This checklist gives general guidance on PCI DSS compliance. However, completing it does not substitute an expert's precise and authoritative evaluation and cannot serve as a definitive certification of your organization's compliance status.

phoenixNAP®
GLOBAL IT SERVICES

PCI compliance refers to adherence to the Payment Card Industry Data Security Standard (PCI DSS). This standard was developed by major credit card brands to ensure that any organization handling, processing, or transmitting credit card information maintains a secure environment.

Here are the key measures and priorities for achieving PCI DSS compliance:

1. Install and Maintain a Firewall Configuration

- □ Document your network topology
- □ Restrict and log traffic
- □ Review firewall rule sets

2. Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- □ Replace default credentials
- □ Harden system services
- □ Maintain secure baseline configurations

3. Protect Stored Cardholder Data

- □ Limit data storage
- □ Encrypt data at rest
- □ Mask PAN display
- □ Securely dispose of unneeded data

4. Encrypt Transmission of Cardholder Data Across Open, Public Networks

- □ Enforce strong encryption
- □ Manage certificates properly
- □ Segment the cardholder data environment

5. Protect All Systems Against Malware and Regularly Update Anti-Virus

Software

□ Deploy antivirus and anti-malware tools

□ Keep definitions and engines updated

□ Respond quickly to alerts

6. Develop and Maintain Secure Systems and Applications

□ Adopt a secure SDLC

□ Apply critical patches quickly

□ Control changes with formal processes

□ Protect web applications

7. Restrict Access to Cardholder Data

□ Implement role-based access control (RBAC)

□ Update access policies regularly

8. Identify and Authenticate Access to System Components

□ Use unique user IDs

□ Strengthen authentication

□ Manage session and lockout policies

9. Restrict Physical Access to Cardholder Data

□ Control entry to sensitive areas

□ Secure media and backups

□ Destroy media properly

10. Track and Monitor All Access to Network Resources and Cardholder Data

□ Enable system logs

□ Use centralized log management

□ Review logs

11. Regularly Test Security Systems and Processes

□ Perform vulnerability scans

□ Conduct penetration tests

□ Deploy IDS/IPS and wireless scans

12. Maintain a Policy That Addresses Information Security for All Personnel

□ Develop a formal security policy

□ Train and educate employees

□ Oversee vendors and third parties

□ Create and test an incident response plan