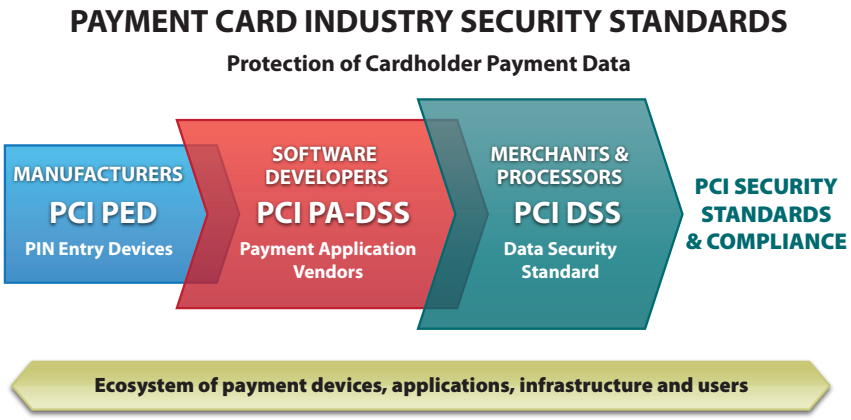
Payment Card Industry Security Standards

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data – with new requirements for software developers and manufacturers of applications and devices used in those transactions. Compliance with the PCI set of standards is mandatory for their respective stakeholders, and is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.



PCI Standards Include:

PCI Data Security Standard: The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts or processes payment cards, it must comply with the PCI DSS.

PIN Entry Device Security Requirements: PCI PED applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions.

Payment Application Data Security Standard: The PA-DSS is for software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement. It also governs these applications that are sold, distributed or licensed to third parties.

PCI SSC Founders

American Express
Discover Network
JCB
MasterCard Worldwide
VISA

Participating Organizations

Merchants, banks, processors, developers and point of sale vendors

PCI Data Security Standard for Merchants & Processors

The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

COMPLIANCE PROGRAM

Assessing

Secure collection and tamper-proof storage of cardholder data; it must be available for analysis

Reporting

Prove compliance if assessed and present evidence that data protection controls are in place

Monitoring & Alerting

Have systems for auto-alerting to constantly monitor access and usage of data

Systems should extend to log data with proof of being collected and stored

PCI AT-A-GLANCE

(visit www.pcisecuritystandards.org for more information)

Overview

Getting Started with PCI DSS

10 Common Myths of PCI DSS

Data Security Do's and Don'ts

Getting Started with PA-DSS

Getting Started with PCI PED

How to Comply with PCI DSS

The PCI Security Standards Council sets the standards for PCI security but each payment card brand has its own program for compliance. Specific questions about compliance should be directed to your acquiring financial institution. Links to payment card brand compliance program include:

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: www.discovernetwork.com/resources/data/data_security.html
- JCB International: www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp (U.S.)

Qualified Assessors. The Council provides programs for two kinds of certifications: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are companies that assist organizations in reviewing the security of its payments transaction systems and have trained personnel and processes to assess and validate compliance with PCI DSS and PA-DSS. ASVs provide commercial software tools to perform certified vulnerability scans for your systems. Additional details can be found on our Web site at: www.pcisecuritystandards.org.

Self-Assessment Questionnaire. The "SAQ" is a validation tool for merchants and service providers who are not required to do on-site assessments for PCI DSS compliance. Different SAQs are specified for various business situations; more details can found on our Web site at: www.pcisecuritystandards.org or contact the acquiring financial institution to determine if you should complete an SAQ.

Payment Application Data Security Standard for Developers

The PA-DSS minimizes vulnerabilities in payment applications. The goal is to prevent the compromise of full magnetic stripe data located on the back of a payment card. PA-DSS covers commercial payment applications, integrators and service providers. Merchants and service providers should use certified payment applications and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.

Payment Application DSS Requirements – Validated by PA-QSA Assessment	
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CIV2, CW2) or PIN block data	8. Facilitate secure network implementation
2. Provide secure password features	9. Do not store cardholder data on a server connected to the Internet
3. Protect stored cardholder data	10. Facilitate secure remote software updates
4. Log application activity	11. Facilitate secure remote access to application
5. Develop secure applications	12. Encrypt sensitive traffic over public networks
6. Protect wireless transmissions	13. Encrypt all non-console administrative access
7. Test applications to address vulnerabilities	14. Maintain instructional documentation and training programs for customers, resellers and integrators

PIN Entry Device (PED) Security Requirements for Manufacturers

This standard, referred to as PED, applies to companies which make devices that accept personal identification number (PIN) entry for all PIN-based transactions. Merchants and service providers should use certified PED devices and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.

PIN Entry Device Security Requirements – Validated by PED Laboratory
Device Characteristics
Physical Security Characteristics (to prevent the device from being stolen from its location)
Logical Security Characteristics (to provide functional capabilities that ensure the device is working appropriately)
Device Management
Device Management during manufacturing
Device Management between manufacturer and initial cryptographic key loading
Considers how the PED is produced, controlled, transported, stored and used throughout its lifecycle (to prevent unauthorized modifications to its physical or logical security characteristics)