



PCI DSS Compliance Policy Manual (2025 Edition)

Organization: Norman Nerds

Effective Date: November 2025

Version: 1.0

I. Introduction & Scope

1. Purpose

This document defines the policies, standards, and operational procedures by which **Norman Nerds** ensures ongoing compliance with the **Payment Card Industry Data Security Standard (PCI DSS) v4.0**.

The policy establishes the governance framework for protecting **cardholder data (CHD)** and **sensitive authentication data (SAD)** against unauthorized access, use, or disclosure.

It applies to all Norman Nerds systems, personnel, and subcontractors involved in storing, processing, or transmitting payment card data on behalf of clients.

2. Regulatory Framework

This policy is based on the following standards and authorities:

- **PCI DSS v4.0 (March 2022)** — published by the PCI Security Standards Council (PCI SSC).
- **Oklahoma Statutes Title 24 §162** — requiring entities to implement and maintain reasonable data security procedures.
- **Federal Trade Commission (FTC) Safeguards Rule** — for service providers handling consumer data.
- **NIST SP 800-53 and SP 800-171** — supporting references for risk management, encryption, and access control best practices.

Norman Nerds adopts these standards as minimum baselines and may apply stricter controls where appropriate.

3. Scope Definition

3.1 System Scope

This policy applies to all systems within the **Cardholder Data Environment (CDE)**, defined as:

- Systems that **store, process, or transmit** cardholder data.
- Systems connected to or that can **impact the security** of the CDE.
- Supporting systems providing authentication, logging, or network segmentation.

3.2 Personnel Scope

All Norman Nerds workforce members with access to payment-related data, including:

- Employees, contractors, interns, and third-party technicians.
- IT administrators managing payment systems or integrations.
- Customer support and development staff interacting with payment APIs or tokens.

4. Cardholder Data Definition

Type	Examples	Storage Allowed?	Protection Requirements
Cardholder Data (CHD)	PAN (Primary Account Number), Cardholder Name, Expiration Date, Service Code	Yes (if encrypted)	AES-256 or stronger encryption; tokenization preferred
Sensitive Authentication Data (SAD)	Full Magnetic Stripe Data, CVV2/CVC2, PIN, PIN Block	No	Prohibited from storage post-authorization
Tokenized Data	Surrogate value mapped via tokenization service	Yes	Stored securely and logically separated from PAN data

5. Policy Objectives

Norman Nerds maintains this PCI DSS Compliance Policy to:

1. Protect all payment-related data under its custody or control.
 2. Establish accountability for all individuals accessing the CDE.
 3. Ensure continuous compliance with PCI DSS requirements.
 4. Demonstrate readiness for annual self-assessment (SAQ) or external audit (ROC).
 5. Support a security culture emphasizing prevention, detection, and rapid response.
-

6. PCI DSS Requirement Mapping

PCI DSS Requirement Policy Section(s) Primary Control Area

Req. 1	Section IV	Network Firewalls & Segmentation
Req. 2	Section IV–V	Secure Configuration & Hardening
Req. 3	Section V	Data Protection & Encryption
Req. 4	Section V	Secure Transmission
Req. 5	Section VII	Vulnerability Management & Anti-Malware
Req. 6	Section VII	Secure Development & Patching
Req. 7	Section VI	Access Control
Req. 8	Section VI	Authentication & Account Management
Req. 9	Section VIII	Physical Security
Req. 10	Section XI	Logging & Monitoring
Req. 11	Section VII–XI	Testing & Vulnerability Scanning
Req. 12	Section X–XII	Governance, Policy Maintenance, and Awareness

7. Policy Maintenance

This policy is reviewed **annually** by the **PCI Compliance Officer** and **Chief Information Security Officer (CISO)**, or upon:

- Significant infrastructure changes (e.g., new data centers, payment processors).
- Changes to PCI DSS requirements.
- Client contract renewals involving PCI scope adjustments.

Approved revisions are documented in **Appendix F – Policy Revision Log** and distributed to all relevant staff within 30 days of approval.

8. Enforcement

Failure to comply with this policy or related procedures may result in disciplinary action, up to and including termination, civil penalties, or criminal prosecution under applicable laws.

Contractors or vendors failing to comply will be subject to contractual remedies, including termination and indemnification.

Norman Nerds

II. PCI DSS Governance and Roles & Responsibilities

1. Purpose

This section defines the governance framework, management structure, and individual responsibilities for maintaining continuous PCI DSS compliance at **Norman Nerds**. It ensures that all employees, contractors, and vendors understand their roles in protecting **Cardholder Data (CHD)** and **Sensitive Authentication Data (SAD)**.

2. PCI Compliance Governance Framework

Norman Nerds implements a **PCI Compliance Program** overseen by the **PCI Compliance Committee (PCC)**. The PCC governs all activities related to PCI DSS compliance, including policy enforcement, audits, incident management, and certification.

2.1 Governance Structure

Role/Entity	Primary Responsibilities
Executive Management	Approves policy, allocates resources, and ensures organization-wide adherence.
PCI Compliance Committee (PCC)	Central authority overseeing compliance, chaired by the Compliance Officer.
PCI Compliance Officer (PCO)	Manages compliance activities, annual SAQ/ROC submission, and liaison with QSAs or ASVs.
IT Security Officer (ITSO)	Oversees network security, encryption, access control, and vulnerability management.
IT Operations / Infrastructure Team	Implements and maintains PCI-compliant technical environments.
Application Development Team	Ensures secure coding practices, reviews SDLC controls, and maintains change control logs.
HR Department	Manages background checks, onboarding, training, and sanctions.
Vendors / Service Providers	Maintain PCI compliance and execute Business Associate or Service Provider Agreements with Norman Nerds.

3. Roles and Responsibilities

3.1 Executive Management

- Ensure sufficient funding, staffing, and resources for compliance.
- Approve PCI DSS policies, procedures, and annual attestation reports.
- Review and sign-off on quarterly and annual risk assessments.
- Respond to significant compliance deficiencies or breaches.

3.2 PCI Compliance Officer (PCO)

- Primary authority for PCI DSS oversight.
- Coordinates internal and external PCI audits (SAQ/ROC).
- Maintains PCI documentation repository and compliance evidence.
- Reviews and approves data flow diagrams for PCI scope confirmation.
- Oversees vendor PCI validation and BAA/Service Provider Agreement renewals.
- Reports compliance status quarterly to executive leadership.

3.3 IT Security Officer (ITSO)

- Implements technical controls for network segmentation, encryption, and logging.
- Manages vulnerability scans, penetration testing, and firewall reviews.
- Validates access control, identity management, and account lifecycle processes.
- Reviews audit logs and intrusion detection alerts.
- Oversees incident containment and eradication during a security event.

3.4 IT Operations

- Maintain PCI systems according to hardening baselines.
- Apply operating system and application patches within established timelines.
- Manage secure configuration of firewalls, routers, and payment gateways.

-
- Document all change control activities in accordance with Section VII.

3.5 Application Development Team

- Follow secure development lifecycle (SDLC) principles.
- Ensure all payment applications comply with **PCI DSS and PA-DSS** (or successor standards, e.g., PCI Secure Software Framework).
- Conduct peer reviews and code analysis for each release.
- Use approved libraries for cryptography, logging, and authentication.
- Document version control, test results, and release authorizations.

3.6 Human Resources (HR)

- Perform pre-employment background checks for employees with PCI access.
- Enforce security awareness training before granting system access.
- Maintain personnel acknowledgment records for PCI policy and confidentiality.
- Coordinate with Compliance on disciplinary actions under the Sanctions Policy.

3.7 Department Managers

- Ensure that their teams adhere to PCI DSS operational policies.
- Report deviations or security incidents to the Compliance Officer immediately.
- Verify that all department-specific SOPs align with PCI DSS requirements.
- Participate in quarterly internal compliance reviews.

3.8 Vendors and Third-Party Service Providers

- Must provide annual PCI DSS compliance validation (AOC or SAQ-D).
- Sign Service Provider Agreements with explicit PCI data-handling clauses.
- Notify Norman Nerds within **5 business days** of any security incident.
- Participate in risk and compliance assessments as required by the PCO.
- Maintain encryption, segmentation, and data transfer protections per Section V.

4. PCI Compliance Committee (PCC)

4.1 Composition

The **PCI Compliance Committee** is chaired by the PCI Compliance Officer and includes representatives from:

- IT Security
- IT Infrastructure
- Legal Counsel
- Finance / Accounting
- HR
- Executive Management

4.2 Meeting Frequency

- Quarterly (minimum) for compliance status review.
- Ad-hoc for incidents, regulatory changes, or audit preparation.

4.3 Responsibilities

- Review PCI DSS version updates and apply necessary changes to policies.
 - Approve quarterly scan reports and penetration testing results.
 - Validate scope and network segmentation documentation.
 - Oversee remediation of noncompliance items.
 - Coordinate annual attestation of compliance (AOC/ROC submission).
 - Evaluate vendor and third-party PCI certifications.
-

5. Compliance Reporting

5.1 Internal Reporting

- The PCI Compliance Officer issues quarterly **Compliance Status Reports** summarizing:
 - Audit results
 - Open and closed remediation actions
 - Upcoming regulatory changes
 - Incident summaries and corrective measures
 - Risk assessment outcomes

These reports are submitted to Executive Management and retained for **six (6) years**.

5.2 External Reporting

- Annual **Self-Assessment Questionnaire (SAQ)** or **Report on Compliance (ROC)** is submitted to acquiring banks or card brands as applicable.
- Quarterly **Approved Scanning Vendor (ASV)** reports are filed and reviewed by the IT Security Officer.
- Breach notifications follow the **Incident Response Policy (Section IX)**.

6. Documentation Requirements

All records supporting PCI compliance — including risk assessments, audit reports, policies, training logs, and agreements — must be:

- Retained for at least **six (6) years** from creation or last effective date.
- Stored in the secure Compliance Repository with access restricted to the PCI Compliance Officer and authorized personnel.
- Version controlled and reviewed annually.

7. Enforcement

Noncompliance with assigned responsibilities may result in:

- Disciplinary action per the **Enforcement and Sanctions Policy (Section XIII)**.
- Termination of access privileges or contracts.
- Reporting to client organizations, acquiring banks, or regulators if warranted.

Norman Nerds

III. Network Security Policy

(Aligned with PCI DSS v4.0 Requirements 1 & 2)

1. Purpose

The purpose of this policy is to establish the technical and administrative requirements for securing **Norman Nerds'** network infrastructure that stores, processes, or transmits **Cardholder Data (CHD)** or **Sensitive Authentication Data (SAD)**.

This policy ensures that all firewalls, routers, and connected systems are configured and maintained to protect the **Cardholder Data Environment (CDE)** from unauthorized access, in accordance with **PCI DSS Requirements 1 and 2**.

2. Scope

This policy applies to:

- All production and test networks connected to the CDE.
- All Norman Nerds internal systems and third-party networks that transmit or could affect the security of CHD.
- All employees, administrators, and vendors responsible for managing or monitoring network systems.

3. Policy Statement

Norman Nerds maintains a **segmented, securely configured, and monitored network environment** to ensure the confidentiality, integrity, and availability of cardholder data.

The company uses firewalls, intrusion detection/prevention systems (IDS/IPS), and secure configurations to prevent unauthorized inbound or outbound traffic.

4. Network Architecture Overview

4.1 Logical Network Zones

Zone	Description	Access Restrictions
Cardholder Data Environment (CDE)	Systems directly handling CHD (e.g., payment applications, databases).	Strictly segmented; inbound access limited to authorized services only.
DMZ (Demilitarized Zone)	Systems providing public services such as payment gateways or web APIs.	Only necessary ports open; one-way communication into CDE.
Corporate Network	Internal systems (email, file sharing, HR, etc.)	No direct connectivity to CDE without jump host or proxy control.
Vendor/VPN Network	Authorized vendor access channels.	MFA and logging enforced; time-based access only.

