WHAT IS PCI DSS?

The PCI DSS version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted 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 DSS January 2005 version has been enhanced in the PCI DSS Version 1.1. The PCI DSS January 2005 version may no longer be used for PCI DSS compliance validation after December 31, 2006.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

**Build and Maintain a Secure Network**

*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data  
*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

*Requirement 3:* Protect stored cardholder data  
*Requirement 4:* Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**

*Requirement 5:* Use and regularly update anti-virus software  
*Requirement 6:* Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

*Requirement 7:* Restrict access to cardholder data by business need-to-know  
*Requirement 8:* Assign a unique ID to each person with computer access  
*Requirement 9:* Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

*Requirement 10:* Track and monitor all access to network resources and cardholder data  
*Requirement 11:* Regularly test security systems and processes

**Maintain an Information Security Policy**

*Requirement 12:* Maintain a policy that addresses information security

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.

Copyright © 2008 PCI Security Standards Council, LLC. All rights reserved.