Study Manager Security

November 1, 2026

Last updated November 1, 2026

Study Manager runs on Amazon Web Services in the United States, with data encrypted in transit and at rest and a database that cannot be reached from the internet. This page describes the controls in place today. It forms part of our Privacy Policy and Terms of Use.

Infrastructure

Area	Control
Hosting	Amazon Web Services, US East (N. Virginia) region. AWS secures the physical data centers and underlying hardware.
Encryption in transit	All traffic between your browser and the Service is encrypted.
Encryption at rest	The database, uploaded files and server disks are encrypted.
Network	The database is not publicly accessible; only the Service's own servers can reach it.
Infrastructure as code	Our AWS setup is defined in version-controlled code, so every change is recorded and repeatable.

Accounts and access

- Passwords are stored only as one-way hashes. No one at Seralogix can read your password.
- Passwords must be at least 12 characters. Repeated failed sign-ins lock the account for 15 minutes, and sign-in attempts are rate-limited.
- The sign-up page uses Google reCAPTCHA to block automated sign-ups.
- Access inside the Service follows each organization's roles. Users see only their own organization's data.
- Each organization's administrators invite users, assign roles and remove accounts.

- We record which version of the Terms of Use each user accepted, and when.

Seralogix access to production

- Only named Seralogix staff can reach production systems, each with an individual account. Credentials are never shared.
- Multi-factor authentication is required for console sign-in to our AWS root and administrator accounts.
- Our AWS console passwords must be at least 14 characters with mixed character types, and the last 24 cannot be reused.
- Servers are managed through AWS Systems Manager rather than SSH keys, and administrative access is logged.

Activity records and logs

- The Service records which user created or changed which study items, and when. Organizations can rely on this for their own records.
- Server logs (IP address, browser type, pages requested, errors) are kept for 14 days to investigate problems and abuse.
- Administrative access to our hosting infrastructure is logged.

Backups and deletion

- The database is backed up automatically, and backups are kept for 14 days.
- Earlier versions of uploaded files are kept for 30 days so they can be recovered.
- Data deleted from active systems is gone from backups within 35 days.

AI features

AI features send data to OpenAI only when an organization allows it:

- AI assistance is off until an administrator turns it on.
- AI drafting can be turned off by an administrator.
- A single study can opt out.

We never send passwords or payment details. OpenAI does not use data sent through its API to train its models. See the Privacy Policy, section 6.

Third parties

We use four subprocessors: AWS, OpenAI, and Google for email and reCAPTCHA. Each is bound by written confidentiality, security and data protection terms. The full list is at seralogix.com/subprocessors. We use no analytics, advertising or tracking providers.

Testing and certifications

We have not yet had a third-party penetration test. Study Manager does not hold a security certification of its own; AWS's SOC 2 and ISO 27001 certifications cover the hosting infrastructure it runs on. We will update this page as that changes.

Incidents

If we confirm unauthorized access to personal information or Customer Data in our systems, we will notify the affected Customer within 72 hours of confirming it. We will explain what happened, what data was involved and what we are doing about it. We will also notify individuals and authorities where the law requires.

Your part

Security is shared. Organizations should keep their user list current, give each person the least access they need, remove users who leave, and use strong, unique passwords.

Reporting a security issue

If you find a vulnerability or suspect unauthorized access, email security@seralogix.com with enough detail for us to reproduce it. Please give us reasonable time to fix it before disclosing it publicly, and do not access other people's data or disrupt the Service while testing. We will acknowledge your report and keep you updated.