

Security overview

Where Clauseloop keeps customer data, the controls that protect it today, what is not in place yet, who else processes data, and our answers to the questions procurement teams ask most.

Generated 23 October 2026 from <https://crm.avantcert.com/trust>. The Trust Center is the current version.

Where your data lives

Our own servers, in India

Clauseloop runs on our own servers at Oracle Cloud Infrastructure in India: the application, its PostgreSQL database and every uploaded file. The database runs Supabase's open-source software on those servers, so no outside database service holds your records.

Cloudflare in front

Cloudflare answers DNS and serves the site to your browser over TLS. It caches only public files such as scripts and images; every response that carries a signed-in session is marked not to be cached.

Email

The emails the application sends, such as portal sign-in links, invoices and reminders, go out through Resend.

In place today

Encryption in transit

Every connection from your browser is encrypted with TLS, and HSTS tells browsers never to connect without it.

Encryption at rest

Our servers store data on Oracle Cloud block volumes, which Oracle encrypts at rest with AES-256 by default. Google tokens for connected calendars are also encrypted with AES-256 before they are stored.

Access rules in the database

PostgreSQL enforces row-level security on every table, with rules for each role, so access is enforced by the database and not only by the application.

Roles, and clients kept apart

Admins, consultants, sales associates and finance managers each reach only the pages and records their role needs. A client portal user reaches only their own organisation's projects, documents and invoices.

Deactivated accounts are cut off

When an admin deactivates a staff account, its sessions end and it can no longer sign in.

Audit log

Privileged actions, such as user and role changes, invoice approvals, payments and settings changes, are written to an audit log with who did what and when.

Application hardening

Every response carries a Content Security Policy, X-Frame-Options, X-Content-Type-Options, a Referrer-Policy and a Permissions-Policy. API calls from the app need a CSRF token, and sensitive endpoints are rate-limited.

Error reports

Application errors are reported to Sentry, with cookies and authorization headers removed before they are sent.

No card numbers

Card payments are made with the payment provider. Clauseloop never sees or stores a full card number.

Not in place yet

Two-factor sign-in

Two-factor sign-in is not available yet. It is planned.

Backups proven by a restore test

A tested restore of the database is planned. Until it has been done, we do not describe our backups as proven.

Uptime monitoring and a status page

Alerts when the service goes down, and a public status page, are planned.

A separate staging environment

Changes are tested on a throwaway copy built for each test run; a standing staging environment is planned.

A written incident-response policy

A written incident-response and breach-notification policy will be published with our data processing agreement.

Certification of SWC itself

Clauseloop is not SOC 2 or ISO 27001 certified.

AI and your data

AI drafting is switched off. No customer, client or lead data is sent to any AI provider.

AI will come back only as an optional, paid add-on that is off unless you ask for it. When it is on, it runs on models we host on our own servers, so nothing leaves our infrastructure, and it is used only to draft sales and client emails. Audit work, reports and documents never go to it.

Subprocessors

Provider	What it does	Data it receives
Oracle Cloud Infrastructure (India)	Hosts the application, its database and uploaded files	Everything stored in the application
Cloudflare	DNS, TLS and delivery of public files	Request details such as IP addresses
Resend	Sends the application's emails	Recipient addresses and email content
Google	Analytics on the public website; Calendar and Search Console only if you connect them	Page views on the public website; the calendar events and search data you connect
PostHog (EU)	Product analytics in the application	The pages staff open, with their user ID
Sentry	Error reports	Error details, with cookies and authorization headers removed
Stripe, PayPal and Cashfree	Payments, only if you connect them	Payment confirmations that carry the invoice number

Report a vulnerability

Email info@swcservices.com with what you found and the steps to reproduce it. Test only with an account of your own, and do not open, change or delete other people's data.

