Acceptable Use Policy

VERSION 1.0 · EFFECTIVE OCTOBER 1, 2026

About this policy

This Acceptable Use Policy ("Policy") applies to everyone who uses the StitchOps Service, including Customer and its Users, under the StitchOps Master Subscription Agreement at **https://www.stitchops.io/legal/msa** (the "Agreement"). Capitalized terms not defined here have the meanings given in the Agreement. StitchOps automates systems the way a person would, so this Policy pays particular attention to authorization, credentials, and the systems a workflow touches.

1. Authorization to automate

You may automate only the systems, accounts, and data you are authorized to access and automate. In particular, you will not use the Service to:

(a) access, automate, or extract data from any system, account, or environment you are not authorized to use, including another organization's systems;

(b) access, use, change, or delete any identity, account, or data without proper authorization;

(c) circumvent authentication, access controls, rate limits, bot detection, or other security measures of a system you are not authorized to administer; or

(d) automate a system in a way its terms prohibit, unless you have the right to do so, such as through a separate agreement with that system's provider.

2. Credentials

You will:

(a) use only Credentials that you, or the person or organization that owns the account, have authorized for the workflow;

(b) give each workflow the minimum access it needs, and remove access it no longer needs;

(c) keep Credentials in your credential vault or in the Service, and never place them in workflow steps, logs, prompts to an AI model, or support cases; and

(d) not use the Service to collect, test, or guess credentials, or to share credentials in ways the system's terms or your own policies do not allow.

3. Load on other systems

You will design and schedule workflows so they do not overload Customer Systems or any third party system, and you will respect published rate limits and fair use terms. StitchOps may slow or pause a workflow that is causing harm to a system or to the Service, and will tell you when it does.

4. Third party terms

You are responsible for complying with the terms of every Customer System and Third Party Product your workflows use, including any terms about automated access. StitchOps does not grant you rights to use any third party system.

5. AI Features

AI Features are optional. If you use them, you will not use them to:

(a) make automated decisions with legal or similarly significant effects on a person, such as hiring, firing, or access to essential services, without appropriate human review;

(b) profile people to predict criminal behavior, infer emotions in a workplace or school except for medical or safety reasons, or categorize people by sensitive biometric data;

(c) create or distribute sexually explicit content involving any person without consent, or any content that exploits minors; or

(d) deceive or manipulate people in ways that cause them significant harm.

6. General prohibitions

You will not use the Service to:

(a) engage in or promote illegal, fraudulent, or deceptive activity;

(b) violate the intellectual property, privacy, or other rights of others;

(c) threaten, incite, or promote violence, terrorism, or hate, or harm minors in any way;

(d) send spam or other unsolicited bulk messages;

(e) upload, store, or run Malicious Code;

(f) access, probe, disrupt, or test the security of the Service, except through responsible disclosure to **security@stitchops.io**;

(g) impersonate StitchOps or any person or organization; or

(h) provide professional advice, such as legal, medical, or financial advice, that requires a license you do not hold.

7. Investigation and enforcement

StitchOps may investigate suspected violations of this Policy. If a violation threatens the security, integrity, or availability of the Service or any system, StitchOps may suspend the affected workflows, Digital Workers, or accounts as

described in Section 2.7 of the Agreement, including notice and a chance to cure where reasonable. You will cooperate to fix any violation. A material violation of this Policy is a material breach of the Agreement.

8. Reporting violations

Report suspected violations to **legal@stitchops.io**, and security issues to **security@stitchops.io**.

9. Changes to this policy

StitchOps may update this Policy as described in Section 15.10 of the Agreement, including at least 30 days notice before a material change. Prior versions are kept at **https://www.stitchops.io/legal/archive**.

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