PCI Policy Template, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Olumuyiwa Agunbiade
Last Review Date: July 2023

PCI Policy Template

Access Control Policy

PCI DSS v 3.2.1

Purpose

To establish the rules for the protection of the cardholder data environment.

Audience

The PCI Access Control Policy applies to all individuals who interact with cardholder data for (Company).

Policy

- Access to the CDE is based on need-to-know.
- The level of access required to perform authorized tasks may be approved, following the concept of least privilege.
- Only approved (Company) devices may be used to connect to the CDE either onsite or remotely.
- Only approved staff can install, modify or remove devices in the CDE.
- All accounts created must have an associated and documented request and approval.

Account Management

PCI DSS v3.2.1: 8, 12

Purpose

To establish the rules for the protection of the cardholder data environment.

Audience

The PCI Account Management Policy applies to all individuals who interact with cardholder data for (Company)

Policy

- All users must sign the (Company) Corporate Information Security and PCI Policy Acknowledgements before access is granted to the CDE.
- All accounts must be uniquely identifiable using the user name assigned by (Company) IT and include verification that redundant user IDs are not used.
- All accounts require at least one approved method to authenticate users to system components (password, token, smart card, biometric, etc.).
- The use of group or shared accounts is prohibited.
- Procedures must exist for account creation, modification and termination.
- All non-console administrative access into the CDE, both internal and external, must incorporate multi-factor authentication.

- Vendor/third-party access accounts must be enabled only when needed and disabled at all other times.
- Vendor/third-party access accounts must be monitored when in use.
- Passwords must be at least 7 characters with a maximum age of 90 days.
- Accounts must be locked out for 30 minutes after 6 failed login attempts.

Asset Management

PCI DSS v3.2.1: 2, 9

Purpose

To establish the rules for the configuration, maintenance and protection of the cardholder data environments.

Audience

The Asset Management Policy applies to all individuals who administer the (Company) cardholder data environments (CDE).

Policy

- All card reader devices must be documented via inventory control and monitoring procedures, including device status (deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit) and inventoried no less than annually.
- All devices must be classified to determine sensitivity.
- Any variances in inventory, including missing or substituted devices, must be reported.
- Non-approved cardholder data capture devices must not be connected to the (Company) CDE.
- Devices that capture payment data (card-present transactions) must be protected from tampering and substitution.
- Access to devices by third-party personnel for repair/maintenance must be monitored.
- All devices and media must be physically secured.
- Backups must be stored in a secure location and the backup location's security must be reviewed at least annually.
- Management must approve all devices that are being moved from a secure area.
- All devices must be transferred using a secure courier or other authorized delivery method that can be accurately tracked.
- Devices that are no longer needed must be securely destroyed.

Data Protection

PCI DSS v3.2.1: 3, 4, 9

Purpose

To establish the rules for the protection of cardholder data.

Audience

The PCI Data Protection Policy applies to all individuals who interact with cardholder data for (Company).

Policy

- Sensitive authentication data (three or four-digit code found on front or back of the credit card) must never be stored after authorization of the credit card.
- Cardholder data and sensitive authentication data is confidential.
- Data must be securely shredded or destroyed when no longer needed.
- The primary account number (PAN) must be masked when displayed and only those with a legitimate business need maybe able to see the full PAN.
- Unprotected PANs must not be sent using end-user messaging technologies (i.e. email, instant messaging, SMS, chat).
- Any department or system at (Company) that plans to process, use, store, or transmit cardholder data must contact the Security/PCI Office prior to using any cardholder data.
- PCI DSS requirements apply if cardholder data is stored, processed or transmitted.
- Permanent storage of cardholder data is prohibited.
- Use of recording devices to store photographs, videos, audio or other forms of sensitive authentication data is prohibited .
- Retention requirements must be established for cardholder data. Cardholder data storage must be kept to a minimum and retained only as long as is required by legal, regulatory and/or business requirements.
- Data must be securely shredded when no longer needed or according to the retention policy.
- The primary account number (PAN) must be masked when displayed.
- The PAN must be rendered unreadable anywhere it is stored using any of the following:
    - One-way hashes based on strong cryptography,
    - Truncation,
    - Index tokens and pads, or
    - Strong cryptography with associated key-management processes and procedures.
- If disk encryption is used, logical access must be managed separately and independently of native operating system authentication.

Encryption Management

PCI DSS v3.2.1: 3, 4

Purpose

To establish the rules for the configuration, maintenance and protection of the cardholder data environments.

Audience

The Encryption Management Policy applies to all individuals who administer the (Company) cardholder data environments (CDE).

Policy

- Encryption key management procedures must be in place.
- Strong cryptography and security protocols must be used when transmitting sensitive cardholder data over open, public networks.
- Unprotected PANs must not be sent using end-user messaging technologies (i.e. email, instant messaging, SMS, chat).

Firewall Management

PCI DSS v3.2.1: 1

Purpose

To establish the rules for the configuration, maintenance and protection of the cardholder data environments.