Network segmentation is validated through **quarterly penetration testing** and **annual scope reviews**.

5. Firewall and Router Management

5.1 Firewall Configuration Standards

- Firewalls must be deployed at all network boundaries and between each logical segment.
- Configuration changes must be approved through the **Change Management Process (Section VII)**.
- Default “deny all” inbound and outbound rules must be enforced; exceptions documented.
- Only required ports, protocols, and services shall be allowed, justified, and reviewed quarterly.

-
- All firewall rules must include:
 - Rule description and business justification.
 - Source and destination IP ranges.
 - Application or protocol type.
 - Expiration or review date.

5.2 Router Configuration Standards

- Router configurations must restrict inbound and outbound traffic to business-necessary protocols.
- Anti-spoofing filters and access control lists (ACLs) must be implemented on edge routers.
- SNMP community strings must be changed from defaults and use SNMPv3 encryption.
- Configuration backups are encrypted and retained for one year.

5.3 Firewall Change Management

- Firewall configuration changes require written authorization from the IT Security Officer.
- All changes must be logged, reviewed, and tested for potential security impact.
- Emergency changes must be documented within 24 hours of implementation and reviewed within five (5) business days.

6. Secure Network Configuration

6.1 Hardening Standards

- All servers and network devices must follow **CIS Benchmarks** or **NIST SP 800-123** hardening guidelines.
- Default vendor passwords, SNMP strings, and security settings must be changed before deployment.
- Unnecessary services (e.g., FTP, Telnet, rlogin) must be disabled.
- Remote management interfaces must use secure protocols (e.g., SSH, HTTPS, RDP with TLS).
- Configuration templates must be reviewed annually by the IT Security Officer.

6.2 Wireless Network Security

- Wireless networks within the corporate or CDE environment must use **WPA3 Enterprise** or equivalent.
- Default SSIDs and passwords must be changed.
- Wireless access points must be approved by the IT Security Officer and documented in the asset register.
- Quarterly rogue wireless scans are conducted and logged.

7. Network Segmentation and Scope Control

- Segmentation controls must isolate systems storing, processing, or transmitting CHD.
- Firewalls, VLANs, and access control lists enforce separation between the **CDE** and non-CDE networks.
- Segmentation effectiveness is validated by **annual penetration tests** and **quarterly network scans**.
- Any scope change (e.g., new system added to CDE) requires a formal risk assessment and approval from the PCI Compliance Officer.

8. Remote Access and VPN Controls

- Remote administrative access to the CDE must use **multi-factor authentication (MFA)**.
- VPN access must be time-bound, logged, and reviewed monthly.
- Vendor access accounts are disabled when not actively in use.
- Remote sessions must use encrypted tunnels (TLS 1.3 or IPsec AES-256).
- Split tunneling is prohibited.

9. Network Monitoring and Logging

- All firewall, router, and IDS/IPS devices must log events to the centralized **Security Information and Event Management (SIEM)** system.
- Logs must include timestamps synchronized with NTP and stored for **at least one (1) year**, with **three (3) months** immediately available for analysis.

-
- Security alerts (e.g., repeated failed connections, intrusion attempts) trigger incident response procedures.
 - Logs are reviewed daily by the IT Security Officer or delegate.
-

10. Testing and Review

Activity	Frequency	Responsible Party	Documentation
Firewall Rule Review	Quarterly	IT Security Officer	Firewall Review Report
Configuration Audit	Semi-annual	Compliance Officer	Configuration Audit Log
Network Penetration Test	Annual	External QSA / ASV	Penetration Test Report
Vulnerability Scanning	Quarterly	IT Security	Scan Results & Remediation Plan
Rogue Wireless Scan	Quarterly	IT Security	Scan Log

11. Documentation and Recordkeeping

- Firewall and router configurations retained for **six (6) years**.
 - Network diagrams updated quarterly and reviewed during compliance meetings.
 - Network change logs stored for one year and archived for six years.
 - All reviews and approvals documented in the **PCI Compliance Repository**.
-

12. Enforcement

Noncompliance with network security standards may result in:

- Revocation of network privileges.

-
- Disciplinary action per the **Sanctions Policy (Section XIII)**.
 - Possible reporting to client organizations or acquiring banks.

IV. Data Protection & Encryption Policy

(Aligned with PCI DSS v4.0 Requirements 3 & 4)

1. Purpose

This policy establishes the standards and controls used by **Norman Nerds** to protect **Cardholder Data (CHD)** and **Sensitive Authentication Data (SAD)** throughout its lifecycle—from creation and storage to transmission and disposal.

The policy ensures compliance with **PCI DSS Requirements 3 and 4**, and mandates that all payment data is encrypted, stored only when necessary, and transmitted securely using approved cryptographic methods.

2. Scope

This policy applies to:

- All systems within the **Cardholder Data Environment (CDE)** that store, process, or transmit CHD.
- All employees, contractors, and vendors with logical or physical access to CHD or encryption keys.
- All electronic media, backups, removable drives, logs, and archives containing CHD or tokenized data.

3. Policy Statement

Norman Nerds is committed to protecting all CHD and SAD using encryption, access control, and key management processes consistent with industry best practices.

Sensitive Authentication Data (e.g., CVV, PIN) must **never be stored post-authorization**, even if encrypted.

All CHD storage and transmission shall be limited to the **minimum necessary scope** required for business or contractual purposes.

4. Cardholder Data (CHD) Elements and Protection Requirements

Data Element	Storage Allowed?	Protection Required	PCI DSS Reference
Primary Account Number (PAN)	Yes (if encrypted or tokenized)	AES-256 encryption; tokenization recommended	Req. 3.4
Cardholder Name	Yes (with PAN protection)	Encrypted or masked	Req. 3.3
Expiration Date	Yes (with PAN protection)	Encrypted or masked	Req. 3.3
Service Code	Yes (with PAN protection)	Encrypted or masked	Req. 3.3
CVV / CVC	No	Never stored post-authorization	Req. 3.2
Full Magnetic Stripe Data	No	Prohibited	Req. 3.2
PIN / PIN Block	No	Prohibited	Req. 3.2

5. Data Encryption Standards

5.1 Data at Rest

- All CHD stored electronically must be encrypted using **AES-256** or stronger symmetric encryption.

-
- Encryption keys must be generated and stored using **FIPS 140-2 Level 2** validated hardware security modules (HSMs) or equivalent secure key stores.
 - CHD must never be stored unencrypted in databases, log files, or backups.
 - Tokenization must be used wherever possible to replace PAN with non-sensitive surrogate values.
 - Encrypted databases must use strong key rotation and separate key storage from encrypted data.

5.2 Data in Transit

- Transmission of CHD over open or public networks must use **TLS 1.3** (minimum) or **IPsec AES-256** VPN tunnels.
- SSL and early TLS are prohibited.
- Email, SMS, or instant messaging platforms must not be used to transmit CHD.
- All APIs transmitting CHD must enforce mutual TLS (mTLS) or OAuth2 with certificate-based authentication.

6. Key Management Policy

6.1 Key Generation

- Encryption keys are generated using NIST-approved random number generators.
- Keys must be unique per system, function, or dataset.
- Key custodians are designated by the IT Security Officer and must have completed PCI training.

6.2 Key Storage and Protection

- Keys are stored in a **dedicated, access-controlled HSM** or key management appliance.

-
- Keys must never be stored in plaintext or in the same location as encrypted data.
 - Access to keys requires multi-factor authentication (MFA) and dual control.

6.3 Key Distribution

- Keys are distributed only to authorized systems through secure channels (e.g., SSH with key wrapping).
- Transmission of keys must use **key encryption keys (KEKs)** or asymmetric encryption.

6.4 Key Rotation and Retirement

- Keys must be rotated:
 - Annually at minimum.
 - Immediately upon compromise or personnel termination.
- Retired or replaced keys must be securely destroyed using HSM zeroization processes.

6.5 Key Custodian Responsibilities

- Maintain custody logs and usage records.
 - Participate in annual key audits.
 - Verify no unauthorized key duplication occurs.
-

7. Data Masking and Display Restrictions

- Displayed PANs must be **masked** to show only the **first six (6)** and **last four (4)** digits.
 - Full PAN display is limited to personnel with documented business need, authorized by the Compliance Officer.
 - Masking controls must be enforced in databases, applications, and reporting interfaces.
-

8. Data Retention and Disposal

8.1 Retention

- CHD must be retained only as long as required for business, legal, or contractual obligations.

-
- Retention schedules are reviewed annually by Legal and Compliance.
 - Systems containing expired CHD must be flagged for secure deletion.

8.2 Disposal

- Electronic CHD is securely deleted using **NIST SP 800-88 Rev.1** sanitization methods.
 - Physical media (e.g., drives, tapes) are destroyed via degaussing or shredding by certified vendors.
 - Disposal activities are logged, and Certificates of Destruction are retained for six (6) years.
-

9. Tokenization and Truncation

- Norman Nerds utilizes PCI-compliant tokenization services to replace PANs with non-sensitive tokens.
 - Tokens must be system-specific and mathematically non-reversible.
 - Truncation (e.g., first six + last four digits) is permitted for reporting purposes only.
 - Tokenized or truncated data must not be combined with other datasets to reconstruct the full PAN.
-

10. Data Transmission over Private Networks

- Internal transmissions of CHD between CDE components must use **TLS 1.3** or **IPsec VPNs**.
 - File transfers must use **SFTP** or **HTTPS** only; unencrypted FTP is prohibited.
 - Data loss prevention (DLP) systems monitor outgoing network traffic for CHD leakage.
 - Transmission logs are retained and reviewed monthly by the IT Security Officer.
-

11. Logging and Monitoring

-
- All encryption, decryption, key access, and CHD-related actions must be logged.
 - Logs must include user ID, timestamp, and system identifier.
 - Unauthorized decryption attempts trigger automated alerts.
 - Logs are retained for **at least one (1) year** and archived securely.
-

12. Testing and Validation

Activity	Frequency	Responsible Role	Evidence Retention
Key Management Review	Annual	IT Security Officer	6 years
Encryption Validation Testing	Annual	Compliance Officer	6 years
TLS Configuration Review	Quarterly	IT Security	6 years
Data Disposal Audit	Annual	Compliance Officer	6 years

13. Documentation and Recordkeeping

- Key management logs, disposal certificates, and encryption validation reports retained **6 years**.
 - Tokenization vendor compliance certificates reviewed **annually**.
 - Encryption algorithms and key lengths documented in the **Cryptographic Standards Register**.
-

14. Enforcement

Noncompliance with this policy may result in:

- Disciplinary action under the **Sanctions Policy (Section XIII)**.
- Revocation of access credentials.
- Contract termination or vendor penalties for third-party violations.

V. Access Control & Authentication Policy

(Aligned with PCI DSS v4.0 Requirements 7 & 8)

1. Purpose

This policy defines the access control and authentication requirements for systems within **Norman Nerds' Cardholder Data Environment (CDE)** to ensure that access to **Cardholder Data (CHD)** and **Sensitive Authentication Data (SAD)** is restricted strictly to authorized individuals, based on job function and business need.

This supports the principles of **least privilege**, **separation of duties**, and **strong authentication** in compliance with **PCI DSS v4.0 Requirements 7 and 8**.

