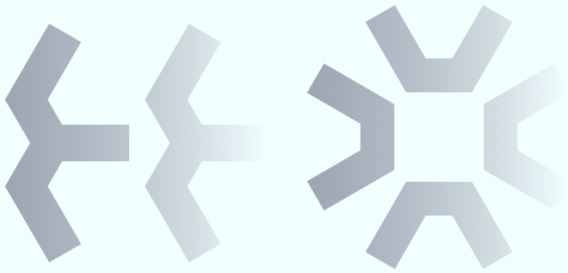
NordLayer®



PCI Policy

Index

Access Control Policy

Purpose

To set forth regulations governing the safeguarding of the cardholder data environment.

Audience

The PCI Access Control Policy is applicable to every person who engages with cardholder data concerning (Company).

Policy

- Entry to the CDE is determined by the principle of need-to-know.
- The level of access needed for authorized tasks can be granted, adhering to the principle of least privilege.
- Exclusive use of approved (Company) devices is permitted for connecting to the CDE, whether onsite or remote.
- Installing, modifying, or removing devices in the CDE is restricted to approved personnel only.
- All created accounts must have a documented request and approval associated with them.

Account Management

Purpose

To set forth regulations aimed at safeguarding the cardholder data environment.

Audience

The PCI Account Management Policy is applicable to every person who engages with cardholder data concerning (Company).

Policy

- Before accessing the CDE, all users are required to acknowledge the (Company) Corporate Information Security and PCI Policy.
- Each account should be uniquely identifiable through the user name assigned by (Company) IT, ensuring no redundant user IDs are used.
- All accounts must have at least one approved method for user authentication to system components (such as password, token, smart card, biometric, etc.).
- The usage of group or shared accounts is strictly prohibited.
- Procedures for account creation, modification, and termination must be in place.
- For all non-console administrative access to the CDE, both internal and external, multi-factor authentication must be incorporated.

- Vendor/third-party access accounts should only be enabled when necessary and disabled at all other times.
- Vendor/third-party access accounts must be monitored while in use.
- Passwords must be a minimum of 7 characters long and have a maximum age of 90 days.
- After 6 failed login attempts, accounts should be locked out for 30 minutes.

Asset Management

Purpose

The objective is to set up guidelines governing the arrangement, upkeep, and safeguarding of cardholder data environments.

Audience

The Asset Management Policy is relevant to any person overseeing the (Company) cardholder data environments (CDE).

Policy

- Inventory control and monitoring procedures must document all card reader devices, including their status (deployed, awaiting deployment, undergoing repair, not in use, or in transit), and this inventory must be updated at least annually.
- Each device must undergo classification to determine its sensitivity level.
- Any discrepancies in the inventory, such as missing or substituted devices, must be promptly reported.
- The (Company) CDE must not be connected to any non-approved cardholder data capture devices.
- Devices responsible for capturing payment data (card-present transactions) must be safeguarded against tampering and substitution.
- Third-party personnel accessing devices for repair/maintenance must be subject to monitoring.
- Physical security measures must be in place to secure all devices and media.
- Backups should be securely stored, and the security of the backup location should be reviewed at least annually.
- Management approval is required for any device relocation from a secure area.
- Secure couriers or authorized delivery methods with accurate tracking capabilities must be used for device transfers.
- Devices that are no longer required must undergo secure destruction.

Data Protection

Purpose

To set forth regulations ensuring the safeguarding of cardholder information.

Audience

The Data Protection Policy is relevant to any person overseeing the (Company) cardholder data environments (CDE).

Policy

- Never retain sensitive authentication data (the three or four-digit code located on the front or back of the credit card) after credit card authorization.
- Both cardholder data and sensitive authentication data are considered confidential.
- Data should be securely destroyed or shredded when it is no longer necessary.
- Mask the primary account number (PAN) when displayed, and restrict access to the full PAN only to those with a legitimate business need.
- Avoid sending unprotected PANs through end-user messaging technologies, such as email, instant messaging, SMS, or chat.
- Before processing, using, storing, or transmitting cardholder data, any department or system at (Company) must contact the Security/PCI Office for approval.
- PCI DSS requirements are applicable if cardholder data is stored, processed, or transmitted.
- Permanent storage of cardholder data is not allowed.
- Prohibit the use of recording devices to store photographs, videos, audio, or any other sensitive authentication data.
- Establish retention requirements for cardholder data, keeping the storage to a minimum and adhering to legal, regulatory, and business requirements.
- Dispose of data securely when it is no longer needed, following the retention policy guidelines.
- Mask the primary account number (PAN) whenever it is displayed.
- Make sure the PAN becomes unreadable anywhere it is stored by employing methods like:
    - one-way hashes based on strong cryptography,
    - truncation,
    - index tokens and pads
    - strong cryptography with associated key-management processes and procedures.
- If disk encryption is utilized, manage logical access separately and independently from the native operating system authentication.