Audience

The Firewall Management Policy applies to all individuals who administer the (Company) cardholder data environments (CDE).

Policy

- Configuration files must be secured and synchronized.
- Firewall must be located at each internet connection and between any DMZ and the internal network zone
- A list of firewall rules, including business justification for use of all services, protocols and ports allowed must be maintained.
- Perimeter firewalls must be installed between all wireless networks and the cardholder data environment (CDE).
- Personal firewalls must be installed on any mobile or employee-owned devices that connect to the internet when outside the network and which are used to access the network.
- A DMZ must be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports.
- Anti-spoofing measures must be implemented to detect and block forged source IP addresses from entering the network.
- System components that store cardholder data must be in an internal network zone, segregated from the DMZ and other untrusted networks.
- Private IP addresses and routing information must not be disclosed to unauthorized parties.

Incident Management

PCI DSS v3.2.1: 12

Purpose

To establish the rules for the protection of the cardholder data environment.

Audience

The PCI Incident Management Policy applies to all individuals who administer the (Company) cardholder data environments (CDE).

Policy

- An incident response plan must be implemented and tested at least annually.
- Incident response personnel must be available on a 24/7 basis to respond to alerts.

Logging and Monitoring

PCI DSS v3.2.1: 10

Purpose

To establish the rules for the configuration, maintenance and protection of the cardholder data environments.

Audience

The Auditing and Monitoring Policy applies to all individuals who administer the (Company) cardholder data environments (CDE).

Policy

- All access to system components must have a corresponding audit trail.
- All critical system time clocks must retrieve time information from a single reference time source on a regular basis so that timestamps in logs are consistent.
- Audit trails must be secured to prevent altering.
- Logs and security events must be reviewed for all system components to identify anomalies or suspicious activity.
- Audit trails must be maintained for at least one year, with a minimum of three months immediately available for analysis.

Network Management

PCI DSS v3.2.1: 1, 2, 4, 5, 11

Purpose

To establish the rules for the configuration, maintenance and protection of the cardholder data environments.

Audience

The Network Management Policy applies to all individuals who administer the (Company) cardholder data environments (CDE).

Policy

Network Configuration

- All vendor-supplied default accounts must be changed, and removed or disabled if unnecessary, before installing a system on the network.
- A network diagram that identifies all connections between CDE and other networks, including any wireless networks must be maintained.
- A data flow diagram that shows cardholder data flow across systems and networks must be maintained.
- Configuration standards must exist:
    - for all system components and address all known security vulnerabilities
    - include a description of groups, roles and responsibilities for management of network components
    - Operational procedures for managing firewalls must be documented
    - Review of firewall rule sets must occur at least every six months.
    - Servers must be limited to one primary function per server or one primary function per system component if virtual.
- All non-console administrative access must be encrypted.
- An inventory of all system components must be maintained.
- Anti-virus must be installed on all systems commonly affected by malicious software (i.e. personal computers and servers).
- All anti-virus must:
    - Be kept current,
    - Perform periodic scans,
    - Generate audit logs
    - Be actively running,
    - Not be able to be disabled or altered by users.

Wireless Networking

- Wireless networks transmitting cardholder data or connected to the CDE must use industry best practices to implement strong encryption for authentication and transmission.
- A process to test for presence of wireless access points must be implemented and conducted quarterly. All authorized and unauthorized wireless access points must be identified.

Physical Security

PCI DSS v3.2.1: 9

Purpose

To establish the rules for the protection of the cardholder data environment.

Audience

The PCI Physical Security Policy applies to all individuals who interact with cardholder data for (Company).

Policy

- Access must be based on job need.
- All access is revoked immediately upon termination and all keys/cards are immediately returned or disabled.
- Controls must be in place to distinguish between onsite personnel and visitors (i.e. ID badges).
- All media must be physically secured.
- Devices that capture payment data (card-present transactions) must be protected from tampering and substitution.
- Device surfaces must be periodically inspected to detect tampering or substitution by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device.
- An inventory of card-reading devices must be maintained.
- Physical access to the CDE must be controlled using appropriate facility entry controls.
- Video cameras and/or access control mechanisms must be in place to monitor physical access to sensitive areas.
- Access to the CDE must follow a formal request and approval process.
- A visitor management process must be implemented to identify and authorize visitors.

Remote Access

PCI DSS v3.2.1: 8, 12

Purpose

To establish the rules for the protection of the cardholder data environment.

Audience

The PCI Remote Access Policy applies to all individuals who access (Company) cardholder data or the cardholder data environment remotely.

Policy

- Two-factor authentication is required for remote access to the cardholder data environment.
- Copying, moving, and storage of cardholder data onto local hard drives and removable electronic media is prohibited.
- Remote working must follow defined (Company) remote working requirements, including, but not limited to:
    - All PCI-related activity must be conducted in a separate environment that is locked when not used,
    - All PCI-related activity must be performed on (Company) provided equipment,
    - All (Company) provided equipment may only be used for work purposes,
    - Call recording must follow the company approved method for recording calls that may include cardholder data.
- Automatic disconnect of sessions for remote access after a period defined by IT must be implemented.

