Archived copy of app.stitchops.io/docs/privacy, Privacy Policy last updated September 9, 2026. Captured October 29, 2026.

Privacy Policy

Last updated September 9, 2026.

StitchOps, Inc. (“StitchOps”, “we”, “us”) provides an automation platform that runs workflows inside applications on our customers' behalf. This policy explains what information we collect, how we use and store it, who we share it with, how long we keep it, and the choices you have. It covers the StitchOps website, the web application, the StitchOps agent, the API, and the AI assistant connectors we publish for Claude, ChatGPT, and Microsoft Copilot (together, the “Services”).

StitchOps is a business service. Our customers are organizations. When a customer uses the Services to automate its own systems, the customer is the controller of the data in those systems and StitchOps is a processor acting on the customer's instructions.

1. Information we collect

Account information

Name, work email address, organization name, authentication identifiers issued by our identity provider, role in the workspace, and billing contact details. If your organization uses single sign-on, we receive the attributes your identity provider releases.

Customer content

Workflow definitions, workflow inputs and typed results, records you store in StitchOps data tables, connection settings for integrations, and credentials you save for the systems you automate. Credentials are encrypted with a key that is unique to your workspace and are decrypted only on your agent at run time.

Operational telemetry

Execution records: which workflow ran, when, on which agent, each step's status and timing, and the typed output each step reported. Agent heartbeats and version information. Application logs and audit logs of administrative actions.

Data processed on your agent

Screen content, screenshots, OCR output, page content, and the values of fields the agent reads or types are processed on the agent inside your environment. They are not transmitted to StitchOps infrastructure unless a workflow step explicitly returns them as a result, or you ask an AI assistant connector to observe the agent.

Website and usage information

Browser type, device, pages visited, referring page, IP address, and interaction events in the application, collected through server logs and standard analytics. We do not sell this information and do not use third-party advertising trackers on the application.

2. How we use information

Purpose	Information used
Provide, run, and support the Services	Account information, customer content, operational telemetry
Authenticate users and enforce workspace isolation	Account information, authentication identifiers
Troubleshoot failures and improve reliability	Operational telemetry, application logs
Detect abuse and protect security	Account information, application logs, audit logs

Bill and communicate about the account	Account information
Comply with law and enforce our terms	Any of the above as required

We do not use customer content or execution results to train machine-learning models. AI features in the product send only the content required for the request you made to the model provider, and we do not permit those providers to train on it.

3. AI assistant connectors

When you connect StitchOps to Claude, ChatGPT, Codex, or Microsoft Copilot, that assistant calls our tools on your behalf. We receive the tool call, the signed-in user's identity, and the workspace it belongs to. We return the tool result to the assistant. Whatever a tool returns becomes visible to the assistant and its provider under that provider's terms and privacy policy. Tools that would return a stored credential value are not available to assistants. We do not receive or store your conversation with the assistant beyond the tool calls themselves, and we do not attempt to extract conversation content from assistants.

4. Who we share information with

We share information only as needed to run the Services:

Recipient	Purpose
Cloud infrastructure providers (Amazon Web Services)	Hosting, storage, key management, and backups
Identity provider (Auth0 by Okta)	Sign-in, single sign-on, and OAuth for connectors
Model providers (Anthropic, OpenAI) when you use an AI feature	Text and image analysis for the specific request

Payment processor (Stripe)	Subscription billing; we do not store card numbers
Email and support tooling	Account communications and support tickets
Professional advisers and authorities	When required by law, to protect rights, or in a merger or acquisition

Sub-processors act under written agreements that limit their use of information to providing their service to us. We do not sell personal information and do not share it for cross-context behavioral advertising.

5. Where information is stored

StitchOps infrastructure runs in the United States. Customers in other regions may transfer information to the United States by using the Services. Where the law requires, we rely on standard contractual clauses or an equivalent mechanism for those transfers.

6. How long we keep information

Information	Retention
Workflow execution telemetry	90 days, then deleted automatically
Agent heartbeat and presence metadata	Up to 26 hours
Customer content (workflows, data tables, saved connections)	For the life of the subscription; deleted within 30 days of termination
Account information	For the life of the account, then deleted with the workspace
Audit logs	At least one year
Encrypted backups	Rotated within 35 days; deleted data is not restored

A workspace administrator can request earlier deletion at any time. We complete verified deletion requests within 30 days and confirm in writing. Records subject to a legal hold are retained until the hold is lifted.

7. Security

We encrypt information in transit and at rest. Saved credentials use per-workspace envelope encryption managed in a hardware-backed key service. Agents connect outbound only and expose no inbound ports. Every request to the API is scoped to a single workspace. Access to production systems is limited to named engineers with multi-factor authentication and is logged. We maintain a vulnerability management program and undergo independent SOC 2 examination. Report a security concern to security@stitchops.io.

8. Your choices and rights

Depending on where you live, you may have the right to access, correct, delete, or export your personal information, to restrict or object to its processing, and to complain to a supervisory authority. Because we process most information on behalf of a customer organization, we may direct your request to your workspace administrator. Send requests to privacy@stitchops.io. We will verify your identity and respond within the time the applicable law allows. We do not discriminate against anyone for exercising these rights.

You can disconnect an AI assistant at any time from that assistant's settings. Doing so revokes its token and stops all further tool calls.

9. Cookies

The application uses cookies and similar storage that are necessary to keep you signed in and to remember preferences. The website may use analytics cookies to measure traffic. You can control cookies in your browser; disabling necessary cookies will prevent sign-in.

10. Children

The Services are not directed to children and we do not knowingly collect information from anyone under 16.

11. Changes to this policy

We will post any changes on this page and update the date at the top. For material changes we will notify workspace administrators by email before the change takes effect.

12. Contact

StitchOps, Inc., a Delaware corporation
Privacy: privacy@stitchops.io
Support: support@stitchops.io

← Support

Browser Extension Privacy →