proctorU

Security Q&A

The security of institution, faculty and student data is of the highest importance to us. To expedite the process of coronavirus contingency planning, we've outlined our responses to the two most common questions we receive from institution security experts. While this is by no means all-inclusive of the security measures we take, it does cover some of the more important standards we abide to for data protection.

1) What controls do you have that protect our data?

Data encryption during transmission: All communication between the mobile application and the PerfectServe platform is encrypted using AES 256-bit TLS 1.2.

Data encryption while being stored: All sensitive data, such as PII, is stored using encryption algorithms no weaker than AES 256. Depending on where data is stored, encryption may be whole disk encryption or encryption applied to the entire database. In addition to the whole-disk/database encryption, sensitive data, such as an exam password, is encrypted at the application layer before being written to the database which provides a two-layer encryption scheme. In all cases, ProctorU employs third-party encryption tools.

Audit trail: All activity is fully auditable and includes the following:

- **Unique user IDs:** Access to the ProctorU platform requires authentication with a unique user ID. The user ID verifies the person's identity, controls what features they can access and tracks activity in the audit trail.

- **Least privilege access:** User accounts are created with minimal privileges. Access to functionality and data must be explicitly granted to a user account.

2) What steps do you take to ensure you develop and deliver a secure platform?

OWASP Focus: All of our software engineers code with OWASP Top 10 in mind. All code is internally peer-reviewed and extensively tested in a sandboxed environment using non-production data.

Static Code Analysis: During the development process, all code is statically analyzed by a third-party to minimize security risks.

Third-party Dependency Checks: During the development process, all third-party libraries are checked to ensure no vulnerabilities exist.

Third-party Tested: An annual basis ProctorU has a third-party security company complete a penetration test and vulnerability scan. The last test was performed in August 2019.

Application Level Edge Protection: ProctorU utilizes a web application firewall (WAF) coupled with an intrusion prevention system (IPS) for application & infrastructure security.

Platform Monitoring: Key services within the platform are monitored for health and responsiveness. In many cases, automatic recovery actions are initiated to ensure the availability of the platform.

If you are a current ProctorU partner or decide to partner with ProctorU for online proctoring, additional security details are available upon request.

For more information, please contact us by visiting **proctoru.com/contact-us.**