PENNSYLVANIA PSHA
SPEECH-LANGUAGE-HEARING ASSOCIATION

110 MORAINE
POINTE PLAZA #1028
BUTLER, PA 16001
WWW.PSHA.ORG

Adopted 2/15/2026

Payment Card Industry (PCI DSS) Compliance Policy

1. Scope & Applicability

This policy applies to all systems, personnel, contractors, third-party service providers, and environments that store, process, transmit, or otherwise access cardholder data in connection with payments made to [Organization Name].

[Organization Name] maintains compliance with the Payment Card Industry Data Security Standard (PCI DSS), including all current and applicable requirements, security objectives, and validation procedures.

---

2. Protection of Cardholder Data

2.1 Data Storage

- Cardholder data will only be stored when strictly necessary for business or legal purposes.
- Sensitive authentication data (e.g., CVV, full track data, PINs, PIN blocks) will never be stored after authorization.
- Stored cardholder data will be rendered unreadable using strong cryptography (e.g., AES-256 or equivalent).

2.2 Data Transmission

- Cardholder data transmitted over open or public networks will be encrypted using strong cryptographic protocols (TLS 1.2+ or successor standards).
- Insecure protocols (e.g., SSL, early TLS, FTP) are prohibited.

---

3. Secure Network & Systems

3.1 Firewalls & Network Controls

- Firewalls and network security controls will be implemented to protect the cardholder data environment (CDE).
- Inbound and outbound traffic will be restricted to only what is necessary.
- Network segmentation will be implemented where feasible to reduce PCI scope.

3.2 Secure Configuration

- Vendor-supplied default passwords and security parameters will be changed before systems are deployed.
- Secure configuration standards will be maintained for all in-scope systems.

PENNSYLVANIA PSHA SPEECH-LANGUAGE-HEARING ASSOCIATION

4. Vulnerability Management

4.1 Anti-Malware

- Anti-malware solutions will be deployed, actively maintained, and monitored on all applicable systems.

4.2 Secure Development

- Secure coding practices will be implemented in accordance with industry best practices.
- Public-facing applications will be protected against common vulnerabilities (e.g., OWASP Top 10).
- Custom code will undergo security review prior to deployment.

4.3 Patch Management

- Critical security patches will be applied in a timely manner.
- Vulnerability scans will be conducted as required by PCI DSS.

---

5. Access Control

5.1 Least Privilege

- Access to cardholder data will be restricted to individuals whose job requires it.
- Role-based access control will be enforced.

PENNSYLVANIA PSHA SPEECH-LANGUAGE-HEARING ASSOCIATION

5.2 Authentication

- Unique IDs will be assigned to each user with system access.
- Multi-factor authentication (MFA) will be required for administrative access and remote access to the CDE.
- Strong password policies will be enforced.

5.3 Physical Security

- Physical access to systems storing cardholder data will be restricted and monitored.
- Visitor logs and badge controls will be maintained where applicable.

PENNSYLVANIA PSHA SPEECH-LANGUAGE-HEARING ASSOCIATION

---

6. Monitoring & Logging

6.1 Audit Logs

- System activity will be logged and monitored.
- Logs will capture user access, administrative actions, and access to cardholder data.
- Logs will be retained per PCI DSS requirements.

6.2 Security Monitoring

- Intrusion detection and/or prevention mechanisms will be implemented.
- Log review and anomaly detection processes will be documented and maintained.

7. Testing & Risk Management

7.1 Vulnerability Scanning

- Internal and external vulnerability scans will be performed at required intervals.
- Approved scanning vendors (ASVs) will be used when applicable.

7.2 Penetration Testing

- Penetration testing will be conducted at least annually and after significant infrastructure changes.

7.3 Risk Assessments

- Regular risk assessments will be conducted to identify and mitigate emerging threats.

---

8. Security Policies & Governance

8.1 Information Security Policy

- A formal information security policy addressing PCI DSS requirements will be maintained and reviewed annually.

8.2 Incident Response

- A documented incident response plan will be maintained.

- In the event of a suspected or confirmed breach involving payment data, [Organization Name] will:
  - Immediately contain the incident
  - Notify affected payment brands and acquiring banks as required
  - Engage qualified forensic investigators if necessary
  - Comply with all legal and contractual reporting obligations

8.3 Third-Party Service Providers

- Service providers that store, process, or transmit cardholder data on behalf of [Organization Name] must maintain PCI DSS compliance.
- Written agreements will require acknowledgment of responsibility for securing cardholder data.
- Compliance validation documentation may be requested annually.

---

9. Data Retention & Disposal

Account data is retained only as long as necessary to meet legal, regulatory, and legitimate business requirements.

PENNSYLVANIA PSHA SPEECH-LANGUAGE-HEARING ASSOCIATION

Data Type	**Retention Period**	**Business Justification**
Tokenized transaction records	7 years	IRS nonprofit audit requirements
Last four digits of PAN	7 years	Financial reconciliation and chargebacks
Refund documentation	7 years	Accounting documentation
Sensitive Authentication Data	Not retained	PCI DSS prohibition

PCI DSS – Account Data Retention & Disposal Program

PSHA minimizes the storage of account data and prohibits retention of sensitive authentication data in accordance with PCI DSS standards.

PSHA:

- Utilizes PCI-compliant third-party payment processors
- Does not store full PAN
- Does not store CVV, PIN, or track data
- Retains only tokenized or truncated payment data necessary for accounting
- Maintains a documented inventory of account data locations
- Defines specific retention timeframes with business justification
- Securely deletes data once retention periods expire
- Conducts documented quarterly verification reviews

Oversight responsibility is assigned to the Executive Director or designated compliance officer.

Documentation of quarterly reviews is maintained for audit and PCI validation purposes.

10. Compliance Validation

[Organization Name] will:

- Determine and maintain its appropriate PCI DSS compliance level.
- Complete the Quarterly PCI Review Checklist
- Maintain documentation of compliance and make it available to acquiring banks or payment brands upon request.

PENNSYLVANIA PSHA SPEECH-LANGUAGE-HEARING ASSOCIATION

---

11. User/Staff Responsibilities

By using our payment systems, users agree:

- Not to attempt to circumvent security controls.
- Not to introduce malicious code into our systems.
- To comply with all applicable payment security standards.

Payment Handling Rules for PSHA Staff and Board

1. Never request full card numbers by email.
2. Never write down CVV codes.
3. Never store card numbers in spreadsheets or documents.
4. If card data is received by email accidentally:
    - Do not forward it
    - Delete immediately

    ○ Notify the Executive Director

5. Use only approved payment systems and POS devices.
6. Do not photograph payment cards.
7. Do not store card data on desktops or shared drives.

All payment processing must occur through PSHA’s approved PCI-compliant payment processor.

Failure to comply may result in disciplinary action.

---

12. Enforcement

Failure to comply with this policy may result in:

- Suspension of access
- Termination of contracts
- Legal action where appropriate

PENNSYLVANIA PSHA SPEECH-LANGUAGE-HEARING ASSOCIATION