2. Scope

This policy applies to:

- All Norman Nerds employees, contractors, and vendors who have access to systems that store, process, or transmit CHD.
 - All information systems, networks, databases, and applications within or connected to the **CDE**.
 - Any accounts used for remote access, administration, or third-party vendor support.
-

3. Policy Statement

Norman Nerds restricts system access to authorized users and enforces **unique identification, strong authentication, and role-based access controls (RBAC)**.

All access requests are reviewed, approved, logged, and periodically revalidated to maintain PCI DSS compliance.



4. Access Control Principles

Principle	Definition	Implementation Requirement
Least Privilege	Users have only the minimum access necessary to perform their duties.	Enforced via RBAC and job function mapping.
Need to Know	Access to CHD is granted only when required for business tasks.	Controlled via documented approval workflow.
Separation of Duties	Sensitive functions divided between multiple roles to prevent fraud.	Administrative rights separated from audit/review roles.
Accountability	Every user is uniquely identifiable and auditable.	Unique IDs; no shared or generic accounts allowed.

5. User Access Management

5.1 User Identification

- Each user must be assigned a **unique user ID**.
- Generic, shared, or group accounts are prohibited (except for system service accounts approved by the IT Security Officer).
- All user IDs are tied to personnel records and employment status in HR systems.

5.2 Access Authorization

- Access requests must be initiated via the **Access Request Form (Appendix D)**.
- Requests must include:
 - System(s) requested
 - Level of access
 - Business justification
 - Manager approval
- The **Compliance Officer** and **IT Security Officer** must approve access to the CDE.
- Temporary access is automatically revoked after expiration dates.

5.3 Access Review

- Access rights are reviewed **quarterly** for all users with CDE access.
- Reviews ensure that:
 - Access remains appropriate for the user's job function.
 - Terminated users' accounts are deactivated within **24 hours**.
 - Inactive accounts (≥90 days) are disabled automatically.

5.4 Privileged Access

- Administrative accounts are restricted to authorized IT personnel.
- Privileged access requires multi-factor authentication (MFA).

-
- Administrative sessions must not use personal or unencrypted devices.
 - All privileged activity is logged, monitored, and retained for one (1) year.
-

Norman Nerds

6. Authentication Controls

6.1 Password Policy

All passwords must comply with PCI DSS v4.0 standards:

Control	Requirement
Minimum Length	12 characters
Complexity	Uppercase, lowercase, number, and special character
Expiration	Every 90 days for privileged accounts; 180 days for general users

Control	Requirement
---------	-------------

History	Previous 12 passwords cannot be reused
---------	--

Lockout	6 failed login attempts triggers 30-minute lockout
---------	--

Idle Timeout	15-minute session timeout for inactive users
--------------	--

Reset Process	Requires verification of user identity and manager authorization
---------------	--

- Default vendor passwords must be changed immediately upon installation.
- Stored passwords must use **bcrypt** or equivalent one-way hashing.

6.2 Multi-Factor Authentication (MFA)

- MFA is required for:
 - All remote access to the CDE.
 - All administrative access (including local).
 - All VPN and privileged network sessions.
- MFA factors must include at least two of the following:

1. Something you know (password).
2. Something you have (hardware token, app-based OTP).
3. Something you are (biometric verification).

- MFA configurations are tested quarterly for functionality and integrity.

7. Access to Databases and Applications

- Access to CHD databases is limited to designated roles (e.g., DBA, application admin).
- Direct access to production databases via administrative tools is prohibited unless specifically approved.
- Application-level access to PAN data must follow masking and logging rules from **Section IV – Data Protection**.

-
- Access logs must record:
 - User ID
 - Access time and duration
 - Objects accessed or modified
 - IP address of the connection
-

8. Remote Access and Vendor Access

- All remote administrative access to systems within the CDE must use **encrypted VPN tunnels (IPsec/TLS 1.3)**.
 - Vendor access is:
 - Pre-approved, time-limited, and monitored.
 - Logged with session recording enabled.
 - Revoked immediately upon completion of work or contract termination.
 - Split tunneling is prohibited.
 - VPN configurations reviewed quarterly by the IT Security Officer.
-

9. Authentication for Non-Console and API Access

- Non-console administrative access (e.g., SSH, RDP, PowerShell) must enforce strong encryption and MFA.
- API keys used for CHD-related transactions must:
 - Be unique per integration.

-
- Have expiration and rotation policies.
 - Be stored securely using key vaults.
 - Be deactivated immediately if compromised.
-

10. Logging and Monitoring

- All authentication attempts (success and failure) are logged centrally in the **Security Information and Event Management (SIEM)** system.
 - Authentication logs must include:
 - Timestamp (NTP-synchronized)
 - User ID or system account
 - Source IP address
 - Authentication method used
 - Logs are reviewed **daily** by IT Security.
 - Alerts are generated for:
 - Multiple failed logins
 - Unauthorized access attempts
 - Disabled or terminated user activity
-

11. Account Lifecycle Management

Lifecycle Stage	Action Required	Responsible Party
Onboarding	User identity verified; access approved by Manager & Compliance	HR / IT Security

Lifecycle Stage	Action Required	Responsible Party
Transfers / Role Changes	Review access and adjust permissions accordingly	HR / Manager
Offboarding	Disable accounts within 24 hours; revoke tokens and credentials	HR / IT Security
Periodic Review	Quarterly access revalidation	Compliance Officer

12. Testing and Validation

Test Type	Frequency	Responsible Role	Evidence Retention
Access Control Audit	Quarterly	Compliance Officer	6 years
MFA Functionality Test	Quarterly	IT Security Officer	6 years
Password Policy Verification	Semi-annual	IT Security	6 years
Privileged Account Review	Quarterly	Compliance Officer	6 years

13. Documentation and Recordkeeping

- Access logs, MFA configuration records, and authorization forms retained for **six (6) years**.
 - HR onboarding/offboarding forms archived securely.
 - Quarterly review reports stored in the **PCI Compliance Repository**.
-

14. Enforcement

Noncompliance with this policy—including unauthorized access, password sharing, or failure to use MFA—will result in:

-
- Immediate revocation of access rights.
 - Disciplinary action under the **Sanctions Policy (Section XIII)**.
 - Potential notification to client organizations or regulatory bodies.

Norman Nerds

VI. Vulnerability Management & Patch Policy

(Aligned with PCI DSS v4.0 Requirements 5, 6, and 11)

1. Purpose

This policy defines the methods and responsibilities for identifying, assessing, remediating, and validating security vulnerabilities across **Norman Nerds'** systems within and supporting the **Cardholder Data Environment (CDE)**.

The goal is to ensure continuous protection against malware, software vulnerabilities, and system misconfigurations that could compromise **Cardholder Data (CHD)** or **Sensitive Authentication Data (SAD)**.

2. Scope

This policy applies to:

- All servers, workstations, applications, and network devices within or connected to the CDE.
 - All systems capable of impacting the security of CHD, including development and testing environments.
 - Third-party software, services, and dependencies supporting payment processing.
-

3. Policy Statement

Norman Nerds maintains a proactive vulnerability management program to detect and remediate vulnerabilities before they can be exploited.

All systems must remain up to date with security patches, anti-malware definitions, and configuration baselines according to defined risk levels.

Vulnerability management is a shared responsibility between the **IT Security Officer**, **System Administrators**, and **Compliance Officer**.

4. Malware Protection (PCI DSS Requirement 5)

4.1 Anti-Malware Deployment

-
- Anti-malware software must be installed, active, and up-to-date on all endpoints and servers capable of being infected by malicious software.
 - Systems must use enterprise-grade endpoint protection capable of:
 - Real-time scanning
 - Behavioral analysis
 - Automatic quarantine and removal
 - Centralized management and reporting

4.2 Signature and Engine Updates

- Signature files must update automatically **at least daily**.
- Systems unable to auto-update must be manually updated and verified weekly.
- Update logs must be retained for six (6) years.

4.3 Scanning and Quarantine

- Scheduled full scans must run **weekly** on all systems in scope.
- Quarantined files must be isolated and reviewed within **24 hours** by IT Security.
- Malware detections must trigger the **Incident Response Policy (Section IX)**.

4.4 System Exemptions

- Systems that cannot host anti-malware software (e.g., appliances, embedded systems) must implement **compensating controls**, including strict network segmentation, monitoring, and file integrity validation.
-

5. Patch Management (PCI DSS Requirement 6)

5.1 Patch Identification and Risk Rating

-
- Norman Nerds tracks vulnerabilities using:
 - Vendor advisories
 - NIST NVD (National Vulnerability Database)
 - CVE/CVSS scoring
 - Patches are prioritized based on **CVSS score** and business impact:

Risk Level CVSS Score Remediation Timeline

Critical	9.0–10.0	Within 48 hours
High	7.0–8.9	Within 7 days
Medium	4.0–6.9	Within 30 days
Low	0–3.9	Within 60 days

5.2 Patch Testing

- All patches must be tested in a controlled staging environment prior to production deployment.
- Testing ensures compatibility, stability, and no degradation of security functionality.
- Documented test results are retained for six (6) years.

5.3 Deployment Procedures

- Approved patches are deployed via automated patch management tools.
- Patch deployment logs must include:
 - System(s) updated
 - Date/time
 - Patch ID or KB reference
 - Responsible administrator
- Deployment validation reports reviewed weekly by the IT Security Officer.

5.4 Change Control

-
- All patches follow the **Change Management Process (Section VII)**, requiring:
 - Risk assessment
 - Manager approval
 - Scheduling
 - Post-deployment verification
-

6. Secure Software Development Lifecycle (SDLC)

6.1 Development Controls

- All software developed or maintained by Norman Nerds must comply with **PCI DSS 6.3–6.5**:
 - Use secure coding practices (e.g., OWASP Top 10).
 - Conduct code reviews for each release.
 - Validate input to prevent injection attacks.
 - Store credentials securely using encryption.
 - Prohibit hardcoded secrets or keys in code repositories.
- Development, test, and production environments must be **segregated**.
- Access to production code restricted to authorized personnel only.

6.2 Vulnerability Scanning in SDLC

- Static (SAST) and dynamic (DAST) scans must be integrated into CI/CD pipelines.
 - Vulnerabilities identified during development must be resolved before production deployment.
 - High or Critical findings must be re-tested and verified before go-live.
-

7. Vulnerability Scanning (PCI DSS Requirement 11.2)

Scan Type	Frequency	Performed By	Evidence Required
Internal Vulnerability Scan	Quarterly	IT Security Officer	Scan results and remediation log
External Vulnerability Scan (ASV)	Quarterly	Approved Scanning Vendor (ASV)	Approved scan report
After Any Significant Change	On-demand	IT Security	Post-change validation report

7.1 Remediation

- Findings are classified by severity and tracked in the **Vulnerability Register**.
- All high or critical findings must be resolved and rescanned within 30 days.
- False positives require documented justification.

8. Penetration Testing (PCI DSS Requirement 11.4)

8.1 Scope

Penetration testing must include both internal and external components of the CDE, and verify network segmentation effectiveness.

8.2 Frequency

- Conducted **annually** by an independent Qualified Security Assessor (QSA) or CREST-certified tester.
- Also conducted **after any significant system or network change**.

8.3 Methodology

- Follows **NIST SP 800-115** or **PTES (Penetration Testing Execution Standard)** methodology.
- Tests include:
 - Network and web application penetration
 - Privilege escalation
 - Data exfiltration attempts
 - Lateral movement simulation
 - Validation of patch and configuration effectiveness

8.4 Reporting and Remediation

- Penetration test results are reviewed by the PCI Compliance Committee.
- Findings are prioritized and tracked until remediation completion.
- Reports are retained for **six (6) years**.

