Sahl | سهل

PCI DSS

□ Build and Maintain a Secure Network and Systems

Firewall

- Is a firewall in place to protect cardholder data?

Default Configurations

- Have vendor-supplied defaults for systems and software been changed?

□ Protect Cardholder Data

Encryption

- Is cardholder data encrypted both at rest and in transit?

Data Minimization

- Is the scope of cardholder data collection and storage minimized?

□ Maintain a Vulnerability Management Program

Vulnerability Scanning

- Are regular vulnerability scans conducted to identify and address security weaknesses?

Anti-malware Software

- Is up-to-date anti-malware software installed and maintained?

Sahl | سهل

PCI DSS

□ Maintain an Information Security Policy

Security Policies

- Does the organization have a written information security policy that addresses PCI DSS requirements?

□ Implement Strong Access Control Measures

Unique User IDs

- Do all users have unique IDs and strong passwords?

Access Control

- Is access to cardholder data restricted based on business need?

□ Regularly Monitor and Test Networks

Network Monitoring

- Are network activities monitored for suspicious behavior?

Penetration Testing

- Are regular penetration tests conducted to identify vulnerabilities?

Ready to take the next step?

Contact Sahl to schedule a free consultation.

Book a Demo