Security questionnaire answers

Certification and governance

Is the company certified to ISO/IEC 27001 or attested to SOC 2?	No	Clauseloop is not SOC 2 or ISO 27001 certified. The Trust Center lists the controls in place today and the ones that are not yet.
Do you publish the subprocessors that process customer data?	Yes	The Trust Center names each outside service that processes data and what it receives.
Is there a way to report a security vulnerability?	Yes	Email info@swcservices.com . The same contact is published in /.well-known/security.txt .

Hosting and infrastructure

Where is customer data hosted?	Yes	On our own servers at Oracle Cloud Infrastructure in India: the application, its PostgreSQL database and uploaded files. The database runs on those servers, not with an outside database service.
Is a content delivery network or proxy in front of the service?	Yes	Cloudflare answers DNS and serves the site over TLS. It caches only public files; responses that carry a signed-in session are marked not to be cached.
Do you keep a separate staging environment?	Planned	Changes are tested end to end on a throwaway database built for each run; a standing staging environment is planned.

Data protection

Is data encrypted in transit?	Yes	Every connection from the browser uses TLS, and HSTS tells browsers never to connect without it.
Is data encrypted at rest?	Yes	Our servers store data on Oracle Cloud block volumes, which Oracle encrypts at rest with AES-256 by default. Google tokens for connected calendars are encrypted again with AES-256 before they are stored.
Is each customer's data isolated from other customers?	Yes	PostgreSQL enforces row-level security on every table, and a client portal user reaches only their own organisation's records.
Do you store payment card data?	No	Clients pay with the payment provider; Clauseloop never sees or stores a full card number.
Can customers export their data?	Partly	Reports export to PDF or Excel from the application. A complete export of everything we hold is done on request.

AI

Is customer data used to train AI models?	No	AI drafting is switched off, and no customer, client or lead data is sent to any AI provider.
Is customer data sent to third-party AI providers?	No	AI is an optional add-on that runs on models we host on our own servers, and it is used only to draft sales and client emails. It is switched off today.

Access control

Is access role-based?	Yes	Admins, consultants, sales associates and finance managers each reach only the pages and records their role needs, and the database enforces the same rules.
Is multi-factor authentication available?	Planned	Two-factor sign-in is not available yet. It is planned.
How do your customers' clients sign in?	Yes	Client portal users sign in with a one-time link sent to their email address; they have no password to lose.
Is access removed promptly when someone leaves?	Yes	When an admin deactivates a staff account, its sessions end and it can no longer sign in.

Application security

Do you use a Content Security Policy and other security headers?	Yes	Every response carries a Content Security Policy, X-Frame-Options, X-Content-Type-Options, a Referrer-Policy and a Permissions-Policy.
Are state-changing requests protected against CSRF?	Yes	API calls from the application need a CSRF token.
Are endpoints rate-limited?	Yes	Portal sign-in links, password resets, public forms and the API are rate-limited per client IP address, read from Cloudflare so it cannot be spoofed.
Are third-party dependencies checked for known vulnerabilities?	Yes	Every release is checked with npm audit for the application and the automation server; a high or critical finding blocks it.

Logging and monitoring

Are privileged actions logged?	Yes	User and role changes, invoice approvals, payments and settings changes are written to an audit log with who did what and when. The database refuses any change to or deletion of an audit entry.
Are application errors monitored?	Yes	Errors are reported to Sentry, with cookies and authorization headers removed before they are sent.
Is uptime monitored, with alerts and a status page?	Planned	Alerts when the service goes down, and a public status page, are planned.

Continuity and incidents

Are backups tested by restoring them?	Planned	A tested restore of the database is planned. Until it has been done, we do not describe our backups as proven.
Do you have a written incident-response and breach-notification policy?	Planned	It will be published with our data processing agreement.

Privacy

Which analytics run, and where?	Yes	Google Analytics runs on the public website only, never in the application or the client portal. Inside the application, PostHog (EU) records which pages staff open; it sets no cookies.
Can you sign a data processing agreement?	Planned	Our data processing agreement is being prepared, together with the written incident-response policy.