

Payment Card Industry Data Security



Data security is an important component of today's payment processing environments and applications. As a participating member in the PCI Security Standards Council, Blackboard is dedicated to the ongoing development and adoption of the Payment Application Data Security Standard (PA-DSS) and the Payment Card Industry Data Security Standard (PCI-DSS).

PAYMENT CARD DATA SECURITY STANDARDS BACKGROUND

The Payment Card Industry (PCI) Security Standards Council was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. It is an independent body formed to develop security standards for account data protection and has been adopted by the major card associations.

The Council maintains the PCI Data Security Standard (PCI-DSS) while working to promote its industry adoption. PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other protective measures.

PCI DSS compliance involves achieving the data security standards set for two separate but equally important elements of credit card acceptance, the software used for processing of credit cards, and the *environment* in which the software application is hosted.

Blackboard has responsibility for delivering *software* compliance, that is, an application that meets the Payment Application Data Security Standard (PA-DSS).

Clients have the responsibility for achieving environmental compliance, that is, for hosting the application in a PCI Compliant (PCI-DSS) manner.

Transaction processing systems are considered PCI Compliant if the **software applications** in use meet the requirements of the PA-DSS and the overall **hosting environment** adheres to the standards set forth in the PCI DSS, as validated by an independent third party assessor, or self-validated if directed by the client's merchant acquirer.

PA-DSS is a PCI Security Standards Council - managed program, with the goal of helping software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. The requirements for PA-DSS are derived directly from the PCI DSS, but specific to the development of applications that capture, transmit, and/or store cardholder data.



Blackboard

PCI DATA SECURITY STANDARD REQUIREMENTS

At 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

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

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

A more detailed summary of PCI DSS requirements can be found at www.pcisecuritystandards.org.

BLACKBOARD'S STATUS

Blackboard recognizes the importance of developing payment applications which adhere to PA-DSS, and subsequently enabling clients to deploy our Blackboard technologies in a PCI DSS compliant environment.

Blackboard is steadfast and focused in its commitment to PA-DSS compliance within our applications. To that end, Blackboard is pleased with its progress to date and well into development to ensure PA-DSS compliance in accordance with Visa's phased-in mandates.

The Blackboard Payment Gateway, the payment solution used for online deposits and e-commerce purchases, as well as point of sale IP credit card transactions, adheres to PCI DSS standards and has been independently validated as PCI DSS compliant for four consecutive years, most recently in May 2008. Blackboard is considered a level one service provider by the PCI Security Standards Council and major card associations.

The Blackboard Payment Gateway is certified by TrustWave's TrustKeeper Compliance Validation Service, which has been accredited by the major card associations' data security programs. In order to remain in compliance, the Blackboard Payment Gateway must pass monthly and quarterly evaluations as well as an annual on-site review by the TrustWave.

The Blackboard Community System can currently be operated within a PCI compliant environment, which can be validated against the PCI DSS Self Assessment Questionnaire - Version C. The Community System is not PA-DSS validated; however, this does not prevent an institution from maintaining a PCI DSS compliant environment.

Blackboard is also taking steps to evaluate its software for PA-DSS compliance. As part of ongoing development efforts, Blackboard intends to make reasonable enhancements to its designs to follow PA-DSS, which, when accomplished, would allow clients to operate the system in compliance with the PCI DSS.

For more information, clients should contact their Blackboard representatives.

