

Silktide Acceptable Use Policy

What the Silktide platform may and may not be used for, forming part of your agreement.

In effect: October 6, 2026 – present

<https://silktide.com/legal/acceptable-use-policy/>

This Acceptable Use Policy (**AUP**) forms part of the Agreement between the Customer and Silktide and applies to all use of the Services by the Customer, its Authorized Users, its Affiliates and its Clients. Capitalized terms not defined here have the meanings given in the Silktide Customer Terms (the **Terms**). The Customer is responsible for ensuring that everyone who uses the Services under its account complies with this AUP.

1. Purpose

- 1.1 The Services are used to scan, test, monitor and improve websites, documents and other digital properties, to remediate documents such as PDFs for accessibility, to measure how visitors use websites, and to monitor how AI platforms and search engines present an organization and its competitors so that it can improve its online visibility. The Documentation describes the products through which these features are offered. This AUP exists to protect the Services, Silktide's other customers, the owners of websites and platforms, and the individuals whose information may be processed, and to make clear what use of the Services is not permitted. It supplements, and does not replace, the restrictions in clause 4.5 of the Terms.

2. Scanning websites, monitoring platforms and measuring visitors

- 2.1 The Customer may submit to the Services only Customer Sites that it owns, or that it is authorized by the owner (including a Client) to have scanned, tested and monitored. The Customer must comply with the terms of use of any third-party platform that hosts a Customer Site, and must not use the Services to scan any website, application or system without proper authority.
- 2.2 Where a feature of the Services is designed to test publicly accessible third-party websites, such as a benchmarking or comparison feature, the Customer may use that feature for its intended purpose within the limits described in the Documentation.

- 2.3 The Customer must not use the Services: (a) to test any website or system for security vulnerabilities, or to gain or attempt to gain unauthorized access to any system, account or data; (b) in a way that is intended to, or is likely to, disrupt, overload or degrade any website or system, including by configuring scans at a frequency or depth that is unreasonable for the Customer Site concerned; (c) to collect or harvest personal data, email addresses or other information from websites for purposes unrelated to the scanning, testing, monitoring and improvement of Customer Sites; or (d) to monitor or surveil individuals.
- 2.4 **AI platforms, search engines and competitor websites.** Where a feature of the Services queries third-party AI platforms or search engines with prompts the Customer configures, or retrieves publicly accessible content from third-party websites the Customer identifies for comparison (clause 6 of the Terms), the Customer may use it to understand and improve how its own organization, brands, products and services are presented, within the limits described in the Documentation. The Customer must not: (a) configure prompts that seek information about identifiable individuals, or use the feature to monitor individuals; (b) identify for comparison any website that is not publicly accessible; (c) use the feature to manipulate, deceive or interfere with a third-party platform, or to create or seed misleading content about itself or others; or (d) publish or share the results other than as permitted by clause 9.2 of the Terms and in compliance with applicable law, including the laws on comparative advertising, defamation and intellectual property. Results reflect what the third-party platforms returned at the time of the query and should be treated as indicative.
- 2.5 **Visitor analytics.** Where the Customer deploys the Services' analytics code on a Customer Site (clause 4.10 of the Terms) to measure how visitors use it, the Customer: (a) may do so only on Customer Sites that it owns or is authorized to measure; (b) chooses, for each Customer Site, the analytics mode described in the Documentation (measurement without cookies, measurement using a first-party cookie, or a combination in which the cookie is used only once a visitor has consented), and is responsible for giving visitors any notice, and obtaining any consent, that applicable law requires for the mode it has chosen and the analytics as it has configured them, and for keeping its own privacy and cookie information accurate; and (c) must not configure the Services to capture data that identifies visitors by name or contact details, such as names, email addresses or the content of form fields, and must not attempt to link analytics data to named individuals or combine it with other data for that purpose.

- 2.6 **Documents submitted for remediation.** Where the Customer submits a document for remediation, the Customer: (a) may submit only documents that it owns or is authorized to have remediated; (b) must not submit documents containing the data described in clause 7.3 of the Terms (such as special categories of personal data, health information, payment card data or government identification numbers) unless agreed in an Order Form, and should review documents for such data before submission; and (c) is responsible for reviewing each remediated document, which is AI Output under clause 5 of the Terms, and satisfying itself that it is accessible before accepting, publishing or relying on it.

