





























































# About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) is a global open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. The Council maintains, evolves, and promotes the Payment Card Industry security standards. It also provides critical tools needed for implementation of the standards such as assessment and scanning guidelines, a self-assessment questionnaire, training and education, and product certification programs.

The PCI SSC founding members, American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., have agreed to incorporate the PCI Data Security Standard as part of the technical requirement for each of their data security compliance programs. Each founding member also recognizes the Qualified Security Assessors and Approved Scanning Vendors qualified by the PCI SSC to assess compliance with the PCI DSS.

The PCI SSC's founding member card brands share equally in the Council's governance and operations. Other industry stakeholders participate in reviewing proposed additions or modifications to the standards, including merchants, payment card issuing banks, processors, hardware and software developers, and other vendors.

## PCI SSC FOUNDERS



## PARTICIPATING ORGANIZATIONS

Merchants, Banks, Processors,  
Hardware and Software Developers  
and Point-of-Sale Vendors

# PCI Data Security Standard

The PCI DSS version 1.2 is a set of comprehensive requirements for enhancing payment account data security. It represents common sense steps that mirror security best practices. Learn more about its requirements, security controls and processes, and steps to assess compliance inside this PCI Quick Reference Guide.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need-to-know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for employees and contractors</li> </ol>

---

This Guide provides supplemental information that does not replace or supersede PCI DSS version 1.2 documents.

