July 18-20, 2019 — Evanston, Illinois

Payment Card Industry Data Security Standard | PCIDSS

Version 3.2 updated December 2018

Synopsis

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed in 2006 by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The objective was to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council enhances the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks. The latest standard v3.1, will requires the latest version of point-to point encryption (P2PE).

MDP Alliance Notes:

This document is intended simply as an outline to create awareness. Visit https://www.pcisecuritystandards.org for more information.

Our events use various payment processors, payment gateways, and point-of-sale devices (bank provided terminals, PayPal Here, Square). The emphasis for us is to be certain that these devices support the latest EMV chip technology.

Most, if not all, of our events are Self-Assessment Questionnaire (SAQ) Validation Type A, B, or C participants (merchants) with our credit card transaction processing. Please verify the questionnaire your event might use based on the requirements available.

Non-compliance will lead to an additional monthly fees by your credit card processing vendor and potential, per-transaction penalty fees. This monthly penalty remains true even with no activity on your account (dormant months).

EMV Chips

The latest introduction (in USA) of security measures regards the EMV Chip on all payment cards. EMV is an acronym for Europay, MasterCard, and VISA. The impact to our events is onsite where we are using various types of devices for point of sale terminals. Visit www.emvco.com for more information.

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Protect stored data Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software or programs Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know Assign a unique ID to each person with computer access Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel

All information excerpted from the https://www.pcisecuritystandards.org website.
To further the adoption of the PCI DSS, the PCI Security Standards Council defines credentials and qualifications for QSAs and ASVs. The PCI Security Standards Council also manages a global training and certification program for QSAs and ASVs, and will publish a directory of certified providers on this Web site.