Jubal Acceptable Use Policy

Effective date: December 14, 2026

Version: 2026-12-14

This Acceptable Use Policy (the AUP) is part of the Jubal Customer Terms of Service (the Terms) between Jubal Inc (Jubal, we, us) and the law firm that subscribes to the Service (the Customer). Terms defined in the Terms have the same meaning here. The AUP applies to the Customer, to every Authorized User, and to anyone else who uses the Service through the Customer's account. The Customer is responsible for its Authorized Users' compliance.

The AUP is not a complete list. If something is not listed here but is harmful, unlawful, or abusive, do not do it.

1. Who Jubal is for

1.1 A tool for law firms. Jubal is software for law firms, their lawyers, and the non-lawyer staff those lawyers supervise. It is not a law firm, it does not give legal advice, and it is not a service for the public to obtain legal help.

1.2 No unauthorized practice of law. You may not use the Service to provide, or to help anyone provide, legal services that the person providing them is not licensed or authorized to provide. In particular:

- A non-lawyer may not use Jubal to give legal advice or legal services to the public, or to anyone other than under the supervision of a lawyer who is responsible for the work.
- You may not offer Jubal, or its outputs, to clients or the public as a substitute for a lawyer's advice, or configure it as a public-facing legal adviser, chatbot, or self-help service.
- You may not give clients or other third parties direct access to Jubal's AI features except through a feature Jubal provides for that purpose, and then only under a lawyer's supervision.

1.3 Supervision. Every use of Jubal on a client matter must be under the supervision of a lawyer at the Customer who is responsible for the matter. The Customer represents that each person who uses the Service under its account is a lawyer admitted where the work is done, or is acting under the direction of such a lawyer, and that the Customer is responsible for that supervision. Jubal does not check bar admission. The representation and this AUP are the restriction.

2. Unlawful and harmful use

You may not use the Service to:

- Violate any law or regulation, any court order, or any rule of professional conduct that applies to you.
- Violate anyone's rights, including privacy, publicity, confidentiality, and intellectual-property rights.
- Create, upload, store, or send content that is defamatory, harassing, threatening, or fraudulent, or that infringes or misappropriates another's rights, including using the Service to generate content intended to harass, intimidate, defame, or deceive any person, party, witness, court, or agency.
- Fabricate or falsify evidence, citations, records, signatures, or documents, or submit AI-generated material to a court, agency, or other person as if it were verified when it has not been.
- Engage in or facilitate fraud, money laundering, identity theft, or any other crime.
- Exploit or harm minors, including by uploading child sexual abuse material. Where the law requires, we will report such material to the appropriate authorities.
- Send unsolicited bulk messages through any Service feature.

3. Content you upload

3.1 Your right to upload. Upload only content that you have the right to upload and to process with the Service — for example, documents you or your client lawfully possess for a representation, or that were produced to you in that representation. You are responsible for any protective order, confidentiality agreement, applicable rule, or client instruction that limits how particular documents may be used or disclosed, and for deciding whether those documents may be processed by the Service and its subprocessors.

3.2 Medical records and protected health information. You may upload medical records and other health information that you or your client lawfully hold for a matter, and that you have the right to process with the Service and its subprocessors. You may not upload protected health information in the capacity of a HIPAA covered entity or business associate unless you and Jubal have signed a business associate agreement covering that use. Jubal will enter into a business associate agreement with a firm that asks for one, by writing to legal@jubal.law.

A matter that is not marked as containing protected health information is treated as not containing it, except that a personal-injury matter is treated as containing it unless you state that it does not. You are responsible for marking matters that contain protected health information. Marking a matter does not make the Service suitable for protected health information.

Do not upload psychotherapy notes. Do not upload substance-use disorder treatment records that you are not authorized to redisclose. Those uploads require Jubal's prior written agreement, which Jubal may decline.

3.3 Other regulated data. Do not upload data subject to export controls, classified information, or payment-card data (card numbers with security codes) unless it is part of a matter record and you have confirmed that doing so is lawful and permitted by the rules that govern that data.