Encryption Management

Purpose

To set forth regulations ensuring the safeguarding of cardholder information.

Audience

The Encryption Management Policy is relevant to any person overseeing the (Company) cardholder data environments (CDE).

Policy

- There should be established procedures for encryption key management.
- When transmitting sensitive cardholder data over open, public networks, it is essential to employ strong cryptography and security protocols.
- It is strictly prohibited to send unprotected PANs using end-user messaging technologies such as email, instant messaging, SMS, or chat.

Firewall Management

Purpose

The objective is to set forth guidelines governing the setup, upkeep, and safeguarding of the cardholder data environments.

Audience

The Firewall Management Policy is applicable to any individuals responsible for administering the (Company) cardholder data environments (CDE).

Policy

- Ensure that configuration files are both secured and synchronized.
- Place a firewall at each internet connection and between any DMZ and the internal network zone.
- Keep a well-documented list of firewall rules, providing business justification for the use of all services, protocols, and allowed ports.
- Deploy perimeter firewalls between all wireless networks and the cardholder data environment (CDE).
- Install personal firewalls on any mobile or employee-owned devices that connect to the internet while outside the network and are used to access the network.
- Implement a DMZ to restrict inbound traffic solely to system components that offer authorized publicly accessible services, protocols, and ports.
- Enforce anti-spoofing measures to detect and block forged source IP addresses from accessing the network.
- Ensure that system components storing cardholder data reside within an internal network zone, separate from the DMZ and other untrusted networks.
- Avoid disclosing private IP addresses and routing information to unauthorized individuals or parties.

Incident Management

Purpose

The aim is to set forth regulations that safeguard the cardholder data environment.

Audience

The PCI Incident Management Policy is applicable to every individual responsible for managing the (Company) cardholder data environments (CDE).

Policy

- It is imperative to put into effect and test an incident response plan on an annual basis.
- Availability of incident response personnel should be ensured round the clock to promptly address any alerts.

Logging and Monitoring

Purpose

The objective is to set forth guidelines governing the setup, upkeep, and safeguarding of the cardholder data environments.

Audience

The PCI Logging and Monitoring Policy is applicable to every individual responsible for managing the (Company) cardholder data environments (CDE).

Policy

- Every system component should be accompanied by a corresponding audit trail.
- To ensure consistency in log timestamps, all critical system time clocks must regularly synchronize with a single reference time source.
- Securing audit trails is imperative to prevent any unauthorized alterations.
- System components' logs and security events must undergo periodic reviews to detect anomalies or suspicious activities.
- Audit trails must be retained for a minimum of one year, with at least three months' worth of data readily accessible for analysis.

Network Management

Purpose

The objective is to set forth guidelines governing the setup, upkeep, and safeguarding of the cardholder data environments.

Audience

The Network Management Policy is relevant to every individual responsible for administering the (Company) cardholder data environments (CDE).

Policy

Network Configuration

- Prior to system installation on the network, all default accounts provided by vendors must be changed, and if unnecessary, removed or disabled.
- It is essential to maintain a network diagram that clearly depicts the connections between the Cardholder Data Environment (CDE) and other networks, including wireless networks.
- A data flow diagram illustrating the movement of cardholder data across systems and networks must be regularly updated and maintained.
- Configuration standards should be in place for all system components to address known security vulnerabilities. This should also include a detailed description of groups, roles, and responsibilities for managing network components.
- Documented operational procedures are necessary for managing firewalls effectively.
- Firewall rule sets must be reviewed at least every six months.
- Servers should be limited to one primary function per server, or in the case of virtualization, one primary function per system component.
- Encryption must be applied to all non-console administrative access.
- An inventory containing all system components must be consistently updated and maintained.
- To safeguard against malicious software, anti-virus software must be installed on all systems commonly affected (e.g., personal computers and servers).
- All anti-virus software must be kept up to date, perform regular scans, generate audit logs, run actively, and not be susceptible to being disabled or altered by users.

