business resource center

Best Practices for Securing Payment Card Information Checklist

We are committed to assisting you in managing your business's loss exposures. All merchants accepting payment cards are required to comply with Payment Card Industry Data Security Standards (PCI DSS). Are you in compliance? Use our checklist below.

- ☐ Build and maintain a secure network including installation and maintenance of firewalls, antivirus, endpoint detection and response, and encryption
- ☐ Use strong cryptography and security protocols such as SSL/TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open public networks
- ☐ Install personal firewall software and endpoint detection and response on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network
- ☐ Maintain and disseminate a policy that addresses information security for all personnel
- ☐ Avoid storage of cardholder data if possible; if stored, limit retention time to that required by business, legal and/or regulatory purposes
- ☐ Implement strong access controls including limiting access to those whose job requires such access, strong passwords and secure storage areas
- ☐ Assign a unique username to each person with computer access
- ☐ Employ two factor authentications for remote access to the network by employees, administrators and third parties
- ☐ Render all passwords unreadable during storage and transmission by using strong cryptography
- ☐ Monitor and test your network, security systems and processes regularly
- ☐ Verify third party service providers are PCI DSS compliant when outsourcing any part of your IT infrastructure
- ☐ Change default passwords for all devices, including POS systems and other internet-facing devices before installing on a network
- ☐ Utilize a checkout or payment page hosted by a PCI DSS compliant service provider to process customer online payment information outside your own business network
- ☐ Implement a tokenization solution when processing payment cards yourself to enable repeat online customers to securely store and access their payment information
- ☐ Never store sensitive authentication data after authorization when processing payment cards; this includes sensitive data that is printed on a card or stored on a card's magnetic stripe or chip, and personal identification numbers entered by the cardholder
- ☐ Contractually commit third party vendors to compliance with PCI requirements and include indemnity requirements when a breach happens