Attestation of Compliance (AOC)

Date: 6-17-2025

Prepared by: Michael Jordan

For Service Providers Who Are PCI DSS Compliant

Part 1: Contact Information

- *Organization Name*: **SecureTech Solutions**
- *Assessor Name*: **Michael Jordan**
- *Assessment Date*: **6-17-2025**
- *Lead Contact Name*: **Mark Taylor**
- *Job Title*: **GRC Team Lead**
- *Contact Phone/Email*: **Mark.Taylor@securetech.com | (858) 457-0967**

Part 2: PCI DSS Assessment Information

Assessment Type (On-Site/Self-Assessment): On-Site

Scope of Systems and Networks Assessed: Cardholder Data Environment, Network Infrastructure, Admin Access Points, Security Monitoring Systems, Encryption Key Management Systems, User Access Control Systems

Assessment Date(s): 6/17/2025

Part 3: PCI DSS Validation

For each requirement, choose one status: In Place / Place with Compensating Controls / Not Applicable / Not Fully Compliant

1. Build and Maintain a Secure Network: In Place

- *Finding:* SecureTech's firewall and network segmentation effectively isolate the CDE from other corporate networks. The configuration limits both inbound and outbound traffic to approved sources, minimizing the attack surface.
- *Recommendation:* Although the configuration meets PCI DSS standards, it is recommended that legacy firewall rules be reviewed every quarter to identify and remove outdated rules that could introduce vulnerabilities.

2. Protect Cardholder Data: In Place with Compensating Controls

- *Finding:* Encryption standards for cardholder data at rest and in transit use AES-256, meeting PCI DSS requirements. However, key rotation has been delayed beyond the recommended 12-month period due to operational constraints.
- *Compensating Control:* SecureTech has implemented an interim measure where access to encrypted data is monitored closely until key rotation is completed next month.
- *Recommendation:* Develop a documented key rotation schedule and ensure encryption keys are rotated annually, with regular audits to verify adherence to this schedule.

3. Maintain a Vulnerability Management Program: In Place

- *Finding:* SecureTech conducts quarterly vulnerability scans and remediates critical vulnerabilities within 30 days. However, remediation for medium-risk vulnerabilities has sometimes been delayed.
- *Recommendation:* Allocate additional resources for the timely remediation of medium-risk vulnerabilities to further minimize exposure, particularly for systems with access to sensitive data.

4. Implement Strong Access Control Measures: Not Fully Compliant

- *Finding:* MFA is enabled for most critical systems; however, administrators still use shared accounts for remote access, which compromises accountability.
- *Remediation Plan:* Transition to unique user IDs for all administrators, and enforce MFA across all high-risk systems to comply with PCI DSS standards.
- *Timeline:* Complete transition to unique IDs by Q2 2024 and finalize MFA enforcement for all critical access points by Q3 2025.

5. Regularly Test Security Systems and Processes: In Place

- *Finding:* The organization conducts monthly intrusion detection systems (IDS) testing within the CDE, with logs sent to the SIEM for monitoring.
- *Recommendation:* To strengthen security posture, conduct advanced testing methods like penetration testing and red teaming exercises annually.

6. Maintain an Information Security Policy: In Place

- *Finding:* SecureTech's information security policy is up-to-date with PCI DSS standards. Employees undergo annual training, achieving a 98% completion rate.
- *Recommendation:* Consider implementing refresher sessions every six months, especially for high-risk areas like phishing awareness.

Part 4: Action Plan for Non-Compliant Requirements

For any requirements that are not fully compliant, provide details of the remediation plan and timelines:

Requirement: Implement Strong Access Control Measures

- *Remediation Plan:* Enforce unique user IDs for all administrative users to ensure accountability. Strengthen MFA requirements by expanding them to cover all remote access points and critical functions.
- *Timeline:* MFA implementation and unique ID transition are ongoing and targeted for completion by Q3 2025. A status report will be submitted by the end of Q4 2025

Requirement: Protect Cardholder Data

- Remediation Plan: An interim plan has been implemented involving continuous access monitoring until key rotation is completed. SecureTech has scheduled the rotation for next month and will conduct a follow-up audit in January 2026 to verify control effectiveness.
- Timeline: key rotation next month. Next January, audit the controls.

Part 5: Attestation and Sign-Off

By signing below, you attest that the information provided in this AOC is accurate and reflects the current state of PCI DSS compliance for the organization.

Signature: Michael Jordan
Printed Name: Michael Jordan
Job Title: GRC Intern
Date: 6-17-2025