Blackboard Student Services: A 360° Security Overview

Control and protection of institutional data is a critical component and priority for Blackboard Student Services. Blackboard understands the strict information security and privacy needs of educational institutions, including traditional 4-year institutions, community colleges, and private companies. Blackboard's staff, processes, and policies are designed to protect and maintain the confidentiality of any personal information (also known as "personally identifiable information" or PII) that is provided to Blackboard by its educational partners and their learners.

Blackboard is committed to enabling the success of institutional partners and the success of their students. This commitment requires that we ensure the security and integrity of the information made available to us by our clients. Blackboard will:

- Authentically represent clients during every interaction with an unwavering dedication to upholding their reputation and the integrity of all data
- Maintain rigorous quality control of data
- Ensure continual improvement to effectively provide data security

This document outlines Blackboard's data protection and security controls to protect the confidentiality of an institution's data and to help protect an institution's reputation. Specifically, this document provides an overview of key safeguards applied to Blackboard's telecommunication system, network, servers, facilities, and applications.

Data Security

Blackboard maintains a PCI Level 1 certification for components of Blackboard Student Services. This certification requires that Blackboard adhere to stringent security policies, processes, and standards. Across all components of Blackboard Student Services, Blackboard implements measures to protect data confidentiality, integrity and availability.

Network Security

Blackboard employs perimeter security controls, such as firewall solutions, to insulate Blackboard's internal network from external access. Blackboard conducts routine port scans to validate hardening standards and re-validates all configurations and rules every six months.

Blackboard's data warehouse is accessible only to its internal network. Its technology infrastructure ensures that only authorized and required personnel have direct access to the data warehouse.

Physical Security

Blackboard's critical systems and applications are hosted in three different data centers across the U.S. Blackboard implements restrictive measures to limit physical access to its data centers, to include the use of secure ID card swipes for contact center access, biometric access panels to enter its server rooms, and unique login authentications for specific personnel.

Personnel Security

All staff, regardless of access level, must pass a thorough background check and sign confidentiality agreements prior to engaging with students.

Security Monitoring and Incident Response

A third-party, managed Security Organization Controls (SOC) provider monitors Blackboard systems for suspicious activities. As potential incidents are identified, they are immediately escalated to the dedicated Blackboard Security Team, led by Blackboard's Chief Information Security Officer. The Blackboard Security Incident Response plan documents the process followed in the event of a Security Incident.

Vulnerability Management

Blackboard routinely scans for vulnerabilities and coordinates remediation strategies. Additionally, Blackboard evaluated software security updates for applicability and impact and promptly applies relevant updates as appropriate.   a quarterly basis. As part of annual PCI audits, components of Blackboard Student Services undergo penetration testing.

Types of Data Stored

Only basic caller information necessary to identify and verify the caller is stored in Blackboard's local systems. For more sensitive data, Blackboard performs a real-time lookup through data integrations, thus eliminating the need to store all sensitive data locally.

Data Encryption Policy

Data including user upload files, procedure documents, and KB or data export files are transferred through Secure File Transport Protocol (SFTP) and can be encrypted per a client's specifications.

To ensure privacy between communication systems, all data is transmitted over Transport Layer Security (TLS), including all web traffic to/from Blackboard web applications. All data that Blackboard retrieves from a school's SIS or, if applicable, back-office systems are encrypted for an additional layer of security before being transmitted over TLS.

Software Integration Security

Blackboard's propriety technology service offering, Blackboard SmartView™, powers its student services technology platform. SmartView does not require direct access to an institution's data system by a Blackboard advisor, which provides increased data privacy and security. Data that is required for service is retrieved in real time through system integration. When data is used, each individual data request through integration is logged for traceability.

In the U.S., Blackboard accesses, collects and processes student data as an outsourced institutional function pursuant to FERPA. Blackboard's technology supports the security of data at the network transport level where site-to-site VPN tunnels are used to secure data in transit. In addition, in the user interface design, 256-bit SSL certificates for encryption of Web interfaces are used.

Quality Assurance

Blackboard's reputation is dependent on the quality of service that it delivers to its customers. To best assure quality, Blackboard:

- Employs a team of quality analysts to proactively review interactions and provide trend analysis.
- Partners with a third party to audit its internal quality for ongoing process improvement.
- Reviews and analyzes survey results proactively, and compares the results to its internal metrics.
- Conducts on-demand call reviews, internal call monitoring, and client calibration sessions.

Business Continuity and Data Safety

Redundancy

Blackboard's critical systems and applications are hosted in three different data centers across the U.S. Each data center has multiple inbound and outbound network connections. To provide redundancy and failover, all three data centers are connected with multiple high-speed MPLS circuits.

Each critical system or application has a primary installation with redundant servers or load balancers in one data center, and a mirror or failover installation in another data center. Each system or application is capable of failover automatically to its redundant counterpart.

Backup and Recovery

Data in Blackboard's critical systems, including but not limited to database data and user uploaded file system files, are backed up incrementally on a daily basis and are backed up in full periodically. The backup files are stored in U.S. data centers with different geo-locations.

Blackboard's critical systems are monitored 24/7. Upon receipt of any performance alert from its monitoring systems, Blackboard's Student Services IT team promptly triages to determine the extent of impact. If the issue is service impacting, then an IT advisory is sent to the Operations team to alert the Student Services advisors. Updates to the advisory are sent, at a minimum, every hour until service is fully restored.

Blackboard's systems are architected so that a complete failure of any critical component results in an automated failover to a redundant component. For example, if an inbound dedicated circuit fails in one data center, then phone calls are automatically routed at the carrier level to circuits in another data center, and then passed to Blackboard advisors over the WAN infrastructure.

If a reported services issue is not a complete outage, but a degradation of service, then Blackboard IT will make its best effort to manually port calls to alternative operations centers by manually logging in to the carrier administrative site and redirecting individual toll-free numbers. A degradation of service can include, but is not limited to, the following:

- Poor voice quality in operations centers such as choppy voice, static, one-way audio.
- Periodic fast busy signals of individual client toll free numbers.

After service has been fully restored, a complete post mortem is conducted with the appropriate parties. The post mortem results along with a complete Reason for Outage (RFO) are provided to the Operations team, which communicates the same to all affected clients.