9. File Integrity Monitoring (FIM)

- All critical systems (e.g., web servers, databases, POS systems) must employ **file integrity monitoring** software.
 - FIM tools must:
 - Detect unauthorized file changes in real time.
 - Alert the IT Security Officer immediately.
 - Log all changes for at least one (1) year.
 - Baseline checks are performed **weekly**.
-

10. Logging and Evidence Retention

- All vulnerability scans, patch reports, malware logs, and penetration test results must be archived securely.
- Minimum retention: **six (6) years**.
- Reports must include:
 - Scan or test date
 - Tools used and version
 - Findings and remediation evidence
 - Responsible parties
- Records are reviewed quarterly by the **Compliance Officer**.

11. Metrics and Performance Indicators

Metric	Target Threshold	Measured By
% of critical vulnerabilities remediated within SLA	≥ 95%	Compliance Officer
% of systems patched within SLA	≥ 98%	IT Security
Malware detection rate (false negatives)	≤ 0.5%	IT Security
Penetration test findings resolved	100%	Compliance Committee

12. Enforcement

Failure to comply with this policy may result in:

- Revocation of system access or administrator privileges.
- Disciplinary action under **Section XIII – Sanctions Policy**.

-
- Notification to acquiring banks or regulatory authorities if noncompliance impacts PCI status.

VII. Change Management Policy

(Aligned with PCI DSS v4.0 Requirements 6.4 & 6.5)

1. Purpose

The purpose of this policy is to establish standardized procedures for the management, approval, implementation, and documentation of system changes within **Norman Nerds'** environments that store, process, or transmit **Cardholder Data (CHD)**.

This ensures that all changes are properly authorized, tested, and logged to maintain the integrity and security of the **Cardholder Data Environment (CDE)** and to prevent unauthorized or insecure modifications.

2. Scope

This policy applies to:

- All hardware, software, and network configuration changes within or connected to the CDE.
 - Changes to applications, databases, operating systems, firewalls, routers, or cloud services.
 - Any third-party or vendor-managed environments that can affect PCI DSS compliance.
 - All Norman Nerds employees, contractors, and vendors involved in system development, maintenance, or administration.
-

3. Policy Statement

All changes to systems and environments under PCI scope must follow a **formalized change control process** to ensure security, traceability, and minimal operational risk.

Unauthorized or undocumented changes are strictly prohibited.

4. Change Management Principles

Principle	Definition	Implementation
Authorization	All changes must be pre-approved by authorized personnel.	Approval via documented change request.
Accountability	Each change has an assigned owner responsible for planning and validation.	Owner identified in change record.
Traceability	Every change must be uniquely tracked and auditable.	Ticketing system with timestamps and version control.
Testing	All changes must be tested prior to deployment.	QA/staging validation with rollback testing.
Segregation of Duties	No single individual may develop, approve, and deploy the same change.	Approval and deployment roles separated.

5. Types of Changes

Change Type	Examples	Approval Level
Standard Change	Routine, low-risk updates with pre-approved templates.	Manager + IT Security Officer
Normal Change	Software updates, configuration modifications, or feature enhancements.	Manager + Compliance Officer + IT Security Officer
Emergency Change	Urgent fix to resolve a critical issue impacting CDE or PCI compliance.	IT Security Officer (retroactive approval required)

6. Change Request and Approval Process

All changes must follow the process outlined below:

6.1 Step 1 – Initiation

- Submit a **Change Request (CR)** via the Change Management System (CMS).
- Include:
 - Change description and business justification.
 - Affected systems or data flows.
 - Security and PCI scope impact analysis.
 - Implementation plan, rollback plan, and testing plan.

6.2 Step 2 – Risk and Impact Assessment

- The **IT Security Officer** performs a risk assessment including:
 - PCI scope validation.
 - Potential service disruption or exposure of CHD.
 - Interaction with other systems or configurations.
- Risk levels are categorized as **Low, Medium, High, or Critical**.

6.3 Step 3 – Approval

- For non-emergency changes:
 - Department Manager approval.
 - Compliance Officer review for PCI impact.
 - IT Security Officer approval for technical and security validation.
- Emergency changes require:
 - Immediate IT Security Officer approval.

-
- Retroactive review by the Compliance Officer within 24 hours.

6.4 Step 4 – Testing

- Conduct functional and regression testing in a **non-production (staging)** environment.
- Validate:
 - No introduction of security vulnerabilities.
 - No degradation of encryption, logging, or authentication functions.
- Document test results in the change record.

6.5 Step 5 – Implementation

- Deploy changes following approved maintenance windows.
- Ensure backups and rollback procedures are available.
- Use automated deployment tools to reduce manual errors.

6.6 Step 6 – Validation and Closure

- Post-implementation validation by IT Security.
 - Confirm:
 - No unexpected issues or outages.
 - Security controls remain intact.
 - CDE scope unchanged.
 - Close the change ticket with attached evidence (logs, screenshots, validation reports).
-

7. Change Documentation Requirements

Each change record must include:

1. Unique change ID and summary.
2. Requestor, approver(s), and implementer(s).
3. Change category and classification.
4. Detailed description and business justification.
5. Risk level and PCI impact rating.
6. Test and rollback results.
7. Approval timestamps and signatures.
8. Post-deployment validation evidence.

Records are stored in the **Change Management System (CMS)** and retained for **six (6) years**.

8. Configuration and Version Control

- All configuration files and code changes must be stored in **version-controlled repositories** (e.g., Git).
 - Repositories must:
 - Require individual user authentication (no shared accounts).
 - Track commits, authors, and timestamps.
 - Include peer review via pull request or approval workflow.
 - Version baselines reviewed **semi-annually** by the IT Security Officer.
-

9. Emergency Change Procedures

- Emergency changes may be implemented immediately to resolve:
 - Active data breaches.
 - Critical system outages impacting CHD security.
 - Regulatory or contractual noncompliance events.
- Procedure:
 1. Obtain verbal or written authorization from the IT Security Officer.
 2. Document the change immediately after implementation.
 3. Conduct post-change testing within 24 hours.
 4. Obtain Compliance Officer review within 1 business day.

10. Security Code Review (PCI DSS Requirement 6.5)

- All internally developed or customized code impacting CHD must undergo a **security-focused code review**.
- Reviews verify that code adheres to **OWASP Top 10** best practices, preventing:
 - Injection attacks
 - Cross-site scripting (XSS)
 - Insecure direct object references
 - Inadequate session management

-
- Data exposure due to insecure serialization or cryptography
 - Reviews must be documented with reviewer name, findings, and resolution evidence.
-

11. Validation and Testing Schedule

Change Category	Testing Environment	Pre-Deployment Testing	Post-Deployment Validation
Standard	Pre-approved production configuration	Periodic QA verification	Weekly automated configuration validation
Normal	QA or staging environment	Required prior to deployment	Mandatory review and closure
Emergency	Live system with immediate need	As feasible	Full review within 24 hours

12. Logging and Monitoring

- All change-related events logged in the **Security Information and Event Management (SIEM)** platform.
 - Logs include:
 - Change ID
 - User performing the change
 - Timestamp and affected systems
 - Validation status
 - Unauthorized changes generate automatic alerts and incident escalation.
-

13. Review and Audit

- Change Management Policy reviewed annually by the **Compliance Officer**.
 - Quarterly **Change Audits** verify:
 - Completeness of change records.
 - Segregation of duties.
 - Adherence to approval workflows.
 - Audit findings reported to the **PCI Compliance Committee** for review and remediation.
-

14. Enforcement

Failure to follow the Change Management Policy may result in:

- Revocation of administrative privileges.
- Disciplinary action under the **Sanctions Policy (Section XIII)**.
- Mandatory incident report and possible compliance escalation.

VIII. Physical Security Policy

(Aligned with PCI DSS v4.0 Requirement 9)

1. Purpose

The purpose of this policy is to define the physical access controls and safeguards necessary to protect systems and facilities that store, process, or transmit **Cardholder Data (CHD)** or support the **Cardholder Data Environment (CDE)**.

Norman Nerds is committed to maintaining the confidentiality, integrity, and availability of CHD through robust facility security, device protection, and visitor management in compliance with **PCI DSS Requirement 9**.

2. Scope

This policy applies to:

- All Norman Nerds offices, data centers, and co-location facilities where systems in scope for PCI DSS are housed.
 - All employees, contractors, visitors, and vendors with physical access to CDE systems or storage areas.
 - All physical assets storing CHD, including servers, workstations, removable media, and network devices.
-

3. Policy Statement

Norman Nerds enforces **layered physical access control** and **environmental protection** for all facilities and systems handling CHD.

Only authorized personnel with a defined business need are granted physical access to the CDE, and all access is logged, monitored, and periodically reviewed.

4. Facility Security Controls

4.1 Perimeter Security

- CDE facilities are protected by **secured perimeters** including locked doors, card-controlled entry, and alarm systems.
- Access to sensitive areas requires **proximity badge and PIN** authentication.
- Doors and server room entries must remain closed and locked at all times when unattended.
- Unauthorized propping open of secure doors is strictly prohibited.

4.2 Surveillance and Monitoring

- CCTV video surveillance covers all ingress and egress points, server rooms, and CDE areas.
- Video feeds are retained for a minimum of **90 days**.
- Security footage is reviewed as part of quarterly physical access audits.
- Motion sensors and door contacts generate alerts for after-hours entry attempts.

4.3 Environmental Controls

- Facilities hosting CDE systems must have environmental protections including:
 - Temperature and humidity control
 - Smoke detection and fire suppression systems

-
- Water and flood sensors near equipment
 - Uninterruptible Power Supply (UPS) and generator backup
 - Environmental monitoring alerts are integrated into the facility management system.
-

5. Access Authorization

5.1 Personnel Authorization

- Access to CDE areas is granted only to employees with **verified background checks** and a **documented business need**.
- Requests must be submitted via the **Physical Access Request Form** and approved by:
 - Department Manager
 - Compliance Officer
 - Security Administrator
- Access permissions reviewed **semi-annually** and revoked upon role change or termination.

5.2 Visitor Access

- All visitors must:
 - Sign the **Visitor Log** upon entry and exit.
 - Present a valid government-issued photo ID.
 - Be issued a **visitor badge** that clearly identifies non-employee status.
 - Be **escorted at all times** by an authorized employee.

-
- Visitor logs must include:
 - Name, company, and purpose of visit
 - Host employee
 - Time in/out
 - Badge number issued
 - Visitor logs retained for **six (6) years**.

5.3 Third-Party Access

- Vendors or service providers requiring physical access to the CDE must have:
 - An executed Service Provider Agreement or NDA.
 - Current PCI DSS compliance validation (SAQ D or AOC).
 - Access granted only for specific dates and durations.
- Third-party access monitored and logged by Security.

6. Physical Access Devices

- All card access systems and keys must be:
 - Individually assigned and tracked in the **Access Control System (ACS)**.
 - Deactivated within **24 hours** of employee separation or contract termination.
 - Audited quarterly to ensure accurate assignment records.
- Lost or stolen access cards must be reported immediately to the **Security Administrator**.
- Mechanical locks must be re-keyed if key loss compromises facility security.

7. Media and Device Control

7.1 Removable Media

- CHD or logs containing CHD must **not** be stored on unencrypted removable media (USB drives, CDs, etc.).
- Any approved media must use **AES-256 encryption** and be tracked by serial number.
- Movement of media offsite requires:
 - Manager approval
 - Logging in the **Media Movement Register**
 - Secure courier or encryption verification

7.2 Device Protection

- Workstations accessing the CDE must:
 - Auto-lock after **15 minutes** of inactivity.
 - Be physically secured with cable locks or in locked enclosures.
 - Display security banners upon login.
- Servers must be mounted in **locked racks or cabinets**.
- Portable devices (laptops, tablets) storing CHD are prohibited unless explicitly authorized by Compliance and encrypted at rest.

