NordLayer®

[Your company name]

CREATING & IMPLEMENTING

Checklist for compliance with PCI DSS

Owner: [Organization / Team / Dedicated person]

Last reviewed: [Date]

Status: Draft

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Goal: Construct and uphold a secure network and systems

Policy & process requirements:

- □ Write formal documents for the examination and validation of network modifications
- □ Establish standards for firewall, router, and personal firewall configurations
- □ Conduct a biannual review of firewall rules
- □ Justify and document ports and services for all inbound and outbound rules

Implementation requirements:

- □ Implement and configure safe firewall and router rules and settings
- □ Apply network segmentation to control connections between trusted and untrusted networks

- □ Block direct public access between the internet and the internal cardholder data environment
- □ Install firewalls on internet-connected portable devices that also access cardholder data
- □ Utilize security features for insecure services within the cardholder data environment
- □ Install barriers between wireless networks and cardholder data environment

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Goal: Foster and sustain a secure network and systems

Policy & process requirements:

- □ Document management procedures for vendor default settings and best practices
- □ Design configuration standards for all system components
- □ Establish and uphold a policy for wireless network security

Implementation requirements:

- □ Alter vendor-supplied defaults and remove unnecessary default accounts during installation
- □ Modify all wireless vendor defaults at installation that link to the cardholder data environment
- □ Implement systems using configuration standards and vendor best practices
- □ Utilize strong cryptography for encrypting all non-console administrative access

Requirement 3: Protect stored cardholder data

Goal: Preserve cardholder data

Policy & process requirements:

- □ Create a policy for data retention and disposal, including secure deletion
- □ Outline a quarterly procedure for identifying and erasing data beyond the retention period
- □ Document key management policies for secure generation, storage, and distribution

Implementation requirements:

- □ Ensure sensitive authentication data is not stored, even if encrypted
- □ Apply a robust key management process, including secure storage and access restriction
- □ Make sure PAN is unreadable when stored and masked when shown, with limited access to authorized personnel

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Goal: Safeguard cardholder data

Policy & process requirements:

- □ Document controls for encrypting data with strong cryptography over public networks
- □ Establish configuration standards for authentication and transmission encryption for wireless networks
- □ Outline a procedure for accepting trusted keys and certificates

Implementation requirements:

- □ Locate areas where cardholder data is transmitted over public networks and confirm strong encryption
- □ Ensure PAN is either unreadable or secured with strong cryptography when sent via messaging technologies
- □ Only accept trusted keys and certificates

Requirement 5: Use and regularly update anti-virus software or programs

Goal: Uphold a program for vulnerability management

Policy & process requirements:

- □ Maintain antivirus policies for detection, removal, and protection against malware

Implementation requirements:

- □ Keep antivirus software up to date, conduct regular scans, and create audit logs
- □ Ensure active antivirus software that cannot be turned off by users on commonly affected systems

Requirement 6: Develop and maintain secure systems and applications

Goal: Maintain a program for vulnerability management

Policy & process requirements:

- □ Detail a process to recognize new security vulnerabilities and risk assessment
- □ Document change control and software development policies, including secure coding

Implementation requirements:

- □ Conduct vulnerability assessments or use automated solutions like web application firewalls
- □ Shield systems from vulnerabilities by installing vendor security patches
- □ Develop software in compliance with industry standards and PCI DSS, ensuring security
- □ Perform code reviews by someone other than the author

Requirement 7: Limit cardholder data access

Goal: Employ robust access control measures

Policy & process requirements:

- □ Document an access control policy focusing on need, privilege, least privilege, and job classifications

Implementation requirements:

- □ Regularly review system access, ensuring that privileges are necessary and restricted

Requirement 8: Assign a unique ID to each person with computer access

Goal: Implement strong access control measures

Policy & process requirements:

- □ Outline a policy for managing user access, including creation, revocation, modification, and user ID management

Implementation requirements:

- □ Remove or deactivate inactive accounts over 90 days old
- □ Require passwords to be at least 7 characters with complexity, changed every 90 days
- □ Mandate multi-factor authentication for non-console and remote access
- □ Avoid generic or shared accounts for critical functions

Requirement 9: Control physical access to cardholder data

Goal: Employ robust access control measures

Policy & process requirements:

- □ Develop a policy for handling and destroying physical media
- □ Document procedures for managing onsite personnel and visitor access

Implementation requirements:

- □ Implement security controls for facility access
- □ Establish a visitor security program, including badges and logs
- □ Ensure secure storage and classification of physical media
- □ Regularly inspect POS devices for tampering or substitution

Requirement 10: Track and monitor all access to network resources and cardholder data

Goal: Monitor and test networks on a regular basis

Policy & process requirements:

- □ Create policies for daily log file monitoring and review
- □ Examine logs for abnormalities or suspicious activity

Implementation requirements:

- □ Implement automated audit trails for specific events
- □ Ensure retention of audit logs for immediate availability and archival

Requirement 11: Regularly test security systems and processes

Goal: Continually monitor and test networks

Policy & process requirements:

- □ Document the process for identifying unauthorized wireless access points
- □ Outline a method for penetration testing based on industry standards

Implementation requirements:

- □ Perform periodic internal and external vulnerability scans
- □ Conduct penetration testing as needed and bi-annual segmentation testing for service providers
- □ Implement intrusion detection or prevention systems
- □ Use a change detection mechanism for unauthorized system modifications

---

Requirement 12: Develop and uphold an information security policy

Goal: Sustain an information security policy

Policy & process requirements:

- □ Document and review the security policy annually
- □ Outline risk assessment, acceptable use policies, incident response plan, and service provider responsibilities

Implementation requirements:

- □ Assign information security tasks to the proper staff
- □ Educate all staff on security awareness and obtain acknowledgements
- □ Perform background checks on potential employees within legal bounds
- □ Regularly review and test the incident response plan
- □ This revised text maintains the structure and content of the original while providing a more varied and detailed expression of the ideas.

Version history

Version	Date	Approver	Review status	Notes
			Under review ▾	
			Not started ▾	
			Not started ▾	
			Not started ▾	