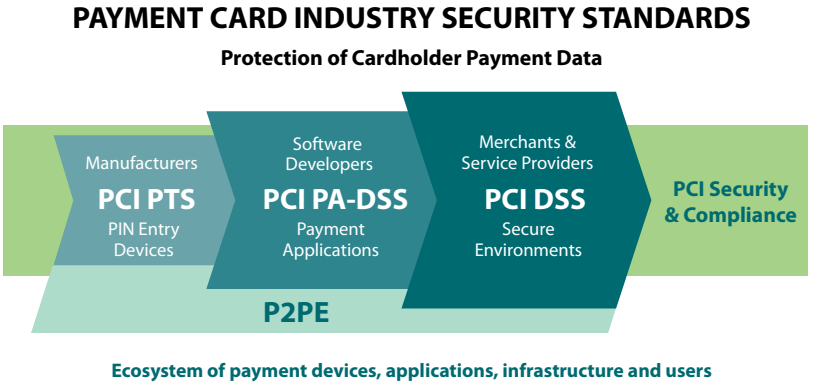
Overview of PCI Requirements

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.



PCI Security Standards Include:

PCI Data Security Standard (PCI DSS)

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you accept or process payment cards, PCI DSS applies to you.

PIN Transaction Security (PTS) Requirements

The PCI PTS is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The PTS standards include PIN Security Requirements, Point of Interaction (POI) Modular Security Requirements, and Hardware Security Module (HSM) Security Requirements. The device requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Financial institutions, processors, merchants and service providers should only use devices or components that are tested and approved by the PCI SSC, listed at: www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices.

Payment Application Data Security Standard (PA-DSS)

The PA-DSS is for software vendors and others who develop payment applications that store, process or transmit cardholder data and/or sensitive authentication data as part of authorization or settlement, when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants to use payment applications that are tested and approved by the PCI SSC. Validated applications are listed at: www.pcisecuritystandards.org/assessors_and_solutions/payment_applications.

QIR PROGRAM

Qualified Integrators and Resellers (QIRs) are integrators and resellers specially trained by PCI Security Standards Council to address critical security controls while installing merchant payment systems. QIRs reduce merchant risk and mitigate the most common causes of payment data breaches by focusing on critical security controls. A list of QIRs is available at https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers.

PCI Point-to-Point Encryption Standard (P2PE)

This Point-to-Point Encryption (P2PE) standard provides a comprehensive set of security requirements for P2PE solution providers to validate their P2PE solutions, and may help reduce the PCI DSS scope of merchants using such solutions. P2PE is a cross-functional program that results in validated solutions incorporating the PTS Standards, PA-DSS, PCI DSS, and the PCI PIN Security Standard. Validated P2PE solutions are listed at: www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions.

PCI Card Production Logical Security Requirements and Physical Security Requirements

The Card Production Logical and Physical Security Requirements address card production activities including card manufacturing, chip embedding, data preparation, pre-personalization, card personalization, chip personalization, fulfillment, packaging, storage, mailing, shipping, PIN printing and mailing (personalized, credit or debit), PIN printing (non-personalized prepaid cards), and electronic PIN distribution.

PCI Token Service Provider Security Requirements

The Token Service Provider (TSP) Security Requirements are intended for Token Service Providers that generate and issue EMV Payment Tokens, as defined under the EMV® Payment Tokenisation Specification Technical Framework.

The PCI Standards can all be downloaded from the PCI SSC Document Library:
https://www.pcisecuritystandards.org/document_library

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	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 cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 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. Identify and authenticate access to system components 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 for all personnel