7.3 Media Destruction

- When media reaches end of life or is no longer required, it must be destroyed via:
 - Cross-cut shredding for paper materials.
 - Degaussing or shredding for electronic media.
- Destruction must be witnessed by Security and logged with a **Certificate of Destruction** retained for 6 years.

8. Delivery and Maintenance Controls

- Equipment deliveries and removals from the facility must be logged and approved.
 - Third-party maintenance personnel must:
 - Sign in and out.
 - Be escorted while in secure areas.
 - Be verified for identity and company affiliation.
 - After maintenance, Security verifies that no tools, devices, or documentation remain onsite.
-

9. Monitoring and Review

Review Activity	Frequency	Responsible Party	Documentation
Physical Access Log Review	Monthly	Security Administrator	Access Audit Report
Access Rights Review	Semi-annually	Compliance Officer	Access Revalidation Report
Visitor Log Review	Quarterly	Security Officer	Visitor Audit Report
Video Surveillance Check	Quarterly	IT Security	Surveillance Validation Log
Key/Card Inventory Audit	Quarterly	Facilities Manager	ACS Audit Record

10. Incident Response for Physical Breaches

- Any unauthorized entry or tampering with CDE facilities or devices must be treated as a **security incident** under **Section IX – Incident Response Policy**.
- Immediate actions include:
 1. Isolate the area and prevent further access.

-
2. Notify Security and the Compliance Officer immediately.
 3. Preserve CCTV and access logs.
 4. Conduct root cause and impact analysis.
 5. Report to management and card brands if CHD is compromised.
-

11. Documentation and Retention

- Visitor and access logs retained **six (6) years**.
 - Surveillance footage retained **90 days minimum** (extended for investigations).
 - Certificates of Destruction, Access Request Forms, and Media Movement Logs stored in the **Compliance Repository**.
-

12. Enforcement

Noncompliance with this policy—including unauthorized entry, unescorted visitor activity, or improper device handling—will result in:

- Disciplinary action under the **Sanctions Policy (Section XIII)**.
- Immediate revocation of access privileges.
- Potential legal or contractual penalties for vendors.

IX. Incident Response Policy

(Aligned with PCI DSS v4.0 Requirement 12.10 and Oklahoma State Law)

1. Purpose

The purpose of this policy is to establish a structured and coordinated **Incident Response (IR) Program** to detect, respond to, contain, investigate, and recover from actual or suspected security incidents that could compromise **Cardholder Data (CHD)** or impact **Norman Nerds'** PCI DSS compliance.

This ensures that incidents are handled in a consistent, timely, and legally compliant manner, minimizing potential harm to affected parties and preserving forensic evidence.

2. Scope

This policy applies to:

- All systems within or connected to the **Cardholder Data Environment (CDE)**.

-
- All Norman Nerds personnel, contractors, and vendors with access to CHD or related systems.
 - All types of incidents, including but not limited to:
 - Unauthorized access or disclosure of CHD
 - Malware infection or ransomware
 - Denial-of-service attacks
 - Insider misuse or fraud
 - Loss or theft of devices or media
 - Physical security breaches
-

3. Policy Statement

Norman Nerds maintains a **PCI Incident Response Plan (IRP)** to ensure rapid identification, containment, and remediation of incidents involving CHD.

All employees are responsible for reporting security incidents immediately.

The **Incident Response Team (IRT)** leads investigations and coordinates communication with clients, regulators, and payment brands as necessary.

4. Incident Response Objectives

1. Detect and contain security incidents quickly.
2. Minimize damage to systems and data.
3. Preserve forensic evidence for investigation.
4. Communicate transparently with affected stakeholders.
5. Comply with PCI DSS, contractual, and legal notification obligations.
6. Prevent recurrence through corrective and preventive actions (CAPA).

5. Roles and Responsibilities

Role	Responsibilities
Incident Response Team (IRT)	Coordinates detection, analysis, containment, eradication, and recovery activities.
Incident Response Manager (IRM)	Leads IRT operations, authorizes escalation, and liaises with management and clients.
PCI Compliance Officer (PCO)	Ensures incidents are evaluated for PCI DSS scope and reporting requirements.
IT Security Officer (ITSO)	Conducts forensic analysis, evidence collection, and root cause analysis.
Communications Officer (CO)	Manages external communications, including notifications to clients, acquirers, or authorities.
Legal Counsel	Reviews incident reports, advises on notification requirements, and ensures compliance with Oklahoma and federal laws.
HR / Management	Executes disciplinary measures for internal incidents and coordinates employee communication.

6. Incident Response Lifecycle

Norman Nerds follows a **five-phase IR lifecycle** modeled after **NIST SP 800-61r2** and PCI DSS 12.10.2.

6.1 Identification

- Potential incidents may be detected through:
 - Intrusion detection/prevention systems (IDS/IPS)
 - SIEM alerts or log analysis
 - User or vendor reports
 - Anti-malware or DLP systems

-
- Physical access or surveillance anomalies
 - Employees must **report all suspicious activity immediately** via:
 - Incident Hotline: 1-800-NORMAN-SEC
 - Email: security@normannerds.com
 - Ticket: "Incident Report" category in the Helpdesk system
 - The **Incident Response Manager** validates and classifies the event within **1 hour** of detection.

6.2 Containment

- Isolate affected systems to prevent data exfiltration or lateral movement.
- Disable compromised user accounts and block malicious IPs.
- Preserve volatile data (memory dumps, session logs).
- Engage network and server teams to segment traffic if required.
- Document containment steps in the **Incident Tracking Log**.

6.3 Eradication

- Remove malware or malicious code from infected systems.
- Patch exploited vulnerabilities.
- Change passwords and revoke credentials used in the attack.
- Conduct forensic scans to ensure full removal.
- Validate integrity of critical files and configurations.

6.4 Recovery

-
- Restore systems from verified clean backups.
 - Validate system integrity and CHD protection mechanisms.
 - Monitor restored systems for recurrence or residual compromise.
 - Re-enable access only after formal approval by the IT Security Officer.
 - Notify stakeholders of successful recovery.

6.5 Lessons Learned

- Conduct a **post-incident review** within **10 business days**.
- Review:
 - Root cause analysis
 - Response timeline effectiveness
 - Gaps in detection, containment, or escalation
 - Required control improvements
- Document findings in the **Post-Incident Report (PIR)** and present to the **PCI Compliance Committee (PCC)**.
- Update policies or configurations as corrective measures.

7. Incident Classification Levels

Severity Definition		Example Incidents	Response Time
Critical	Confirmed compromise of CHD or PCI systems	Breach, exfiltration, ransomware	Immediate / within 1 hour
High	Attempted compromise or significant vulnerability exploitation	Unauthorized access attempts, malware infection	2 hours
Medium	Non-PCI systems impacted or potential precursor activity	Suspicious login, phishing	4 hours
Low	Minor events with no data exposure	Policy violation, accidental misconfiguration	1 business day

Norman Nerds

8. Notification and Reporting

8.1 Internal Notification

- The Incident Response Manager notifies:
 - Executive Management
 - Compliance Officer
 - IT Security Team
 - Legal Counsel (if legal exposure is likely)
- Status updates provided at least every 4 hours for active incidents.

8.2 External Notification

- When CHD is confirmed or suspected to be compromised:
 - Notify **affected clients and acquiring banks** immediately.

-
- Notify **payment brands (Visa, MasterCard, Discover, AmEx)** per PCI DSS 12.10.5.
 - Notify **Oklahoma Attorney General** and affected residents within **45 days**, as required by **Oklahoma Title 24 §163**.
 - Coordinate with forensic investigators as required by payment brand agreements.

8.3 Law Enforcement

- If criminal activity is suspected, contact **Oklahoma State Bureau of Investigation (OSBI)** or **FBI Cyber Division**.
 - Legal Counsel must approve any engagement before evidence is released.
-

Norman Nerds

9. Forensic Investigation Procedures

- Evidence must be handled in a manner that preserves integrity and chain of custody.
- Use forensically sound tools to capture:
 - Disk images
 - Memory dumps
 - Network traffic captures
 - Log files and system audit trails
- Evidence logs must include:
 - Collector name, date/time, and method used
 - Storage location and hash verification (SHA-256)
- Forensic results retained for **six (6) years** or per legal requirement.

10. Communication Plan

Communication Type	Audience	Responsible Party	Method
Internal Alert	IT & Management	Incident Response Manager	Email + Pager Notification
Client Notification	Affected Clients	Compliance Officer	Secure Email / Encrypted Report
Regulator Notification	Attorney General / PCI Brands	Legal Counsel	Secure Transmission / Certified Mail
Public Statement	Media, General Public	Communications Officer	Approved Press Release
Post-Incident Summary	Executives / PCC	Compliance Officer	Written Report

11. Documentation and Recordkeeping

All incident records must include:

- Date/time of detection and resolution
- Affected systems and data classification
- Description of actions taken
- Containment and remediation evidence
- Final root cause analysis and CAPA plan

All incident documentation is retained for a minimum of **six (6) years** and stored securely in the **Incident Management Repository (IMR)**.

12. Testing and Training

-
- The **Incident Response Plan** is tested **annually** through tabletop and live simulations.
 - Test scenarios include malware outbreak, data breach, and system compromise.
 - Test results documented, reviewed by the Compliance Committee, and updated as needed.
 - All employees receive **annual incident reporting training** as part of PCI awareness.
-

13. Enforcement

Failure to comply with this policy—including delayed reporting, unauthorized disclosure, or mishandling of evidence—will result in:

- Disciplinary action under **Section XIII – Sanctions Policy**.
- Potential civil or criminal penalties under state or federal law.
- Contractual remedies for vendors.

Norman Nerds

X. Vendor & Third-Party Management Policy

(Aligned with PCI DSS v4.0 Requirements 12.8 & 12.9)

1. Purpose

This policy establishes the requirements and processes for the selection, assessment, monitoring, and management of **vendors and third-party service providers** that store, process, transmit, or otherwise impact the security of **Cardholder Data (CHD)** on behalf of **Norman Nerds** or its clients.

The policy ensures that external entities maintain **equivalent levels of PCI DSS compliance** and that contractual, operational, and technical safeguards are implemented to protect payment card data and maintain Norman Nerds' compliance posture.

2. Scope

This policy applies to:

- All vendors, service providers, and subcontractors engaged by Norman Nerds that have access to CHD or can influence the security of systems within the **Cardholder Data Environment (CDE)**.
- All vendor contracts, service agreements, and outsourced operational relationships.
- All Norman Nerds departments responsible for procurement, IT, or vendor coordination.

3. Policy Statement

Norman Nerds will engage only with vendors and service providers that demonstrate adequate **PCI DSS compliance**, maintain strong data protection controls, and agree contractually to uphold these obligations.

All vendors are required to complete **security due diligence**, provide evidence of compliance, and be monitored continuously throughout their engagement.



4. Governance Structure

4.1 Roles and Responsibilities

Role	Responsibilities
Procurement Department	Initiates vendor onboarding, ensures inclusion of PCI DSS clauses in contracts.
PCI Compliance Officer (PCO)	Evaluates vendors’ PCI DSS compliance evidence, maintains the approved vendor register.
IT Security Officer (ITSO)	Conducts technical assessments, penetration tests, or reviews security controls for vendors.
Legal Counsel	Ensures that all contracts include appropriate confidentiality, liability, and breach notification clauses.

Role	Responsibilities
Vendor Relationship Owner (VRO)	Acts as the point of contact for ongoing vendor performance and risk monitoring.

