PCI Data Security Standards Checklist

The Payment Card Industry (PCI)—composed of Visa, MasterCard, Discover, and AMEX—requires every organization that accepts credit cards to complete an annual PCI compliance renewal questionnaire.

Completing the Self-Assessment Questionnaire (SAQ) involves answering a series of True/False questions regarding how you and your employees handle sensitive payment information. The SAQ ensures your company is adhering to the regulations created by the PCI Security Standards Council.

Before you begin the SAQ, we recommend using this checklist to guarantee your company is following the best practices for data and information security. Once you can check off every item, you'll know without a doubt your company is keeping sensitive data safe and completing the SAQ will be a breeze.

- ❏ Any paper document containing cardholder data is physically secured in a locked filing cabinet or safe.
- ❏ No document that contains cardholder information also includes the CID/CVV2 card security code.
- ❏ Any document that contains cardholder information is considered confidential and is accessible only by employees with a specific business need.
- ❏ No document that contains cardholder information is moved from its secure location without prior approval from management.
- ❏ When no longer needed for business or legal reasons, any paper document that contains cardholder information is securely destroyed via cross-cut shredding or burning to prevent reconstruction.
- ❏ Accessing CPACharge requires an employee to use a personal unique ID, which they are forbidden to share with anyone else.
- ❏ The account ID and password an employee uses to access cardholder data are not used to log in to any other software.
- ❏ Shared and/or group accounts are not used for any system administration activities or to access sensitive information.

- ❏ User passwords for computers and software on the network follow security best practices, including a length of at least 7 characters and a combination of both numbers and letters.

- ❏ No account for any software on any device with access to the network uses the vendor-supplied default password.

- ❏ Upon termination, an employee's access to any sensitive information is immediately disabled and all user permissions are revoked.

- ❏ Comprehensive policies and procedures regarding employee computer use, physical security, and data security are documented and enforced at every level of the organization.

- ❏ Upon hiring, every employee signs an official information security policy. (You can view a sample agreement here.)

- ❏ Employees receive regular training on how to safely handle sensitive information and protect the privacy of customers.

- ❏ An established plan for responding to security threats and cyberattacks is in place.

- ❏ All software, computers, and mobile devices on the network are regularly updated with the latest patches and security updates to protect against known vulnerabilities.