theSimCal

Security Overview

FOR IT AND PROCUREMENT REVIEWERS · Version 1.0 · Last updated September 4, 2026 · Reviewed annually

How theSimCal separates one organization's data from another's, how that data is protected in transit and at rest, where it is hosted, and what we do and do not claim.

1 Scope of this document

theSimCal is a hosted booking and scheduling platform for healthcare simulation centers. Each customer organization runs as a separate instance of the application, with its own database, its own web address, and its own configuration. The platform is fully hosted, so there is nothing to install on your network and no integration work is needed to start using it.

This document describes the security controls built into that platform. It is a plain description of how the system works. It is not a certification, not an audit report, and not the output of a third-party penetration test. Where a control is partial or still being rolled out, we say so rather than rounding up.

Controls proportionate to the data. theSimCal books rooms, equipment and staff time. For most users the only personal information it holds is a name and a work email address. It holds no patient data, no health information and no payment details, so the consequence of a compromised account is a disrupted schedule rather than exposed patient records. We have deliberately kept the platform easy to get into, because a coordinator who cannot sign in before a session starts is a real operational problem, and heavy authentication protecting a room calendar is friction without a matching benefit. **Some organizations have stricter internal requirements regardless of the data involved. If yours does, we are glad to discuss adding the controls you need. Ask us.**

2 What theSimCal holds, and what it does not

WHAT IT STORES

- Account details for staff and requesters: name, work email, role, and department or affiliation
- Booking requests and their scheduling details: session title, learner group and numbers, dates, times, rooms, equipment and staffing
- Notes and messages exchanged about a request
- Center configuration: rooms, assets, task trainers, manikins, availability and operating hours
- Files a user chooses to attach, plus logos and room or asset photographs

WHAT IT DOES NOT STORE

- Patient records or any clinical documentation
- Health information about learners or staff
- Payment card numbers or banking details
- Student grades, assessment scores or academic records
- Social insurance, social security or other government identifiers

Our recommendation. Do not attach identifiable patient information to a booking. The platform is designed to schedule simulation sessions, rooms and equipment, not to serve as a clinical record system. See section 7 for how attachments are served.

3 Separation between organizations

This is the control that matters most in a platform serving many organizations, so it is enforced at several independent layers rather than one. A failure at any single layer does not expose another organization's data.

Separate databases and scoped credentials apply to every instance without exception. The operating-system separation described below is the current platform standard, and every instance now runs on it.

Separate database. Every organization has its own database. There are no shared tables and no tenant-identifier column that code could forget to filter on. The wrong data is not reachable because it is not in the database being queried.

Scoped credentials. Each instance authenticates with a database user granted read and write on that one database and nothing else. Our provisioning tooling refuses to deploy an instance whose credentials carry cluster-wide privileges.

Separate operating-system account. Each instance runs as its own unprivileged Linux user, in its own directory, readable only by that user. No instance runs with administrative rights on the server.

No shared network port. Instances communicate with the web server over a private local socket with restricted permissions, not a network port. One instance cannot reach another instance's API, even from the same machine.

Isolated secrets. Configuration secrets are held in a file readable only by the system administrator account, then handed to the application as environment variables at startup. The application process itself cannot open the file, and neither can any other instance.

Resource limits. Each instance runs under memory, CPU and process ceilings, so one organization's traffic or a runaway job cannot degrade service for the others.

4 Data protection

In transit. All traffic between browsers and the platform is encrypted with TLS 1.2 or TLS 1.3. Older protocol versions are disabled. Certificates are issued by Let's Encrypt and renew automatically. Plain HTTP requests are redirected to HTTPS, and browsers are instructed to use HTTPS exclusively for the domain (HSTS).

At rest. Databases are hosted on MongoDB Atlas, which encrypts stored data and backups at rest. Uploaded files are stored in Amazon S3, which encrypts objects at rest by default.

Backups. Database snapshots are taken daily, retained for seven days, and held in the same region as the instance they belong to. A snapshot older than seven days no longer exists, which also sets the outer limit on how long deleted data can persist in backup.

Passwords. User passwords are never stored in readable form. They are stored as bcrypt hashes, and the plaintext is not retained anywhere, including in logs. Password reset links are single use, invalidated as soon as they are redeemed, and carry 120 bits of randomness from a cryptographically secure generator, which puts guessing one out of practical reach.

5 Data residency

Organizations are hosted in the region appropriate to their jurisdiction. An instance's data, meaning its database, uploaded files and outbound email, stays within the region it was provisioned in.

REGION	APPLICATION SERVER	DATABASE	FILES AND EMAIL
Canada	DigitalOcean, Canada	MongoDB Atlas, Canada	AWS, Canada
United States	DigitalOcean, United States	MongoDB Atlas, United States	AWS, United States
United Kingdom	DigitalOcean, United Kingdom	MongoDB Atlas, United Kingdom	AWS, United Kingdom

Credentials for file storage and email are held separately per region, so an incident affecting one region's keys does not extend to another's. Your instance's region can be confirmed in writing on request, and further regions can be provisioned where an organization's policy requires one that is not listed here.

