

## 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	<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. Protect all systems against malware 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. Identify and authenticate access to system components</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 all personnel</li></ol>