PCI Compliance Policy for ASHRAE Houston Chapter

Forward

PCI DSS (Payment Card Industry Data Security Standard) compliance is essential for any organization that handles, processes, or stores payment card data. For the ASHRAE Houston Chapter, compliance ensures that the chapter secures member payments and protects sensitive information. Below is a PCI compliance guideline tailored for the ASHRAE Houston Chapter:

Purpose

To ensure the secure handling of payment card information and compliance with the Payment Card Industry Data Security Standard (PCI DSS) in all transactions conducted by the ASHRAE Houston Chapter.

Scope

This policy applies to all ASHRAE Houston Chapter personnel, volunteers, systems, and processes involved in handling payment card transactions, including online payments, event registrations, and membership renewals.

Key Compliance Requirements

1. Build and Maintain a Secure Network

- **Firewall Configuration**: Implement and maintain firewall configurations to protect cardholder data. Ensure firewalls are regularly updated and monitored.
- **Secure Systems and Applications**: Use only secure, PCI-compliant payment gateways for processing transactions (e.g., Stripe, PayPal). Avoid storing cardholder data locally.

2. Protect Cardholder Data

- **Encryption**: Ensure that cardholder data transmitted over open, public networks is encrypted using strong encryption protocols (e.g., TLS 1.2 or higher).
- **Storage Restrictions**: Do not store sensitive authentication data (e.g., CVV) after authorization.

3. Maintain a Vulnerability Management Program

- **Anti-Virus Software**: Use up-to-date anti-virus and anti-malware software on all devices used for payment processing.
- **Regular Updates**: Keep all software, including operating systems and payment processing tools, updated to protect against vulnerabilities.

4. Implement Strong Access Control Measures

- **Access Limitation**: Restrict access to payment card data to only those individuals who need it for business purposes.
- **Unique User IDs**: Assign unique IDs to each individual with computer access to ensure accountability.

5. Regularly Monitor and Test Networks

- **Logging and Monitoring**: Enable and maintain logs for all systems that process payment card data. Retain logs for a minimum of one year.
- **Vulnerability Scans**: Conduct quarterly scans and annual penetration tests to identify potential vulnerabilities.

6. Maintain an Information Security Policy

- **Policy Documentation**: Document and communicate an information security policy to all personnel and volunteers handling cardholder data.
- **Regular Training**: Provide annual PCI compliance training to all staff and volunteers.

Roles and Responsibilities

Chapter Officers and Volunteers

- Ensure all transactions are processed through PCI-compliant payment gateways.
- Report any suspected data breaches immediately to the designated compliance officer.

Designated PCI Compliance Officer

- Oversee PCI compliance efforts and ensure the implementation of all required controls.
- Coordinate annual PCI DSS assessments and remediation efforts.

Incident Response Plan

In case of a data breach or suspected security incident:

1. Immediately isolate affected systems.

2. Notify the PCI Compliance Officer.

3. Conduct an internal investigation and report findings to payment processors and affected individuals as required.

4. Work with third-party forensic experts if needed.

Review and Updates

This policy will be reviewed annually or after significant changes in payment processing systems to ensure ongoing compliance with PCI DSS requirements.

Approved by:

Julie Thomet

ASHRAE Houston Chapter President

Effective Date: 12/10/2024

This policy is a foundational document. You should work with a certified PCI DSS consultant or your payment processor to ensure that all specific requirements are met for your chapter's operations.