4. Security and system integrity

You may not, and may not help anyone else to:

- Upload or transmit malware, viruses, worms, ransomware, or any other harmful code.
- Probe, scan, or test the vulnerability of the Service or any system or network connected to it, or breach or circumvent any security or authentication measure, without Jubal's prior written permission. Security researchers: see Section 8.
- Access, or try to access, any account, matter, firm, data, or system you are not authorized to access, including other customers' data.
- Interfere with or disrupt the Service, its servers or networks, or other customers' use of it, including by denial-of-service attacks or by sending requests at a volume designed to degrade it.
- Attempt to break out of, disable, or circumvent the sandbox in which Jubal's desktop agent runs commands, or use the Service to reach network destinations the Service does not itself offer.
- Tamper with, modify, or bypass the Jubal desktop application's update, licensing, sign-in, or security mechanisms.

5. Accounts and access

You may not:

- Share sign-in credentials, passkeys, or sessions between people. Each Authorized User must have and use their own account.
- Create accounts with false information, impersonate any person, or misrepresent your affiliation with a firm.
- Sell, resell, sublicense, rent, or lease access to the Service, or provide it to anyone outside the Customer, except as the Terms expressly permit (for example, inviting guests or view-only users through the features Jubal provides).
- Use a view-only seat or any free seat to do work that requires a paid seat, or otherwise disguise who is doing the work.

6. Limits, trials, and fair use

6.1 Usage limits. The Service has limits — for example, usage allowances per seat, a spending ceiling per firm, request-rate limits, and the limits that apply during a Free Trial (number of people, number of matters, and AI usage). You may not circumvent, or attempt to circumvent, any of these limits, including by splitting one firm into several accounts, creating additional accounts, or manipulating seat types.

6.2 One trial per firm. Each firm may receive one Free Trial. You may not request or use more than one Free Trial for the same firm, including by using different email domains, different firm names, or different people. Jubal may decline or end any trial it believes is a duplicate. Jubal currently limits trials to one per work email domain.

6.3 Rate and abuse limits. We may throttle, queue, or refuse requests that exceed reasonable limits or that we believe are automated abuse.

7. The models, the software, and competition

You may not, and may not help anyone else to:

- Reverse engineer, decompile, disassemble, or try to derive the source code, models, prompts, or underlying structure of the Service, except to the extent applicable law expressly permits it despite this restriction.
- Attempt to extract, reproduce, or disclose Jubal's system prompts, skills, instructions, model configurations, or the weights or parameters of any model used by the Service, including through prompt injection or jailbreak techniques.
- Use the Service, or any output of it, to develop, train, or improve a product or model that competes with the Service, or to benchmark the Service for publication without Jubal's written consent.
- Scrape, crawl, or harvest data from the Service by automated means, other than through the export features the Service provides.
- Copy, frame, or mirror any part of the Service.
- Remove or obscure any proprietary notice in the Service.
- Use the Service in violation of the usage policies of the model providers Jubal uses, as Jubal makes those policies available to you.

8. Reporting

8.1 Report misuse. If you become aware of a violation of this AUP, or of a security vulnerability, tell us promptly at security@jubal.law, or at hello@jubal.law for anything else.

8.2 Security research. Testing the Service requires Jubal's prior written permission under Section 4. Jubal has not adopted a vulnerability-disclosure policy.

9. Enforcement

9.1 What we may do. If we reasonably believe that the AUP has been violated, we may, as the circumstances reasonably require: investigate; warn the Customer; remove or disable access to specific content; throttle or suspend the AI features, a user, or the account; terminate the Terms under their termination provisions; and cooperate with law enforcement or report as the law requires.

9.2 Notice. Where practical and lawful, we will tell the Customer before we act, and give the Customer an opportunity to fix the problem. We may act without prior notice where we reasonably believe that immediate action is necessary to protect the Service, other customers, Jubal, or any person, or to comply with law.

9.3 How we investigate. Jubal investigates primarily from usage, billing, audit, and security records, which do not contain document content. Where an investigation requires access to Customer Content, we will limit that access to what the investigation reasonably requires, as described in the Terms.

9.4 No duty to monitor. We are not obliged to monitor use of the Service or Customer Content. Not acting on a violation is not a waiver.

10. Changes

We may update this AUP as described in Section 16 of the Terms. The version and effective date are at the top of this policy.