3. Content submitted to the Services

- 3.1 The Customer must not upload, enter or otherwise submit to the Services any content that: (a) is unlawful, or infringes the Intellectual Property Rights, privacy rights or other rights of any person; (b) is defamatory, harassing, threatening, hateful or discriminatory; (c) contains viruses, malware or other malicious code; or (d) the Customer does not have the right to submit.
- 3.2 As set out in clause 7.3 of the Terms, the Services are not designed to process special categories of personal data, protected health information, payment card data, government-issued identification numbers or other data subject to heightened regulatory requirements, and the Customer must not intentionally submit such data or configure the Services to collect it unless expressly agreed in an Order Form. Incidental processing of such data that is published on a Customer Site the Customer is authorized to scan is not a breach of this AUP.

4. Protecting the Services

- 4.1 The Customer must not, and must not permit anyone to: (a) interfere with or disrupt the integrity, security or performance of the Services or the data they contain; (b) probe, scan or test the vulnerability of the Services, or breach or circumvent any security or authentication measure, other than in accordance with section 6; (c) share login credentials, allow more than one individual to use a single Authorized User account, or access the Services using another person's credentials; (d) access the Services by automated means other than through the APIs and integrations Silktide makes available, exceed documented API rate limits, or scrape, crawl or systematically extract data from the Services; (e) circumvent or attempt to circumvent usage limits or access

restrictions; (f) reverse engineer, decompile or attempt to derive the source code, algorithms or scoring methodologies of the Services, except to the extent permitted by law; (g) access or use the Services to build, train or improve a competing product or service, or to copy their features or user interface; (h) misrepresent the Customer's identity or affiliation, or impersonate any person or organization; (i) use the Services to send unsolicited communications or to distribute advertising; or (j) frame, mirror or republish any part of the Services other than Output as permitted by the Terms.

5. Features that use artificial intelligence

- 5.1 Where the Services include features that use machine learning or generative artificial intelligence, the Customer must not use them: (a) to generate content that is unlawful, deceptive or intended to mislead; (b) to attempt to extract, reproduce or reverse engineer the underlying models, prompts or training data; (c) to process data that the Customer is not permitted to submit to the Services; or (d) to develop, train or improve a competing machine learning or artificial intelligence model or system using AI Output. AI Features are disabled by default and only process Customer Data when an administrator of the Customer's account has enabled them and selected an AI Processing Region and the providers to be used, as described in clause 5 of the Terms; the providers available depend on the AI Processing Region selected and are identified on the Sub-processor Page as optional AI sub-processors. AI Output should be reviewed by a suitably qualified person before being relied on or published, and the Customer may change its AI Processing Region or providers, or disable AI Features, at any time.

6. Security research

- 6.1 Silktide welcomes reports of security vulnerabilities in the Services. Anyone who identifies a potential vulnerability should report it to Silktide by email to security@silktide.com, should not exploit it, access or modify data belonging to others, or disrupt the Services, and should give Silktide a reasonable opportunity to investigate and remediate before making any public disclosure. Testing of the Services for vulnerabilities is permitted only with Silktide's prior written agreement.

7. Agency, Client and commercial use

- 7.1 Use of the Services on behalf of Clients is permitted only in accordance with clause 4.4 of the Terms. The Customer must not resell the Services, offer them on a standalone

basis, or present them as its own or a third party's product, unless an Order Form expressly permits it. Output may be shared with Clients and used in the Customer's own services as permitted by clause 9.2 of the Terms.

8. Compliance with law

- 8.1 The Customer must use the Services in compliance with all applicable laws, including laws relating to data protection and privacy, computer misuse and unauthorized access, intellectual property, export controls and sanctions, and consumer and marketing communications.

9. Enforcement

- 9.1 Silktide may investigate any suspected breach of this AUP and may, in accordance with clauses 12.7 and 18 of the Terms, remove or disable access to content, suspend the account or access of any Authorized User, or suspend or terminate the Services. Silktide will, where reasonably practicable, notify the Customer and give it an opportunity to remedy the breach before taking action, unless the breach poses an imminent risk to the Services, to other customers or to any person, or Silktide is required by law to act immediately. Silktide may report unlawful activity to law enforcement or regulatory authorities where it is required or reasonably considers it appropriate to do so, and the Customer will cooperate with any such investigation.
- 9.2 Anyone may report a suspected breach of this AUP by email to legal@silktide.com.

10. Changes

- 10.1 Silktide may update this AUP in accordance with clause 20 of the Terms. Updates that impose materially greater restrictions on the Customer are treated as updates that materially reduce the Customer's rights for the purposes of that clause.