Cerego

Cerego takes cyber security very seriously. Our team is committed to reaching the highest standards required to protect the sensitive data of today's businesses and educational institutions. We strive to ensure that your data is handled securely and utilize the most advanced technology for Internet security that is available today.

Physical Security & Hosting:
Cerego is entirely hosted within the AWS and GCP clouds. We host our commercial offerings strictly in US regions and our federal and military services in the AWS GovCloud.

Data Encryption:
Cerego requires SSL/TLS encryption to encrypt all traffic between client devices and our servers. Unlike most companies, we do not allow unencrypted traffic to access any part of our system. We value the security of your data, and mandate full disk encryption for all employee workstations and encrypt all traffic in and out of servers during system management and maintenance.

Security Compliance:
Cerego is transitioning to achieve DFARS 252.204-7012 compliance in order to store Controlled Unclassified Information (CUI). We are currently contracting with a FEDRAMP 3PAO consultant and have completed an internal security audit and gap analysis. We have already implemented most of the relevant NIST SP 800-171 controls, as defined in the DFARS regulation, and will achieve full compliance, as outlined in our System Security Plan (SSP) and Plan Of Action And Milestones (POAM).

User Authentication:
Access to Cerego is provided by a combination of a username or email and a password, or through OAuth 2.0 based authentication strategy. We never store your passwords, and all passwords are individually salted and hashed using one of the highest standards for password protection, the Blowfish algorithm. Sessions are maintained using an encrypted cookie utilizing the latest OWASP recommendations for session management.

Permissions and Access scoping:
All permissions to resources within our system are managed by a role based permission system which vets each endpoint and only serves appropriate content to the authenticated account. Multiple tiers of roles allow you to finely control and tailor access to management tasks within your organizational account.

Sensitive Data:
Cerego neither collects nor stores any sensitive data such as government issued ID numbers, credit card or financial information, or health records.

Logging and Auditing:
Cerego uses a centralized logging solution in order to manage all access logs and provide a reliable audit trail.

Availability:
All Cerego services are provided using auto-scaling servers and automated self-healing failovers. We guarantee 99.9% uptime to all of our clients. We monitor all of our services continuously and have numerous automated checks that alert our engineering team in the event of an incident. You can see a recent history and track the status of our services at https://status.cerego.com

Data Privacy:
Cerego is committed to protecting your sensitive data, and we will never share your data with third-party services without your consent.

Testing:
We test all changes in a dedicated replica of our production environment. Our engineering team uses Test Driven Development (TDD) practices to ensure our APIs are verified against a suite of thousands of automated tests that are continuously running. A nightly audit job verifies the integrity of all data stored within our database.