5. Vendor Classification and Risk Rating

Vendors are classified according to the **risk they pose to CHD security**:

Tier	Description	Examples	PCI DSS Requirement Level
Tier 1 (High Risk)	Vendors that store, process, or transmit CHD, or manage systems within the CDE.	Payment processors, hosting providers, managed security services	Full PCI DSS compliance validation (SAQ D or ROC)
Tier 2 (Moderate Risk)	Vendors with indirect access to CHD systems or data (e.g., IT support, developers).	Cloud storage, backup services	SAQ A or equivalent compliance statement
Tier 3 (Low Risk)	Vendors without system or data access, but with potential physical or administrative impact.	Cleaning staff, document shredding, HR consultants	NDA and background checks only

6. Vendor Due Diligence and Onboarding

6.1 Pre-Engagement Assessment

Before entering any contractual agreement, the vendor must:

- Complete the **Vendor Security Assessment Questionnaire (VSAQ)**.
- Provide:
 - Current **PCI DSS Attestation of Compliance (AOC)** or **SAQ**.
 - Cybersecurity policy summary or SOC 2 Type II report.
 - Data protection, encryption, and incident response policy excerpts.

-
- Evidence of employee background checks and training.
 - The **PCI Compliance Officer** reviews submitted documentation to verify adequacy.

6.2 Risk Assessment

- Each vendor undergoes a **formal risk assessment** based on:
 - Nature of data handled.
 - Connectivity to Norman Nerds' systems.
 - Incident history and financial stability.
- Vendors scoring above the risk threshold require **executive approval** before onboarding.

6.3 Contractual Requirements

All vendor contracts must include:

1. **PCI DSS Compliance Clause** — Mandating adherence to current PCI DSS requirements.
2. **Data Protection Clause** — Ensuring encryption, access controls, and secure storage of CHD.
3. **Breach Notification Clause** — Requiring notification to Norman Nerds within **24 hours** of a suspected incident.
4. **Right to Audit Clause** — Allowing Norman Nerds to audit vendor controls annually or as needed.
5. **Termination Clause** — Allowing immediate termination upon noncompliance or breach.
6. **Confidentiality and Non-Disclosure Clauses (NDA)** — Protecting all client and CHD-related data.

7. Ongoing Vendor Monitoring

7.1 Compliance Verification

- Vendors must provide updated PCI DSS compliance evidence **annually**.
- The **Compliance Officer** verifies expiration dates for all AOCs and SAQs.
- Vendors failing to provide valid evidence are flagged as **noncompliant** and placed on probation until remediation.

7.2 Performance and Security Monitoring

-
- Vendor performance is reviewed **quarterly**, assessing:
 - SLA adherence.
 - Incident reports.
 - Penetration test or vulnerability scan results (if applicable).
 - Timeliness of remediation efforts.
 - High-risk vendors subject to more frequent reviews and audits.

7.3 Third-Party Attestations

- Norman Nerds may request **third-party audit attestations** or security certifications for validation (e.g., ISO 27001, SOC 2 Type II).
- For cloud or managed service providers, vendor **shared responsibility models** must be clearly documented.

Norman Nerds

8. Vendor Offboarding and Termination

When vendor relationships end:

1. All access credentials and network connections are revoked immediately.
2. Vendor accounts in Norman Nerds systems are disabled within **24 hours**.
3. Vendor must return or certify the destruction of all CHD or proprietary data.
4. The **Vendor Offboarding Form** must be completed, signed by Compliance and IT Security.
5. Offboarding records are retained for **six (6) years**.

9. Breach Response and Notification

If a vendor experiences a security incident involving CHD:

- They must **notify Norman Nerds within 24 hours** of discovery.
- Vendor must:
 - Provide an initial incident summary within 48 hours.
 - Conduct a forensic investigation and share results with Norman Nerds.
 - Coordinate containment and remediation efforts.
 - Bear all reasonable costs associated with notification, remediation, and forensic analysis if negligence is proven.
- Norman Nerds will assess whether PCI DSS or Oklahoma notification obligations apply under **Title 24 §162–164**.

10. Vendor Audit Program

Activity	Frequency	Responsible Party	Documentation
PCI Compliance Evidence Review	Annual	PCI Compliance Officer	Vendor Compliance Register
Contract Clause Verification	Annual	Legal Counsel	Contract Review Checklist
Vendor Risk Assessment	Annual	IT Security / Compliance	Risk Assessment Report
Vendor Access Audit	Quarterly	IT Security	Access Review Log
Vendor Offboarding Review	As needed	Compliance Officer	Offboarding Form

11. Documentation and Recordkeeping

All vendor management records must be retained in the **Vendor Compliance Repository** for at least **six (6) years**, including:

-
- Vendor Security Assessment Questionnaires (VSAQs).
 - Risk and due diligence reports.
 - Copies of PCI DSS AOCs, SAQs, or certifications.
 - Contracts and NDAs.
 - Access and offboarding records.
 - Audit results and corrective action plans.
-

12. Enforcement

Noncompliance with this policy—including failure to perform due diligence, maintain vendor records, or enforce contractual security clauses—may result in:

- Revocation of procurement authority.
- Contract termination or legal action against vendors.
- Disciplinary action per **Section XIII – Sanctions Policy** for internal personnel.

XI. Logging, Monitoring, and Audit Policy

(Aligned with PCI DSS v4.0 Requirement 10)

1. Purpose

The purpose of this policy is to define the requirements for logging, monitoring, and auditing system activity within **Norman Nerds' Cardholder Data Environment (CDE)** to ensure the detection, tracking, and analysis of security-related events that could indicate unauthorized access or compromise of **Cardholder Data (CHD)**.

This policy ensures compliance with **PCI DSS Requirement 10**, which mandates that all system components in scope for PCI DSS produce and retain audit logs sufficient to reconstruct events related to CHD access, modification, or deletion.

2. Scope

This policy applies to:

- All systems that **store, process, or transmit CHD**.
 - All components connected to or capable of impacting the CDE, including firewalls, routers, servers, applications, and databases.
 - All employees, contractors, and vendors responsible for system administration, monitoring, or audit functions.
-

3. Policy Statement

Norman Nerds shall collect, monitor, analyze, and retain logs from all PCI-relevant systems to provide accountability and forensic traceability.

All log data is protected against tampering, unauthorized access, and deletion, and is centrally managed through the company's **Security Information and Event Management (SIEM)** platform.

4. Logging Requirements

4.1 Events to be Logged

All systems within the CDE must log the following event types:

1. **User access events:**
 - Successful and failed login attempts.
 - Account lockouts and password resets.

-
- Privilege escalations or role changes.

2. System events:

- Startup, shutdown, or restarts of critical services.
- Configuration and policy changes.

3. Network events:

- Firewall rule modifications.
- VPN or remote access sessions.

4. Application events:

- Access to CHD or masked PAN data.
- Database query activity involving CHD.

5. Security events:

- Intrusion detection or prevention alerts.
- Anti-malware detections and quarantines.
- File integrity monitoring (FIM) alerts.
- Suspicious outbound traffic or DLP triggers.

4.2 Log Data Elements

Each log entry must include at minimum:

Element	Description
User ID	Account or process responsible for the event
Event Type	Description of action performed

Element	Description
Date and Time	Accurate, synchronized timestamp
Origin	Source IP address or system name
Success or Failure	Whether the event succeeded or failed
Affected Resource	File, system, or application accessed or modified

5. Time Synchronization

- All systems must synchronize their clocks using **Network Time Protocol (NTP)** to a trusted, authenticated source.
- Time discrepancies greater than **±2 seconds** from NTP standard are automatically corrected.
- Time synchronization logs retained for six (6) years.
- Accurate timestamps ensure forensic evidence remains admissible and verifiable.

6. Centralized Log Management

6.1 SIEM Integration

- All critical systems and network devices forward logs in real time to the **Norman Nerds Security Information and Event Management (SIEM)** platform.
- SIEM automatically aggregates, normalizes, and correlates log data from multiple sources.
- Data retention within SIEM is configured for **12 months active storage** and **six (6) years archival storage**.

6.2 Log Transmission and Protection

- Logs are transmitted over **TLS 1.3** or **IPsec VPN** to prevent interception or tampering.
- Logs stored in encrypted form (AES-256) with role-based access restrictions.
- Only authorized personnel (Compliance Officer, IT Security Officer, or auditors) can access logs.

-
- SIEM access is subject to multi-factor authentication (MFA).
-

7. Log Retention and Storage

Log Type	Minimum Retention	Access Availability
System and Application Logs	1 year active, 6 years archived	3 months immediately accessible
Security Logs (IDS/IPS, FIM, SIEM)	1 year active, 6 years archived	3 months immediately accessible
Network Logs (firewalls, routers)	1 year active, 6 years archived	3 months immediately accessible
Authentication and Access Logs	1 year active, 6 years archived	3 months immediately accessible

Archived logs are digitally signed or hashed (SHA-256) to ensure integrity verification.

8. Monitoring and Alerting

8.1 Continuous Monitoring

- The **IT Security Team** monitors SIEM dashboards continuously (24/7) for:
 - Repeated login failures
 - Unauthorized access attempts
 - Unexpected firewall changes
 - Malware or intrusion alerts
 - Suspicious data transfer activity
- Automated alert rules are defined for all high-severity conditions.

8.2 Alert Management

- Alerts classified by severity:
 - **Critical** – Possible CHD breach or CDE compromise (immediate escalation).

-
- **High** – Unauthorized access attempt or failed security control (1-hour response).
 - **Medium** – Suspicious user or network behavior (4-hour response).
 - **Low** – Minor anomalies (reviewed daily).
- All alerts are logged in the **Incident Tracking System** and linked to corresponding investigation tickets.
-

9. Log Review Procedures

Review Activity	Frequency	Responsible Role	Output
Firewall & IDS/IPS Logs	Daily	IT Security Officer	Security Event Report
Access Control & Authentication Logs	Daily	IT Security	User Access Review Summary
Application & Database Logs	Weekly	Application Administrator	Data Access Report
System Configuration Logs	Weekly	Infrastructure Manager	Configuration Audit Report
SIEM Alert Summary	Monthly	Compliance Officer	Monthly Security Summary Report
Log Integrity Verification	Quarterly	IT Security	Log Integrity Report

Each report is retained for **six (6) years** and reviewed during quarterly **PCI Compliance Committee** meetings.

10. File Integrity Monitoring (FIM)

- FIM tools must be configured to detect unauthorized changes to critical files (system binaries, configurations, logs).

-
- FIM generates alerts for:
 - Unauthorized file modifications.
 - Unexpected file deletions.
 - New file creation in protected directories.
 - Baseline configurations reviewed weekly and updated as authorized.
 - FIM event reports are integrated into the SIEM.
-

11. Audit Trail Review and Maintenance

- Audit trails must reconstruct:
 - Who accessed or modified CHD.
 - What actions were taken.
 - When access occurred.
 - Where access originated.
 - All audit trail mechanisms are reviewed annually for completeness.
 - Audit trails must be protected against:
 - Modification or deletion.
 - Insertion of false records.
 - Unauthorized access by system administrators (via separation of duties).
-

12. Testing and Validation

Test Type	Frequency	Responsible Role	Evidence Retention
SIEM Functionality Validation	Quarterly	IT Security Officer	SIEM Audit Log
Log Integrity Verification	Quarterly	Compliance Officer	Integrity Check Report
Log Retention Validation	Annual	Compliance Officer	Retention Compliance Record
Alert Effectiveness Test	Quarterly	IT Security	Incident Drill Report

13. Audit and Reporting

- The **PCI Compliance Officer** conducts **quarterly reviews** of SIEM audit logs and monitoring effectiveness.
- Findings, exceptions, and improvements are documented in the **Quarterly Audit Report**.
- Reports presented to the **PCI Compliance Committee (PCC)** for approval and follow-up.
- External auditors (QSA, ROC) have read-only access to required logs during compliance assessments.

