Mursion

Security

Last updated January 2022

Internal Personnel Security

- All Mursion employees must complete and stay current on our security awareness training programs
- All security personnel must acquire and maintain industry security training certificates
- All software engineers are trained with a security mindset that focuses on implementing security best practices during the Software Development Lifecycle

Data Encryption

- All data is transferred using TLS 1.2
- All data is encrypted at rest and in transport using AES 256 encryption
- All client data is logically separated from each other on AWS

Software

- Our software is tested by independent third parties for security vulnerabilities with every iterative release of our software (or at least annually)
- Delivery through Mursion proprietary software "Mursion Magic" authenticates with encrypted JSON tokens, adding an extra layer of protection.
- Access to Mursion Magic simulation requires learner authentication, and links are unique per session, which prevents users from accidentally or maliciously joining sessions

Convenience

- Our platform's SSO integration utilizes OAUTH, OIDC, and SAML 2.0
- Learners can easily access their secure simulation recordings via the Mursion portal's private accounts.
- Clients decide what personally identifying information is collected by Mursion and how it is used.

Cloud Infrastructure

- All data is hosted and processed in an SSAE 16 SOC2 compliant data center (AWS)
- Mursion's SIEM system responds to infrastructure incidents 24/7 to ensure all systems are always secure and fully functional.

Accessibility & Compliance

- Mursion meets WCAG 2.1 Level AA standards for accessibility and provides assistive technology for people with physical disabilities.
- Mursion provides industry-leading security and stability, including Soc-2 & GDPR Compliance.
- Mursion follows all regulations on FERPA and CCPA.