Security

How Asynchrone Space protects your workspace and data, and what is not shipped yet.

October 31, 2026 · Asynchrone Space · asynchrone.space/legal/security

Encryption

All traffic between your browser and Asynchrone Space uses TLS. Repository and integration tokens are encrypted with AES-256-GCM before they are stored, and passwords are hashed with scrypt; we never store them in plain text.

Data at rest sits on encrypted storage volumes in our hosting environment. Beyond the integration tokens above, we do not encrypt individual database columns.

Access control

Organizations include role-based access control with owner, admin, member and viewer roles, and file access can be restricted per person and per file.

Our own staff reach customer workspaces only through a separate internal control tower that requires a password and a TOTP authenticator. Every action taken there is written to a platform audit trail, and support impersonation is a single-use handoff valid for one minute that opens a one-hour session — never a shared session cookie. The workspace sees an impersonation banner and can end the session at any time.

Enterprise workspaces also include a customer-facing audit log of member, role, invitation and settings changes, with CSV export and a configurable retention window. Owners and admins read it from the workspace settings.

Data location and backups

The application and the PostgreSQL database that holds your workspace, including uploaded files, run on OVHcloud infrastructure in Gravelines, France, inside the European Union. No customer data is stored outside the EU except where a sub-processor listed at asynchrone.space/legal/subprocessors receives it.

Backups and point-in-time recovery are configured by the operator of each deployment at the database level; they are not a self-service feature. If your contract requires documented backup and restore objectives, confirm the current runbook with security@asynchrone.space before signing.

What is not available yet

We would rather list what is missing than let a questionnaire discover it. The following are not shipped today:

- SAML single sign-on and SCIM provisioning.
- Third-party certifications such as SOC 2 or ISO 27001.
- Self-service restore from a backup.

Reporting a vulnerability

We monitor for anomalies and act on reports. If you believe you have found a vulnerability, email security@asynchrone.space — we acknowledge reports within 3 business days and tell you what we found and when we expect to fix it. Please do not open a public issue.

We disclose incidents promptly and transparently to affected organizations. Our data processing agreement commits us to notifying customers within 24 hours of becoming aware of a personal data breach.