Mentornity Security

Data Security

Customer data is managed and stored using industry-standard database technologies.

All sensitive data is encrypted and stored securely in the database, with encryption keys managed safely.

Our applications are ‘HTTPS only,’ and all data in transit is encrypted using TLS 1.2 and 1.3. Lower TLS versions are disabled to adhere to the best security standards.

Our calendar integrations use secure server-to-server authentication protocols.

Official APIs are always used to read and write data for calendar synchronization when users choose to sync their calendars.

Operational Security

Access to customer data is restricted to Mentornity employees who require it to fulfill their job responsibilities.

We have a privacy program and comprehensive information security policies that define our approach to managing security and privacy.

Dedicated security and privacy teams oversee our security and privacy programs and constantly monitor our networks to detect suspicious activity.

Software Security

We follow a Secure Software Development Lifecycle (SDLC) model that incorporates security and privacy by design throughout all phases of product development, testing, release, and post-release support.

Our products offer advanced security tools, including two-factor authentication, account lockout, password policies, and session timeout settings, allowing users to enhance their account security further.

We perform numerous vulnerability tests to maintain a high level of product security.

Our employees receive regular training on security issues, trends, and defensive programming concepts.

Infrastructure Security and Monitoring

Our applications are hosted on Amazon AWS data centers located in Europe.

These data centers provide the highest level of physical security around the clock, including biometrics, intrusion detection systems, and interior and exterior surveillance.

We regularly update our infrastructure in accordance with recommendations provided by Amazon.