Wireless Networking

- Industry best practices should be applied to ensure robust encryption for authentication and transmission on wireless networks that transmit cardholder data or are connected to the CDE.
- A quarterly assessment process must be established to detect the presence of wireless access points, and all authorized and unauthorized ones must be promptly identified.

Physical Security

Purpose

To set forth guidelines that ensure the safeguarding of the cardholder data environment.

Audience

The PCI Physical Security Policy is applicable to any individual who engages with cardholder data on behalf of (Company).

Policy

- Access to the system must align with job requirements.
- Upon termination, all access privileges are immediately revoked, and keys/cards must be promptly returned or deactivated.
- Effective controls must be established to differentiate between onsite personnel and visitors, utilizing identification badges, for instance.
- Media storage must be physically safeguarded at all times.
- Devices handling payment data (card-present transactions) must be protected against tampering and substitution.
- Regular inspections of device surfaces should be conducted to detect any signs of tampering or substitution, including verification of serial numbers or other device characteristics to ensure authenticity.
- A comprehensive inventory of card-reading devices must be maintained.
- Physical access to the CDE (Cardholder Data Environment) must be strictly controlled, utilizing appropriate facility entry measures.
- Monitoring mechanisms such as video cameras and/or access control systems should be in place to oversee physical access to sensitive areas.
- Access to the CDE must adhere to a formal request and approval process.
- For visitors, a robust management process must be implemented, encompassing identification and authorization procedures.

Remote Access

Purpose

To set forth guidelines that ensure the safeguarding of the cardholder data environment.

Audience

The PCI Remote Access Policy pertains to any individuals remotely accessing (Company) cardholder data or the cardholder data environment.

Policy

- Remote access to the cardholder data environment necessitates two-factor authentication.
- The copying, moving, and storage of cardholder data onto local hard drives and removable electronic media are strictly forbidden.
- Remote work must adhere to the specified (Company) remote working requirements, which include the following:
- All PCI-related activities must be conducted in a separate environment, which should be locked when not in use.
- The use of (Company) provided equipment is mandatory for all PCI-related tasks.
- (Company) provided equipment is exclusively meant for work-related purposes.
- Call recording should be carried out following the company-approved method, which may involve handling cardholder data.
- Sessions for remote access will be automatically disconnected after a duration specified by IT.

Software Development

Purpose

The objective is to set forth guidelines governing the setup, upkeep, and safeguarding of cardholder data environments.

Audience

The PCI Software Development Policy is applicable to every person engaged in software development.

Policy

- Secure development of internal and external software applications is imperative.
- Before applications become active or are released to customers, all development, test, and custom application accounts, user IDs, and passwords must be removed.
- Prior to release to production or customers, custom code must undergo thorough review to identify and address potential coding vulnerabilities.
- Developers must undergo training in secure coding techniques.
- Application development should strictly adhere to secure coding guidelines.
- For public-facing web applications, ongoing efforts must be made to address new threats and vulnerabilities.
- To ensure the security of public-facing web applications, either of the following approaches must be adopted:
    - Conduct manual or automated application vulnerability security assessments at least annually and after any changes.
    - Implement an automated technical solution that detects and prevents web-based attacks, continuously monitoring all traffic in front of public-facing web applications.

Training

Purpose

To set forth guidelines governing the safeguarding of the cardholder data environment.

Audience

The PCI Training Policy is applicable to every individual who interacts with (Company) cardholder data or the cardholder data environment.

Policy

- Every employee at (Company) who comes into contact with or could impact the security of cardholder data as part of their job responsibilities is required to successfully finish an annual training program focused on cardholder data security.

Vendor Management

Purpose

To define guidelines governing the establishment and supervision of vendors within the (Company) cardholder data environments.

Audience

The Vendor PCI Policy is applicable to any person overseeing or controlling access to vendors within the (Company) cardholder data environments (CDE).

