Prepared by: Michael Jordan
Date: 6-23-2025

PCI DSS Compliance Audit Report

Summary

This PCI DSS compliance audit of SecureTech focused on critical domains: access controls, data protection, network security, and incident response. While several strong security controls are in place, notable deficiencies were found in key areas, including encryption key management, access monitoring, and incident response readiness. Remediation of these issues is essential to minimize risk and achieve full PCI DSS compliance.

Audit Findings and Recommendations

Access Controls

Findings:

- Administrative access is granted through shared accounts, which compromises accountability and violates PCI DSS standards.
- Multi-factor authentication (MFA) is not currently enforced for privileged accounts, increasing vulnerability to credential-based attacks.
- Access logs are reviewed inconsistently, and no automated system is in place to alert on failed login attempts.

Recommendations:

- Discontinue the use of shared credentials and assign unique user IDs for all administrative users.
- Enforce MFA for all privileged accounts within the next reporting quarter.
- Deploy automated alerts for failed login attempts and establish a routine access log review process on a quarterly basis.

Data Protection

Findings:

- Cardholder data is encrypted at rest using AES-256; however, the encryption keys are stored on the same server as the database, undermining security.

- TLS certificates used for data transmission have expired, potentially exposing sensitive data in transit.
- Full Primary Account Numbers (PANs) are visible in system logs, contrary to PCI DSS masking requirements.

Recommendations:

- Relocate encryption keys to a secure location such as a hardware security module (HSM) or an approved key management system.
- Renew all expired TLS certificates immediately and implement an automated renewal tracking system.
- Reconfigure log settings to mask PANs, showing only the last four digits as required.

Network Security

Findings:

- Firewalls effectively segment the Cardholder Data Environment (CDE) from the rest of the network.
- Some firewall rules are outdated, allowing access from untrusted IP ranges.
- Current antivirus solutions do not utilize behavior-based detection, limiting their ability to identify advanced threats.

Recommendations:

- Conduct quarterly firewall rule reviews to remove outdated or risky access permissions.
- Enhance existing antivirus solutions with an Endpoint Detection and Response (EDR) system for improved threat detection.
- Adjust Intrusion Detection System (IDS) alert thresholds to include medium-severity events for proactive monitoring.

Incident Response

Findings:

- The incident response plan lacks clearly defined roles and responsibilities for escalation and containment.
- Breach notification timelines are ambiguous, particularly regarding the start of the 72-hour reporting period.
- No incident response drills or tabletop exercises have been performed in the past 18 months.

Recommendations:

- Define specific roles within the incident response team, covering containment, investigation, and regulatory reporting.
- Clearly state that the 72-hour notification window begins upon breach detection.
- Schedule and execute tabletop exercises at least twice a year to validate and improve the incident response process.

Key Observations

SecureTech demonstrates strong capabilities in network segmentation; however, outdated firewall configurations and insufficient monitoring reduce the effectiveness of those protections. Encryption methods are fundamentally sound but must be supported by improved key management and data masking to meet PCI DSS requirements.
The current incident response strategy requires immediate enhancement, including defined responsibilities and regular testing, to ensure organizational readiness.

Recommendations Summary

- Require MFA and unique credentials for all privileged users.
- Store encryption keys securely and independently from the data they protect.
- Perform routine firewall audits to remove obsolete or risky rules.
- Conduct biannual incident response drills to strengthen response capability.

Conclusion

SecureTech is on a solid path toward PCI DSS compliance but must address key gaps to ensure robust data protection and regulatory alignment. Implementing the recommendations in this report will significantly bolster SecureTech’s security posture and readiness for future audits or incidents.

Reflection

This audit highlighted the critical need for continuous assessment and refinement of compliance efforts. Identified gaps in encryption, access controls, and incident response procedures underscore the value of proactive security management. The process reinforced the interdependence of technical defenses, governance policies, and operational discipline in maintaining compliance and protecting sensitive data.