# Trust and Compliance

VERSION 1.0 · EFFECTIVE OCTOBER 1, 2026

## About this page

This page brings together how StitchOps, Inc. ("StitchOps") protects customer data and where to find the documents security, privacy, and procurement reviews ask for. The commitments themselves are in the Master Subscription Agreement at **https://www.stitchops.io/legal/msa** and the Data Processing Addendum at **https://www.stitchops.io/legal/dpa**.

## 1. Compliance

StitchOps, Inc. has completed its SOC 2 Type 2 examination covering Security, Availability, Confidentiality, Processing Integrity, and Privacy, along with HIPAA and GDPR Article 5 attestations, performed by Sensiba LLP for the period 15 May 2026 to 14 August 2026. Reports are available under NDA at **https://trust.stitchops.io**.

(a) **Scope.** The examination covers the StitchOps Cloud: the Control Plane, web application, and APIs, and the Amazon Web Services infrastructure StitchOps operates. Digital Workers, StitchOps Edge deployments, and customer managed credential vaults run on the customer's own infrastructure, under the customer's own controls, which keeps the data workflows handle in the customer's environment.

(b) **Next examination.** The next SOC 2 Type 2 examination covers a 12 month period.

(c) **ISO 27001.** Certification is being finalized. This page will be updated when the certificate is issued.

(d) **HIPAA.** A Business Associate Agreement is available on request.

(e) **GDPR.** The Data Processing Addendum includes the Standard Contractual Clauses and the UK and Swiss transfer terms. Privacy requests go to privacy@stitchops.io.

(f) **Penetration testing.** Independent penetration tests at least annually, with findings remediated.

## 2. How the platform protects data

(a) **Data stays with Customer.** The Digital Worker runs on Customer's own infrastructure. Screen content and the Personal Data workflows handle stay there. The Control Plane stores workflow definitions, account details, and execution metadata with redacted values.

(b) **Outbound only.** Digital Workers connect outbound over TLS 1.2 or higher and need no inbound ports.

(c) **Credentials.** Credentials stay in Customer's own credential vault by default, are resolved on the Digital Worker at run time, and are never sent to an AI model.

(d) **AI is optional.** Customers use their own AI model by default, can turn AI off, and Customer Data is never used to train AI models.

The security page at **https://www.stitchops.io/security** covers the architecture in more detail.

## 3. Data protection documents

(a) **Data Processing Addendum.** GDPR, UK, Swiss, and US state privacy terms, signed by StitchOps: **https://www.stitchops.io/legal/dpa**

(b) **Subprocessors.** Who processes customer data, for what, and where: **https://www.stitchops.io/legal/subprocessors**

(c) **AI Features and Providers.** How AI is used and controlled: https://www.stitchops.io/legal/ai

(d) **Security measures.** Annex II of the Data Processing Addendum.

## 4. Trust Center

Our Trust Center at **https://trust.stitchops.io** has our current security documentation and answers to common security questionnaires.

## 5. Contact

(a) **Report a security issue:** security@stitchops.io

(b) **Privacy and data protection requests:** privacy@stitchops.io

(c) **A security walkthrough with the team that built the platform:** https://www.stitchops.io/contact?topic=security

---

StitchOps, Inc., a Delaware corporation, 2707 Arapahoe Avenue #180, Boulder, CO 80302. Questions: legal@stitchops.io