Policy

- A comprehensive assessment of vendors accessing the CDE is mandatory.
- A record of all vendors must be maintained, including the information about the PCI DSS requirements managed by each service provider and (Company).
- Prior to commencing any service and annually thereafter, vendors must undergo evaluation.
- Vendors with PCI DSS compliance requirements need to have their compliance status reviewed annually.
- Vendor access should only be granted when necessary and disabled when not in use.
- While vendors are using their access, their activities must be monitored.
- Vendors must provide written acknowledgment of their responsibility for the security of cardholder data handled on behalf of the customer or that may affect the security of (Company)'s CDE.

Vulnerability Management

Purpose

The objective is to define guidelines governing the setup, upkeep, and safeguarding of cardholder data environments.

Audience

The Vulnerability Management Policy is relevant to any individuals responsible for administering the (Company) cardholder data environments (CDE).

Policy

Patching

- Conducting a system scan is essential to identify security vulnerabilities, and this task should be carried out by an authorized third party. Once vulnerabilities are detected, they must be classified based on their severity levels.
- Installing all relevant patches provided by vendors is crucial, and their prioritization should align with the associated risks. Critical patches must be applied within 30 days of their release.

- Every alteration made to system components must adhere to a rigorous change control process.

Vulnerability Scanning and Penetration Testing

- Regular vulnerability scans, both internal and external, should occur at least every quarter or whenever significant network changes take place.
- Follow-up scans must be carried out until all vulnerabilities identified in the initial quarterly scan are resolved.
- External vulnerability scans should be conducted by an Approved Scanning Vendor (ASV).
- At least once a year, internal and external penetration testing must be performed, utilizing an industry-accepted penetration methodology, to cover the entire perimeter of the Cardholder Data Environment (CDE) and critical systems.
- Intrusion-detection and/or intrusion-prevention systems must be implemented to detect and/or prevent network intrusions. Generated alerts must be diligently reviewed and addressed.

Definitions

CDE: The computer system network that contains cardholder data or sensitive authentication data, along with the systems and segments directly connected to or supporting cardholder processing, storage, or transmission.

Waivers

After undergoing the (Company) Waiver Process, it is possible to request exemptions from specific policy provisions.

Enforcement

Individuals discovered to have breached this policy could face disciplinary measures, ranging from reprimands to the possibility of termination from their position, in addition to potential civil or criminal consequences.

If any vendor, consultant, or contractor is found to have breached this policy, they could face penalties ranging from the revocation of access rights and termination of contract(s) to potential civil or criminal consequences.

Appendix

The items that are not covered in the isolated PCI policy but are necessary for PCI DSS compliance as part of the entire Information Security Program are:

- Information Security Policy
    - To be reviewed at least once a year

    - Clear definition of security policies/procedures outlining the security responsibilities for all staff
- Risk assessment process
    - Conducted annually
    - Identifying crucial assets, threats, and vulnerabilities
    - Culminating in a formal, documented risk analysis
- Usage Policies for Critical Technologies and Appropriate Use (e.g., wireless technology, remote access, email, and internet usage), ensuring:
    - Specific approval by authorized individuals
    - Authentication for technology usage
    - A detailed list of devices and personnel with access
    - A means to precisely determine ownership, contact information, and purpose
    - Permissible technology uses
    - Approved network locations for these technologies
    - A roster of company-sanctioned products
    - Automatic remote-access technology disconnection after a set inactivity period
    - Remote-access technology activation for vendors/business partners as required and immediate deactivation afterward
    - For personnel accessing cardholder data via remote-access, restrictions on copying, moving, and storing data on local drives or removable media, except when authorized for specific business needs
- Individual or Team Responsibility for Information Security Management:
    - Creation, documentation, and distribution of security policies/procedures
    - Security alerts and information monitoring, analysis, and distribution
    - Establishment, documentation, and distribution of incident response and escalation procedures
    - User account administration, including additions, deletions, and alterations
    - Access monitoring and control to all data
    - Pre-hire screening of prospective employees
    - Establishment and maintenance of policies and procedures for managing service providers involved with cardholder data, as follows:
        - Keeping a list of service providers
        - Maintaining a written agreement recognizing the service providers' responsibility for cardholder data security
        - Ensuring a formal process for engaging service providers with appropriate due diligence
        - Annual monitoring of service providers' PCI DSS compliance
        - Keeping records of PCI DSS requirements managed by the entity or service provider
- For Service Providers:
    - Written acknowledgment to clients regarding responsibility for cardholder data security
    - If segmentation is employed, execution of penetration testing on segmentation controls every six months or following any segmentation control changes.