Security

Redacted

Hosting and Maintenance

Hosted by Redacted a SaaS solution designed to automate the administration, collection and reporting of institutional assessment data. With Redacted your school will retain a high degree of customization, while eliminating many of the costly and time-consuming demands of your current processes.

Redacted software, and any associated institutional data collected through the use of the software. Upon contract termination, all course evaluation data will be removed from the Redacted provides all system maintenance and updates during your term of service.

SSAE 16 Compliance

Redacted atacenter, located in Redacted is SSAE 16 SOC-2 Type II compliant. Redacted olocation, located Redacted SSAE 16 SOC-1 Type II compliant. Both facilities have successfully undergone review by independent auditors.

Datacenter Security

Redacted were developed with the help of a customer advisory board comprised of representatives Redacted The board developed a specific datacenter and security protocol based on ISO Payment Card Industry Data Security Standards. The Redacted has since successfully undergone in-depth security audits by two well-known universities, including Redacted . Redacted datacenter, Redacted Redacted

Redacted general premises are secured with steel doors, security cameras and reinforced windows. Points of entry are secured by both a biometric lock and an alarm— Redacted Located within the secure facility, Redacted cinderblock, and has only one point of entry, secured with a second biometric lock that only admits Redacted staff, and an alarm that only admits Redacted staff.

Digital Security

Redacted digital security measures include the performance of port scans twice weekly, which search for web vulnerabilities. Employees are incentivized to discover and report potential vulnerabilities. We also perform external network scans twice yearly, and whenever changes are made to the network. Redacted utilizes a custom “punch back” tool designed to foil potential cyber attackers. Redacted set to high availability.

Redacted proactively monitors website activity for support purposes, sending immediate, automated email warnings to school administrators upon detection of any suspicious activity. Automated monitoring and notifications include:

- Email notices to all system administrators when data is imported.
- Automated warning messages to Redacted staff when an administrator’s password is reset.
- Proactive monitoring of suspect user actions.
- Tracking and reporting malicious student activity to school administrators.

Suspicious activity warnings detected by the software are sent via email to both Redacted Support and to school evaluation administrators. Customer Support staff then investigates the issue, and contacts the school’s Primary Evaluation Administrator (PEA). For more information, please see: Redacted

Backup and Disaster Recovery

[redacted] data is placed on [redacted] and are mirrored SQL servers set to high availability. We log ship our SQL records to our [redacted] colocation every 15 minutes. [redacted] This ensures that no data will be lost in the event of catastrophic damage to the primary server room. In the event of catastrophic failure, our DNS servers will fail over [redacted] colocation automatically within five minutes.

Data Infrastructure

The [redacted] is based on a [redacted] database servers in high safety mode with automatic failover. [redacted] is SSAE 16 SOC-1 Type II compliant, and receives log-shipped database updates every 15 minutes. [redacted] software. The application's function depends on a specified schema-owner with DBA access.

FERPA Compliance

All information provided to [redacted] remains the property of the client institution and may be subject to the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), as amended. Once the contract is terminated, [redacted] will destroy all data collected during the contractual period.

The [redacted] relies on student and course registration data uploaded by the client institution. While [redacted] very few data fields to function effectively, there are many optional fields that can be used to expand data analysis capability. This means that the amount of FERPA-protected or other sensitive data that we store will vary depending on what data the client institution chooses to upload. Regardless of FERPA-protected status, any sensitive data received by [redacted] — it is never re-disclosed to other parties, and all sensitive student data is protected by stringent security policies:

All employees are required to undergo rigorous security training on FERPA disclosure regulations and the treatment of sensitive data. [redacted] employee security training stipulates that:

- No personal information is ever to be given over the phone;
- Employees must construct complex passwords for all hardware and software used, and change them regularly;
- Employees must keep passwords strictly confidential;
- Physical documents containing sensitive information are destroyed immediately; and
- Employees will only discuss sensitive data with school-appointed administrators. No sensitive data is ever released to system users who do not have administrator-level access.

Any violation of these security policies constitutes grounds for dismissal.

Secure User Access Permissions

[redacted] layered permission base to ensure users may access only the content and administrative settings appropriate to their roles. [redacted] four distinct groups of users, each having specific privileges and access to the system:

STUDENTS: Able to view and complete evaluations for only those courses in which they are enrolled. To protect student confidentiality, [redacted] includes customizable settings that will hide evaluation results should too few students complete the survey for a given course. Additional options can allow students to view a summary report of instructor evaluation results.

INSTRUCTORS: Able to view results and response rates for only those classes that they teach. Additional options include granular reporting access controls for team-taught and cross-listed courses, with specific access controls by teacher type (ex. Primary Instructor, Teaching Assistant).

DEPARTMENT HEADS, DEANS, PROVOSTS OR OTHER SUPERVISORIAL FACULTY: Able to view response rates and reports for only the departments, course levels , and course types for which viewing access has been specifically assigned. Access may be assigned by instructor, or by department, course level and course type.

ADMINISTRATORS: Able to access all reports and modify viewing access for all other users.

[redacted] [redacted]