The 12 PCI DSS Requirements

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems

1. Install and Maintain Network Security Controls.
2. Apply Secure Configurations to All System Components.

Protect Account Data

3. Protect Stored Account Data.
4. Protect Cardholder Data with Strong Cryptography During transmission Over Open, Public Networks.

Maintain a Vulnerability Management Program

5. Protect All Systems and Networks from Malicious Software.
6. Develop and Maintain Secure Systems and Software.

Implement Strong Access Control Measures

7. Restrict Access to System Components and Cardholder Data by Business Need to Know.
8. Identify Users and Authenticate Access to System Components.
9. Restrict Physical Access to Cardholder Data.

Regularly Monitor and Test Networks

10. Log and Monitor All Access to System Components and Cardholder Data.
11. Test Security of Systems and Networks Regularly.

Maintain an Information Security Policy

12. Support Information Security with Organizational Policies and Programs.

Referenced from the Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0