Software Development

PCI DSS v3.2.1: 6

Purpose

To establish the rules for the configuration, maintenance and protection of the cardholder data environments.

Audience

The PCI Software Development Policy applies to all individuals involved in software development.

Policy

- Internal and external software applications must be developed securely.
- Development, test and/or custom applications accounts, user IDs and passwords must be removed before applications become active or are released to customers.
- Custom code must be reviewed prior to release to production or customers in order to identify any potential coding vulnerabilities.
- Developers must be trained in secure coding techniques.
- Application development must be based on secure coding guidelines.
- *For public facing web applications*: New threats and vulnerabilities must be addressed on an ongoing basis.
- *For public facing web applications:* Applications must be protected by either:
    - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools/methods at least annually and after any changes; or
    - Installing an automated technical solution that detects and prevents web-based attacks in front of public-facing web applications to continually check all traffic.

Training

PCI DSS v3.2.1: 9, 12

Purpose

To establish the rules for the protection of the cardholder data environment.

Audience

The PCI Training Policy applies to all individuals who access (Company) cardholder data or the cardholder data environment.

Policy

- All (Company) employees who in contact with or could affect the security of cardholder data as part of their job duties must complete an annual training program related to cardholder data security.

Vendor Management

PCI DSS v3.2.1: 12

Purpose

To establish the rules for the set up and management of vendors to (Company) cardholder data environments.

Audience

The Vendor PCI Policy applies to all individuals who manage or administer access to vendors to the (Company) cardholder data environments (CDE).

Policy

- A vendor risk assessment must be performed on all vendors accessing the CDE.
- A list of all vendors must be maintained and account for information about which PCI DSS requirements are managed by each service provider, and which are managed by (Company).
- Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.
- Vendors with PCI DSS compliance requirements must have their compliance status reviewed on an annual basis.
- Vendor access must be enabled only during the time period needed and disabled when not in use.
- Vendor access must be monitored when in use.
- Vendors must acknowledge in writing that they are responsible for the security of the cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of (Company)'s CDE.

Vulnerability Management

PCI DSS v3.2.1: 6, 11

Purpose

To establish the rules for the configuration, maintenance and protection of the cardholder data environments.

Audience

The Vulnerability Management Policy applies to all individuals who administer the (Company) cardholder data environments (CDE).

Policy

Patching

- System scanning must be conducted to identify security vulnerabilities using an authorized third party. Vulnerabilities must be categorized based on severity.
- All applicable vendor-supplied patches must be installed according to risk. Critical patches must be installed within 30 days of release.
- All system component changes must follow a change control process.

Vulnerability Scanning and Penetration Testing

- Internal and external vulnerability scans must be run at least quarterly or upon significant changes to the network.
- Rescans must be conducted until all vulnerabilities identified in the first scan of the quarter are resolved.
- External vulnerability scans must be conducted by an ASV.
- Internal and external penetration testing must be performed at least annually based on an industry-accepted penetration methodology for the entire CDE perimeter and critical systems.
- Intrusion-detection and/or intrusion-prevention must be used to detect and/or prevent intrusions into the network. Alerts generated must be reviewed and addressed.

Definitions

CDE: Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

Waivers

Waivers from certain policy provisions may be sought following the (Company) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Author	Reason/Comments
1.0.0	July 2023		Olumuyiwa Agunbiade	Document Origination

Appendix

The following is a list of items not addressed as part of the stand-alone PCI policy that must exist as part of the overall Information Security Program for PCI DSS compliance:

- Information Security Policy
    - Reviewed at least annually
    - Ensure security policies/procedures clearly define information security responsibilities for all personnel.
- Risk assessment process
    - Performed annually;
    - Identifies critical assets, threats, and vulnerabilities; and
    - Results in a formal, documented analysis of risk
- Usage policies for critical technologies and proper use (i.e. wireless technology, remote access, email and internet usage), which ensure:
    - Explicit approval by authorized parties,
    - Authentication for use of the technology,
    - A list of all such devices and personnel with access,
    - A method to accurately and readily determine owner, contact information, and purpose,
    - Acceptable uses of technology,
    - Acceptable network locations for the technologies,
    - List of company-approved products,
    - Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity,
    - Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use,
    - For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.
- Assign to an individual or team the following information security management responsibilities:
    - Establish, document, and distribute security policies and procedures.
    - Monitor and analyze security alerts and information and distribute to appropriate personnel.
    - Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
    - Administer user accounts, including additions, deletion, and modifications.
    - Monitor and control all access to data.
- Screen potential personnel prior to hire.
- Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:
    - Maintain a list of service providers.
    - Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data they interact with on behalf of the customer.
    - Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
    - Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
    - Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

- *For service providers:* Acknowledge in writing to customers that they are responsible for the security of the cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
- *For service providers:* If segmentation is used, perform penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. controls at least every six months and after any changes to segmentation controls/methods.

Question & Answer?