6 Accounts and permissions

The platform distinguishes three levels of access: administrators, who manage the organization's settings, rooms, assets and staff; staff members, who manage bookings; and requesters, who submit and track their own booking requests. Permission is checked on the server for every request, not merely hidden in the interface.

Everyone at your center signs in under their own named account, so an action is attributable to a person rather than to a shared login. Sessions are identified by a 384-bit random token issued at sign-in and revoked at sign-out. Administrators can add and remove staff accounts, and other administrators, themselves, so access can be revoked immediately when someone leaves, without waiting on a support request.

Two things to state plainly, both of them deliberate. The platform does not currently offer multi-factor authentication, so account security rests on password strength, and a session stays valid until the user signs out rather than expiring after a period of inactivity. Given what the platform holds, a name, a work email and a

room booking, we judged the friction of extra sign-in steps to cost coordinators more than it protects them. That is a trade-off, not an oversight, and it is one we will revisit for any organization that needs it handled differently. We do recommend that staff sign out on shared or public computers, and that administrators remove accounts promptly when someone leaves.

7 Uploaded files

Files attached to bookings, staff notes and feedback, along with logos and room and asset photographs, are stored in Amazon S3 rather than on the application server.

Worth understanding before you upload sensitive material. Each file is stored at a web address containing 120 bits of random data, which makes the address impossible to guess or enumerate. However, the file is served to anyone who holds that address. Access is not re-checked against the requester's login. In practice these addresses circulate in emailed notifications, so they should be treated like an unlisted link: private in practice, but not access-controlled. Moving attachments to short-lived signed links is planned for 2027.

8 Infrastructure and operations

Hosting	Application servers run on DigitalOcean. Databases are managed instances on MongoDB Atlas. File storage and outbound email use Amazon Web Services. All three are selected per region.
Operating system	Ubuntu LTS, currently 26.04, chosen for its long-term support window rather than a short-lived interim release.
Application runtime	Node.js 24. Instances track the latest minor release of that branch, so security fixes are picked up without an unplanned major-version change.
Server access	Administrative access is by SSH key only. Password authentication is disabled entirely, and SSH listens on a non-standard port to reduce automated scanning. Production credentials are held by a small number of named people, and are recoverable through documented escrow so that no single person's absence can prevent an instance being maintained or restored.
Network exposure	A host firewall permits only web traffic and administrative SSH. Application instances are not reachable from the network directly, only through the web server.
Intrusion mitigation	Repeated failed authentication attempts result in the source address being blocked automatically.
Patching	Operating-system security updates are applied automatically.
Repeatable provisioning	New instances are created by an automated, version-controlled process rather than by hand, so every organization receives the same hardened configuration and no step is skipped under time pressure.
Logging	Each instance logs to the host's system journal, separately from other instances, for diagnosis and incident review.

9 Service providers

These are the third parties involved in running the platform, and what each one holds.

PROVIDER	PURPOSE	DATA INVOLVED
DigitalOcean	Application hosting	Application processes and system logs
MongoDB Atlas	Managed database and snapshots	All records held in your instance
Amazon Web Services	File storage and outbound email	Uploaded files, notification email content and recipient addresses
Let's Encrypt	TLS certificates	Domain names only
Cloudflare	Public website hosting and its contact form	Website visits, and contact-form submissions from thesimcal.com

The public website at thesimcal.com is hosted separately from the platform. Its contact form is protected by Cloudflare Turnstile and delivers to our own inbox. No customer records are held there.

10 What this document does not claim

theSimCal does not currently hold SOC 2, ISO 27001 or equivalent certification, and has not undergone an independent penetration test.

No claim of HIPAA, PIPEDA or UK GDPR compliance is made here. Compliance depends on how your organization uses the platform and what data you choose to place in it, and is properly established through a data processing agreement rather than a product document.

We are glad to complete a security questionnaire, sign a data processing agreement, discuss any control above in more detail, or look at adding a control your organization requires that is not listed here.

11 Questions, questionnaires and reporting an issue

Write to **security@thesimcal.com** with anything raised by this document: a specific control, your instance's region, a vendor assessment questionnaire, or a suspected security issue. We aim to reply within two business days, and we will acknowledge a reported issue before investigating it. Please do not disclose a suspected issue publicly until it has been resolved.

If your organization needs a control that is not described here, that is a conversation, not a barrier to adoption. Tell us what your policy requires and we will look at how to meet it.

Security Overview, version 1.0. Last updated September 4, 2026.

Reviewed annually and whenever the platform changes materially.