14. Documentation and Recordkeeping

All audit and monitoring documentation must include:

- Source system and log type.
- Reviewer's name, date, and time of review.
- Findings, anomalies, and remediation actions.
- Management approval and closure evidence.

Records are retained in the **Compliance Repository** for **six (6) years**.

15. Enforcement

Noncompliance with this policy—including failure to enable logging, manipulate logs, or ignore alerts—will result in:

- Immediate escalation to the Compliance Officer.
- Disciplinary measures under **Section XIII – Sanctions Policy**.
- Potential termination of administrative privileges or employment.
- Contractual or regulatory reporting obligations if intentional tampering is discovered.

Norman Nerds

XII. Security Awareness, Training & Continuous Compliance Policy

(Aligned with PCI DSS v4.0 Requirements 12.6 and 12.11)

1. Purpose

This policy establishes the requirements for **security awareness education, training, and continuous compliance monitoring** at **Norman Nerds** to ensure all workforce members understand their roles in protecting **Cardholder Data (CHD)** and maintaining **PCI DSS compliance**.

It ensures that personnel remain knowledgeable about emerging security threats, data protection obligations, and incident response procedures throughout their employment.

2. Scope

This policy applies to:

- All Norman Nerds employees, contractors, interns, and third-party personnel with access to systems that store, process, or transmit CHD.
 - All new hires as part of onboarding, and all existing staff during annual and ad-hoc security awareness activities.
 - All departments and roles involved in PCI DSS operations, management, and vendor oversight.
-

3. Policy Statement

Norman Nerds requires that all personnel receive **initial and ongoing PCI DSS security training**.

Training and awareness programs are mandatory, role-based, and tracked for completion.

Compliance with these programs is verified through continuous reviews, testing, and documented evidence as part of the company's **PCI Continuous Compliance Program**.

4. Security Awareness Program Overview

4.1 Program Objectives

1. Ensure that every employee understands their PCI DSS responsibilities.
2. Reinforce best practices for handling, storing, and transmitting CHD securely.
3. Raise awareness about evolving security threats (phishing, social engineering, malware, insider threats).
4. Promote a proactive reporting culture for suspicious activities.
5. Maintain an auditable record of all training events and completions.

4.2 Training Structure

The awareness program consists of:

- **Onboarding Training:** Provided to all new employees within 5 business days of hire.
- **Annual Refresher Training:** Mandatory for all staff every 12 months.
- **Role-Based Training:** Specialized instruction for system administrators, developers, compliance staff, and vendors.
- **Ad-Hoc Training:** Issued in response to new PCI DSS updates, audit findings, or emerging threats.

5. Training Curriculum

Module	Target Audience	Topics Covered	Delivery Method
PCI DSS Overview	All personnel	PCI DSS principles, CHD protection, scope awareness	E-learning + quiz
Acceptable Use & Access Control	All personnel	Passwords, MFA, workstation security, access procedures	Online training
Incident Response & Reporting	All personnel	Recognizing and reporting security incidents	Interactive scenario

Module	Target Audience	Topics Covered	Delivery Method
Secure Development Practices	Developers	OWASP Top 10, input validation, code reviews	Classroom or virtual workshop
Data Encryption & Key Management	IT Security, DBAs	PCI DSS Req. 3 & 4 technical controls	Instructor-led
Physical Security	Facilities, IT	Badge use, visitor control, secure storage	On-site walkthrough
Vendor & Third-Party Security	Procurement, Legal	Due diligence, contract clauses, vendor risk	E-learning
Social Engineering Awareness	All personnel	Phishing, vishing, and tailgating prevention	Quarterly simulation
Continuous Compliance & Audit Readiness	Management & Compliance	Internal reviews, evidence collection, remediation	Workshop

Each training module includes a comprehension test with a minimum passing score of **80%**.

6. Documentation and Tracking

- All training completions are tracked in the **Learning Management System (LMS)**.
 - The LMS records:
 - Employee name and department
 - Course name and completion date
 - Assessment score and certification number
 - Renewal or next due date
 - Compliance reports generated **quarterly** for review by the **Compliance Officer**.
 - Training completion is a prerequisite for **system access provisioning**.
-

7. Employee Acknowledgment

Each employee must electronically sign the **PCI Security Awareness Acknowledgment Form**, confirming:

- They understand and agree to comply with PCI DSS and company security policies.
- They will immediately report any suspected security incident or policy violation.
- They are aware of disciplinary actions associated with policy noncompliance (Section XIII).

Acknowledgments are retained for **six (6) years** in personnel records.

8. Continuous Compliance Review (PCI DSS Requirement 12.11)

8.1 Purpose

Continuous compliance reviews verify that security and operational practices remain aligned with PCI DSS requirements throughout the year, not only during annual audits.

8.2 Review Activities

Norman Nerds conducts quarterly **Continuous Compliance Reviews** including:

- Verification of firewall and router configurations.
- Access control and password policy audits.
- Patch management validation and vulnerability remediation review.
- Incident response readiness assessment.
- Evidence collection for self-assessment (SAQ) or Report on Compliance (ROC).
- Review of vendor PCI DSS attestations and certificates.

8.3 Methodology

- Compliance Officer and IT Security jointly review logs, configurations, and controls.
- Each review documented in the **Compliance Validation Report (CVR)**.

-
- Nonconformities logged and assigned corrective action owners with due dates.
 - Status of open compliance items reviewed monthly by the **PCI Compliance Committee (PCC)**.

8.4 Internal Audit Integration

- Findings from Continuous Compliance Reviews feed into the **Annual PCI Internal Audit Plan**.
 - Independent validation by the Compliance Officer ensures objectivity.
 - Audit evidence retained for **six (6) years**.
-

9. Awareness Reinforcement Activities

To maintain a culture of vigilance, Norman Nerds conducts the following recurring activities:

Activity	Frequency	Responsible Department
Phishing simulation campaigns	Quarterly	IT Security
Security newsletters and alerts	Monthly	Compliance
Security posters / internal communications	Quarterly	HR / Marketing
PCI DSS update briefings	As needed	Compliance Officer
“Security Champion” recognition program	Semi-annual	Executive Management

10. Metrics and Key Performance Indicators (KPIs)

Metric	Target	Measured By
Training completion rate	≥ 99%	Compliance Officer
Phishing simulation click rate	≤ 5%	IT Security
Awareness acknowledgment compliance	100%	HR / Compliance
Quarterly compliance reviews completed	100% on schedule	Compliance Officer

Metric	Target	Measured By
Identified training-related incidents	≤ 1 per quarter	Security Awareness Team

Results are reviewed quarterly by the **PCI Compliance Committee** and used to adjust training or awareness materials.

11. Testing and Validation

Validation Type	Frequency	Responsible Role	Retention Period
Security Training Audit	Annual	Compliance Officer	6 years
Phishing Simulation Report	Quarterly	IT Security Officer	6 years
Continuous Compliance Review Report	Quarterly	Compliance Officer	6 years
Awareness Program Evaluation	Annual	HR / Compliance	6 years

12. Enforcement

Failure to complete required training, submit acknowledgments, or participate in compliance reviews may result in:

- Temporary suspension of system access.
 - Disciplinary action per **Section XIII – Sanctions Policy**.
 - Contract suspension for third-party personnel.
-

13. Recordkeeping

All records related to training, awareness activities, and compliance reviews must be retained for **six (6) years**, including:

- Course materials and attendance logs.
- Acknowledgment forms.

-
- Quarterly review reports and audit evidence.
 - Training completion certificates.

Documents are stored in the **Compliance Repository** and are available for QSA or ROC validation.

XIII. Enforcement & Sanctions Policy

(Aligned with PCI DSS v4.0 Requirement 12.10.6)

1. Purpose

The purpose of this policy is to define the disciplinary, contractual, and administrative actions that may be taken by **Norman Nerds** in response to noncompliance with the company's **PCI DSS policies, security controls, or regulatory obligations**.

This policy ensures that all workforce members, contractors, and vendors are aware of the consequences of failing to protect **Cardholder Data (CHD)** and adhere to established security protocols.

2. Scope

This policy applies to:

- All Norman Nerds employees, contractors, consultants, interns, and third-party service providers.
- All personnel with logical or physical access to the **Cardholder Data Environment (CDE)**.
- Any individual whose actions or omissions could affect PCI DSS compliance, data confidentiality, integrity, or availability.

3. Policy Statement

Norman Nerds enforces a **zero-tolerance approach** to willful or negligent violations of PCI DSS and company security policies.

All employees and vendors are required to understand their obligations under PCI DSS, Oklahoma data protection laws, and corporate ethics guidelines.

Sanctions are applied consistently, fairly, and in proportion to the severity of the violation.

4. Roles and Responsibilities

Role	Responsibilities
HR Department	Administers disciplinary actions for employees; maintains sanction records.
PCI Compliance Officer (PCO)	Determines impact of policy violations on PCI compliance status; coordinates with HR.
IT Security Officer (ITSO)	Investigates technical incidents and provides evidence of violation.
Legal Counsel	Ensures sanctions and termination actions comply with Oklahoma employment law.
Department Managers	Ensure staff are informed of expectations and report policy breaches promptly.
Vendors / Service Providers	Must adhere to contractually required PCI DSS and security obligations.

5. Violations Subject to Enforcement

Violations may include, but are not limited to:

5.1 Data Security Violations

- Unauthorized access, disclosure, or modification of CHD or system credentials.
- Storing CHD in unauthorized locations (e.g., email, USB, personal cloud).
- Circumventing encryption, MFA, or access control measures.
- Failure to report a known or suspected data breach.

5.2 Policy and Process Violations

- Failure to comply with documented PCI DSS policies or procedures.
- Ignoring required patch management, configuration, or audit review duties.
- Bypassing change management or firewall authorization processes.
- Sharing passwords, access tokens, or privileged credentials.

5.3 Negligence or Misconduct

- Mishandling physical media containing CHD.
- Falsifying compliance records or audit results.
- Unauthorized use of systems for personal or illegal activities.
- Intentional tampering with logs or evidence during incident investigations.

5.4 Vendor / Third-Party Violations

- Failure to maintain current PCI DSS certification (SAQ/AOC).
- Breach of contract clauses related to data protection.
- Unauthorized subcontracting without approval.
- Delayed breach notification beyond required timeframes.

6. Sanction Levels

Sanctions are proportionate to the severity, intent, and impact of the violation:

Severity Level Description		Potential Consequences
Level 1 – Minor	Unintentional violation with no data exposure or compliance impact.	Written warning, mandatory retraining, manager notification.
Level 2 – Moderate	Repeated or negligent violation with limited risk to CHD or systems.	Formal reprimand, probation, access restriction, compliance retraining.

Severity Level Description		Potential Consequences
Level 3 – Major	Serious violation causing potential or confirmed CHD exposure or PCI noncompliance.	Suspension, loss of role privileges, written performance action plan.
Level 4 – Critical	Intentional misconduct, data theft, or obstruction of investigation.	Immediate termination, legal action, civil/criminal referral, vendor contract termination.

All disciplinary actions must be documented in the **Sanctions Log**, reviewed by HR, and co-signed by the **PCI Compliance Officer**.

7. Investigation and Enforcement Process

7.1 Identification

- Violations may be detected through:
 - Security monitoring (SIEM, FIM, DLP).
 - Audit findings.
 - Incident reports or whistleblower submissions.
 - Manager or peer reports.

