storing unnecessary cardholder data

Many breaches involve data that shouldn't have been stored. Never store CVV2, PIN, or full track data. Minimize retention of other cardholder data elements.

3

Using default passwords and configurations

Attackers actively exploit default credentials. Change all vendor defaults before deployment and maintain secure configuration standards for all systems.

4

Neglecting vendor management

Third-party vendors with access to your cardholder data can introduce vulnerabilities. Maintain a registry of service providers and ensure they comply with PCI DSS.

5

Inadequate security awareness training

Human error remains a leading cause of data breaches. Provide regular, role-specific training for all personnel handling payment data or working in the CDE.

Your Compliance Timeline and Implementation Checklist

Typical 6-Month Implementation Timeline

Month 1-2: Assessment Phase

Scope definition, gap analysis, SAQ selection

Month 3-4: Remediation Phase

Address gaps, implement controls, update policies

Month 5: Testing Phase

Vulnerability scans, penetration testing, validation

Month 6: Documentation Phase

Complete SAQ/ROC, submit compliance reports

Essential Implementation Steps

Inventory all systems that store, process, or transmit cardholder data

Document data flows showing how card data moves through your environment

Implement network segmentation to isolate the cardholder data environment

Deploy security controls including firewalls, encryption, and access management

Establish logging and monitoring with daily review procedures

Create security policies covering all 12 PCI DSS requirements

Train all staff on security awareness and PCI DSS responsibilities

Schedule quarterly scans with an Approved Scanning Vendor (ASV)

Conduct annual assessments and submit attestation of compliance

About Cybersecurity Non-Profit (CSNP)

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety
- Senior Digital Safety
- Women's Security
- Parents & Educators

Everything we offer is completely free. We believe cybersecurity education should be accessible to everyone, regardless of budget or technical background.

Get Started Today

Visit Our Website

csnp.org

Explore our programs and community

Access Free Resources

csnp.org/resources

Guides, tools, and templates for your security journey