Katch-Up Media LLC Information Security Policy

Version: 1.0
Effective Date: 02/14/2025
Last Updated: 02/14/2025
Approved By: Modelle McRae, CEO

1. Introduction

Katch-Up Media LLC is committed to maintaining the security and integrity of payment card data by adhering to the Payment Card Industry Data Security Standard (PCI DSS). This policy establishes security requirements to protect cardholder data (CHD) and personally identifiable information (PII) while working with third-party vendors: Talech, SureCart, and Stripe.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and systems that handle, process, store, or transmit cardholder data. It covers all aspects of data security, including physical, network, and application security controls.

3. PCI DSS Compliance Requirements

Katch-Up Media LLC adheres to the following PCI DSS requirements:

3.1 Build and Maintain a Secure Network

- Implement firewall configurations to protect CHD.
- Change default passwords and settings before deploying systems.

3.2 Protect Cardholder Data

- Encrypt transmission of CHD across open, public networks using TLS 1.2 or higher.
- Store CHD only when necessary and encrypt sensitive data at rest using AES-256 encryption.

3.3 Maintain a Vulnerability Management Program

- Install and maintain updated antivirus software.
- Regularly update and patch systems to address security vulnerabilities.

3.4 Implement Strong Access Control Measures

- Limit access to CHD to authorized personnel only.
- Require multi-factor authentication (MFA) for access to sensitive systems.

3.5 Regularly Monitor and Test Networks

- Implement logging mechanisms and regularly review access logs.
- Conduct quarterly vulnerability scans and annual penetration testing.

3.6 Maintain an Information Security Policy

- Conduct employee training on security policies and PCI DSS requirements.
- Perform regular risk assessments and policy reviews.

4. Third-Party Vendor Security Compliance

Katch-Up Media LLC partners with the following third-party vendors for payment processing and e-commerce transactions:

4.1 Talech

- Provides point-of-sale (POS) solutions.
- Ensures PCI DSS compliance for payment processing systems.
- Encrypts all payment transactions to protect cardholder data.

4.2 SureCart

- Handles e-commerce transactions.
- Uses tokenization to secure CHD and prevent unauthorized access.
- Maintains PCI DSS compliance for all transaction processing.

4.3 Stripe

- Processes online payments.
- Uses end-to-end encryption and tokenization to protect CHD.
- Complies with PCI DSS Level 1 certification requirements.

5. Incident Response Plan

In case of a data breach or security incident:

1. Identify and contain the breach.
2. Notify affected parties and regulatory bodies as required.
3. Conduct a forensic investigation to determine the root cause.
4. Implement corrective actions and update security controls.
5. Review and update the incident response plan accordingly.

6. Employee Responsibilities

- Adhere to security policies and procedures.
- Report any suspected security incidents immediately.
- Use secure passwords and protect login credentials.

7. Enforcement and Compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination. Regular audits and assessments will be conducted to ensure adherence to PCI DSS standards.

8. Review and Updates

This policy will be reviewed annually or when significant changes to systems, business processes, or compliance requirements occur.

For any questions or concerns regarding this policy, contact: hello@katch-up.com.