Security overview

Version 1.0 | Last updated 29 September 2026

This is a translation of the French original, which governs in case of divergence.

This page summarises, for a customer or its security team, the technical and organisational measures in force for Avanserv SRL's services as of the date at the top of the page. It complements, without replacing, annex B of the data processing agreement, which is contractually binding for a given customer. What is planned is presented as such.

Hosting

The services are hosted by Scaleway SAS, a company under French law, in the fr-par region (France). The site and the application are served from this region. A transfer outside the Union stays possible for some exchanges with third parties, governed as article 9 of the data processing agreement describes for a customer, and the privacy policy for a visitor of the site.

Encryption

Traffic to the site and the application is encrypted in TLS, with the certificate issued and renewed automatically. The app.avanserv.com platform database is encrypted at rest. The "access_token" and "refresh_token" session cookies carry the Secure and HttpOnly flags outside development; the "avanserv_signed_in" cookie, which tells the public site that a session exists elsewhere without revealing its content, is deliberately readable by code running in the browser and does not carry the HttpOnly flag.

Tenant separation

Separation between customer organisations is logical, on shared infrastructure. Only an organisation's projects and single sign-on (SSO) configurations are filtered by organisation on every read, write and delete, with no way to bypass it from the interface or the API. Other records, such as accounts, files and public form submissions, are not subject to this filter: accounts reach an organisation through a

membership rather than through this filter, and the set is protected instead by the access control described below.

Authentication and passwords

A password is never stored in the clear: only a bcrypt hash is kept. Setting or changing a password requires a minimum length of 12 characters and refuses the most common passwords; no composition rule (an uppercase letter, a digit, a special character) is enforced by default. When the service answers within three seconds, the password is also checked against known breaches with the Have I Been Pwned service, by comparing a cryptographic hash fragment that lets neither the password be reconstructed nor a person be identified; past that delay, the check is skipped and the password is accepted.

Access control

Rights are granted through a declarative model built on roles and privileges, applied on every request: what is not explicitly authorised is refused.

Secrets

Credentials the services need at runtime (database passwords, application keys) are kept in Scaleway's secret manager and synchronised into the runtime environment by a dedicated controller, on a regular interval (hourly for the application) rather than at the moment of each change; no secret is committed to the code.

Change management

Every merge of code to the production branch requires continuous integration (formatting, static analysis, typing, tests) to pass, with no exception. The requirement to go through a pull request carries one exception, reserved for a technical automation account on the repository. Infrastructure changes also go through a pull request, but are applied from an operator's own checkout rather than automatically on merge.

Backups

The app.avanserv.com platform database is backed up once a day, and each backup is kept for seven days. For data a customer hosts with the provider, the backup follows

the terms set in the quote, as the data processing agreement and article 7 of the SLA provide; absent a mention in the quote, no backup is owed.

Logging

Requests the application serves are logged with a request id; a signed-in session adds the organisation and the account concerned. Email addresses are masked in these logs before they are written. Centralised collection of these logs, metrics and traces, with an alert that reaches an on-call person, is planned and is not yet active: each log stays today on the node that produced it, under that runtime environment's default rotation.

Vulnerability disclosure

Anyone who finds a security flaw in our systems can report it under the coordinated vulnerability disclosure policy.

Incident notice

The notice commitments for a personal data breach are in the data processing agreement and in the privacy policy.

Questions about these measures: security@avanserv.com.