7.2 Investigation

- The **IT Security Officer** conducts preliminary evidence collection.
- The **Compliance Officer** determines whether the incident constitutes a PCI DSS violation.
- **Legal Counsel** ensures the process adheres to due process and Oklahoma labor laws.
- A formal **Incident Investigation Report (IIR)** is produced within **10 business days**.

7.3 Determination

- The **PCI Compliance Committee (PCC)** reviews investigation results and recommends sanctions.
- Final approval provided by the **Executive Management** and **HR Director**.
- Findings communicated confidentially to affected personnel.

7.4 Implementation

- HR enforces disciplinary measures and updates personnel records.
 - IT Security ensures removal or restriction of access privileges if applicable.
 - Vendors found in violation receive written notice with a defined remediation window or immediate termination depending on severity.
-

8. Vendor Enforcement and Contractual Remedies

For third-party providers or contractors:

- Breaches of PCI DSS or data protection obligations trigger immediate investigation.
 - Vendors must cooperate fully with incident inquiries and provide forensic or compliance evidence.
 - Contractual remedies may include:
 - Termination for cause.
 - Indemnification for damages or regulatory fines.
 - Suspension of services until compliance is restored.
 - Mandatory retraining or re-certification.
 - Reinstatement of vendor access contingent on written approval from the **Compliance Officer**.
-

9. Appeal and Review Process

- Employees or vendors may appeal disciplinary decisions in writing within **10 business days** of notification.
- Appeals reviewed by an independent **Sanctions Review Panel** consisting of HR, Legal, and Compliance.
- The panel's decision is final and documented in the Sanctions Log.

-
- No retaliation is permitted against individuals who report violations or appeal in good faith.
-

10. Documentation and Recordkeeping

- All sanctions, investigation reports, and related communications are retained for **six (6) years** in the **Compliance Repository**.
 - Access limited to HR, Compliance, Legal, and Executive Management.
 - Records include:
 - Incident summary and evidence.
 - Sanction level and justification.
 - Corrective action or retraining documentation.
 - Approval signatures and closure date.
-

11. Corrective and Preventive Actions (CAPA)

Following any confirmed violation, the **Compliance Officer** must:

1. Identify root cause and contributing factors.
2. Develop corrective actions to prevent recurrence.

-
3. Assign responsibilities and deadlines for mitigation.
 4. Verify implementation during the next compliance review.
 5. Document results in the **CAPA Register**.
-

12. Enforcement Consistency and Confidentiality

- Sanctions are applied consistently regardless of position or tenure.
 - All disciplinary and vendor enforcement actions remain confidential.
 - Only individuals with a legitimate business need may access sanction-related records.
 - Annual HR audits ensure equitable enforcement across departments.
-

13. Legal and Regulatory References

This policy supports compliance with:

- PCI DSS v4.0 Requirement 12.10.6
 - Oklahoma Title 24 §162–165 – Data Breach Notification and Security Laws
 - NIST SP 800-53 Rev. 5 (PL-4 & PS-8) – Personnel Sanctions and Accountability Controls
 - Federal Trade Commission (FTC) Safeguards Rule – Enforcement Standards for Data Protection
-

14. Enforcement Authority

Final enforcement authority lies with the **Executive Management Team**, advised by:

- PCI Compliance Officer
- HR Director
- Legal Counsel

These authorities may delegate investigatory responsibilities but retain final sanction approval powers.

15. Policy Review and Updates

- The **Sanctions Policy** is reviewed **annually** by the PCI Compliance Officer and Legal Counsel.
 - Updates must incorporate:
 - New or amended PCI DSS enforcement requirements.
 - Oklahoma or federal employment and data protection law changes.
 - Lessons learned from internal investigations or audits.
 - Revised policies distributed within 30 days of approval and acknowledgment required from all staff.
-

16. Enforcement Examples

Violation Example	Severity	Action Taken
Employee fails to lock workstation with CHD access.	Minor	Written warning and retraining.
Developer bypasses change control for live payment app patch.	Moderate	1-week suspension, change control audit, retraining.
Admin disables logging on CDE server to speed up testing.	Major	Access removal, probation, written final warning.
Vendor stores CHD on unapproved system, exposing PAN data.	Critical	Contract termination, forensic audit, regulator notification.

17. Enforcement Outcome Reporting

- Quarterly **Sanction Summary Reports** compiled by the **Compliance Officer** for executive review.
- Reports identify:

-
- Number and type of violations.
 - Sanction trends.
 - Preventive measures implemented.
 - Lessons integrated into training programs (Section XII).

XIV. Continuous Improvement, Policy Review & Attestation

(Aligned with PCI DSS v4.0 Requirements 12.1.3 and 12.11.2)

1. Purpose

This section defines the processes through which **Norman Nerds** maintains ongoing compliance, continuously improves its PCI DSS control environment, and documents official management attestation to the effectiveness of its security policies and practices.

By implementing continuous review and improvement mechanisms, Norman Nerds ensures that PCI DSS compliance is not treated as a one-time certification effort, but as an **ongoing, living process** integrated into everyday operations.

2. Scope

This policy applies to:

-
- All PCI DSS–related policies, procedures, and controls implemented by Norman Nerds.
 - All personnel responsible for maintaining and enforcing PCI DSS requirements.
 - All business units, systems, and vendors contributing to the protection of **Cardholder Data (CHD)**.
-

3. Policy Statement

Norman Nerds commits to:

1. Conducting regular policy reviews and updates to align with the latest **PCI DSS standards, client expectations, and threat intelligence**.
2. Ensuring all system and procedural improvements are documented, communicated, and auditable.
3. Maintaining **executive-level attestation** confirming organizational adherence to PCI DSS requirements.

Continuous improvement is built into Norman Nerds’ **PCI Compliance Lifecycle**, ensuring that controls evolve as the company grows and the threat landscape changes.

4. Continuous Improvement Framework

The continuous improvement process integrates lessons learned from audits, incidents, and compliance reviews into Norman Nerds’ operational and policy frameworks.

Phase	Description	Frequency	Responsible Party
Plan	Identify compliance gaps and control enhancements from prior assessments, incidents, and reviews.	Quarterly	PCI Compliance Officer
Implement	Apply improvements to controls, documentation, and staff training.	Ongoing	Department Managers / IT Security
Monitor	Track effectiveness of implemented improvements via metrics and testing.	Monthly	Compliance Officer / Internal Audit
Evaluate	Validate improvements during annual PCI audit or external QSA review.	Annual	Compliance Officer / Executive Management

5. Policy Review and Maintenance

5.1 Annual Review

- All PCI DSS policies and procedures must be reviewed at least **annually** and after any:
 - Major change in PCI DSS requirements.
 - Security breach or incident involving CHD.
 - Significant modification to Norman Nerds' network, systems, or business processes.
- Each review must confirm:
 - Continued alignment with **PCI DSS v4.0** controls.
 - Accuracy and currency of referenced procedures and forms.
 - Effectiveness of security roles, responsibilities, and oversight mechanisms.

5.2 Review Responsibilities

- **Primary Reviewer:** PCI Compliance Officer
- **Secondary Reviewers:** IT Security Officer, Department Heads, Legal Counsel
- **Approver:** Executive Management

All reviews are documented using the **Policy Review Log**, which records:

- Reviewer names and titles
- Review date and version
- Summary of changes and rationale
- Signatures of reviewers and approvers

6. Continuous Compliance Program Metrics

The **PCI Compliance Officer** maintains key performance metrics to measure the effectiveness of Norman Nerds' compliance posture:

Metric	Target / Frequency	Owner
Policy updates completed on schedule	100% annually	Compliance Officer
PCI control testing coverage	100% of in-scope systems	IT Security Officer
Open audit findings resolved	100% within 90 days	Department Managers
Employee training compliance	≥ 99% completion rate	HR / Compliance
Continuous compliance review completion	100% quarterly	Compliance Officer

Metrics are reported quarterly to the **PCI Compliance Committee (PCC)** and annually to **Executive Management**.



7. External Audit and Certification Alignment

- Norman Nerds will undergo an **annual PCI DSS self-assessment (SAQ-D)** or, where applicable, an **independent Report on Compliance (ROC)** performed by a Qualified Security Assessor (QSA).
- Findings and recommendations from QSA audits are tracked to closure through the **Corrective Action and Preventive Action (CAPA)** program.
- Audit reports and attestation documentation retained for **six (6) years**.

8. Communication of Policy Updates

- Updated versions of this manual and related procedures must be distributed to all affected personnel and management teams.
- Notification of updates delivered via internal communications and mandatory acknowledgment forms in the **Learning Management System (LMS)**.

-
- Employees are required to review and acknowledge all major policy updates within **10 business days** of issuance.
-

9. Executive Attestation of Compliance

At least annually, the **Executive Management Team** of Norman Nerds must provide a signed **PCI DSS Compliance Attestation Statement**, certifying that:

1. All applicable PCI DSS requirements have been reviewed and implemented.
2. All systems storing, processing, or transmitting CHD have been validated and remain within PCI scope.
3. Appropriate policies, controls, and monitoring mechanisms are in place and functioning effectively.
4. Any gaps identified in compliance have been remediated or are under an approved remediation plan.
5. All employees and vendors have received mandatory training and acknowledge their PCI responsibilities.

Norman Nerds – PCI DSS Compliance Attestation Statement (2025)

Effective Date: November 1, 2025

Policy Version: 1.0

We, the undersigned, attest that Norman Nerds maintains compliance with the **Payment Card Industry Data Security Standard (PCI DSS) v4.0** as of the date above, and that all requirements applicable to our environment have been addressed in accordance with the scope of this manual.

Name	Title	Department	Signature	Date
[Name]	Chief Executive Officer (CEO)	Executive	_____	_____
[Name]	Chief Information Security Officer (CISO)	Information Security	_____	_____
[Name]	PCI Compliance Officer	Compliance	_____	_____
[Name]	Chief Technology Officer (CTO)	Technology	_____	_____
[Name]	Legal Counsel	Legal Affairs	_____	_____

10. Documentation Retention

All documents related to policy reviews, audit findings, and attestation records must be retained for a **minimum of six (6) years**.

These include:

- Policy Review Logs
- Compliance Validation Reports
- CAPA records
- Executive Attestation Statements
- QSA / SAQ audit evidence and correspondence

Records are securely stored within the **Compliance Repository**, accessible only to authorized personnel under multi-factor authentication and encryption.

11. Continuous Improvement Cycle Integration

Norman Nerds incorporates feedback from:

- Security incidents (Section IX)
- Vendor and audit findings (Section X & XI)
- Employee and QSA feedback
into its next policy review cycle.

Each improvement or control enhancement is logged in the **Continuous Improvement Register**, which tracks:

- Issue origin and description
- Corrective or preventive action taken
- Owner and completion date
- Validation and approval signatures

The register is reviewed quarterly by the **PCI Compliance Committee**.

12. Policy Effectiveness and Acknowledgment

All Norman Nerds personnel and vendors are required to:

1. Review this PCI DSS Compliance Policy Manual in full.
2. Acknowledge understanding and adherence via signed or electronic form.
3. Recognize that compliance with this policy is a condition of employment or engagement.

Acknowledgment logs are retained for audit and legal purposes.

13. Enforcement and Review Authority

This policy shall be enforced under the authority of:

- Executive Management
- PCI Compliance Officer
- IT Security Officer
- Legal Counsel

All reviews, revisions, and attestations must be approved by the **PCI Compliance Committee (PCC)**.

14. Effective Date and Version Control

Version	Effective Date	Description of Change	Approved By
1.0	November 5, 2025	Initial issue of PCI DSS Compliance Policy Manual for Norman Nerds	Executive Management / PCI Compliance Committee

Norman Nerds