JTAI

Acceptable Use Policy

Just-Tech, LLC

Effective Date: March 6, 2026

This Acceptable Use Policy ("AUP") governs access to and use of the JTAI Service (the "Service") provided by Just-Tech, LLC ("Just-Tech"). This AUP is incorporated by reference into the JTAI SaaS Subscription Agreement (the "Agreement"). Capitalized terms not defined herein have the meanings set forth in the Agreement.

Subscriber and its Authorized Users must comply with this AUP at all times when accessing or using the Service. Subscriber is responsible for all acts and omissions of its Authorized Users as if such acts and omissions were Subscriber's own.

1. Purpose and Scope

JTAI is an AI-powered knowledge platform designed to centralize institutional resources and provide streamlined access through AI features and a traditional archive interface.

The Service may be used solely for Permitted Use and in strict accordance with the Agreement, this AUP, and applicable Law. Any use of the Service not expressly authorized by the Agreement and this AUP is prohibited.

2. Prohibited Uses

Subscriber and its Authorized Users shall not use the Service to:

2.1 Violate Law or Rights

- Violate any applicable federal, state, local, or international Law.
- Infringe, misappropriate, or otherwise violate any Intellectual Property Rights, privacy rights, publicity rights, or other rights of any Person.
- Transmit or store material that is defamatory, fraudulent, deceptive, threatening, harassing, or otherwise unlawful.
- Impersonate Just-Tech, another Subscriber, any Authorized User, or any third party, or otherwise misrepresent Subscriber's identity or affiliation.

2.2 Improper Handling of Sensitive or Regulated Data

- Upload, input, or transmit regulated data unless Subscriber has independently determined that such use complies with applicable Law and all contractual and professional obligations.

- Use the Service to process protected health information subject to HIPAA, cardholder data subject to PCI-DSS, classified information, export-controlled technical data, or other regulated data categories, unless expressly authorized in writing by Just-Tech in the applicable Order.
- Transmit data to AI Features where Subscriber lacks the authority or required consent to do so under applicable Law, professional conduct rules, or contractual obligations.
- Upload or process attorney-client privileged communications, client confidential information, or other data subject to professional confidentiality obligations through the AI Features without evaluating the legal and ethical implications of doing so.

Subscriber bears sole responsibility for determining whether use of the Service for any specific category of data is appropriate and lawful.

2.3 Security Violations

- Attempt to gain unauthorized access to the Service, Just-Tech Systems, or any related systems or networks.
- Probe, scan, or test the vulnerability of the Service or any system or network without express written authorization from Just-Tech.
- Circumvent, disable, or interfere with security-related features or access controls.
- Share Access Credentials among multiple individuals or permit concurrent use of a Seat by more than one individual.
- Use another Authorized User's account or Access Credentials without authorization.
- Fail to promptly notify Just-Tech of any known or suspected unauthorized use of Access Credentials or security breach at support@jtai.law.

2.4 Interference and Abuse

- Use the Service in a manner that interferes with or disrupts the integrity, availability, or performance of the Service or any third-party systems.
- Introduce viruses, malware, Trojan horses, ransomware, spyware, or other malicious or harmful code.
- Use automated means, including bots, scrapers, or scripts, to access or extract data from the Service, except through approved APIs in accordance with the Documentation.
- Exceed Usage Limits specified in the applicable Order or attempt to bypass usage controls.
- Take any action that places an unreasonable or disproportionate load on Just-Tech Systems.

2.5 Competitive and Reverse Engineering Misuse

- Reverse engineer, decompile, disassemble, or attempt to derive the source code, underlying models, or architecture of the Service.
- Use the Service or Service Output to develop, train, fine-tune, benchmark, or validate a competing product or service.
- Publish or disclose performance benchmarking or evaluation results without Just-Tech's prior written consent.

2.6 AI Feature Misuse

Subscriber and Authorized Users shall not use AI Features to:

- Generate content for unlawful, fraudulent, or deceptive purposes.
- Create or distribute malicious code.

- Generate content intended to harass, threaten, defame, or impersonate others.
- Craft inputs designed to bypass AI safeguards, filtering mechanisms, or content controls ("prompt injection" or "jailbreaking").
- Rely on AI Subscriber Output as a substitute for professional legal, financial, medical, or other regulated advice without independent human review and verification.
- Disable, circumvent, or bypass any source citation, filtering, or safety tools or functions built into the AI Features.

Subscriber is solely responsible for reviewing and independently validating AI Subscriber Output prior to any use or distribution. AI Subscriber Output does not constitute legal, business, financial, or other professional advice and should not be relied upon as such.

2.7 Unauthorized Commercialization

- Resell, sublicense, distribute, or otherwise make the Service available to third parties except as expressly permitted in the Agreement.
- Operate the Service as a service bureau or outsourced platform for third parties.

2.8 Geographic and Sanctions Restrictions

- Access or use the Service from any location outside of the United States, or permit such access, without Just-Tech's prior written authorization.
- Access or use the Service in violation of U.S. export control or sanctions Laws.
- Permit access to the Service by any individual, entity, or jurisdiction subject to U.S. economic sanctions or embargoes.

3. Data and Content Responsibility

Subscriber represents and warrants that it has all rights, permissions, and consents necessary to upload and process Subscriber Data through the Service and, where applicable, through Licensor-Facilitated AI Providers.

Subscriber is solely responsible for:

- The legality, accuracy, quality, and appropriateness of all Subscriber Data.
- The independent review, validation, and appropriate use of all Service Output, including AI Subscriber Output.
- Maintaining adequate backup copies of all Subscriber Data and Service Output. Just-Tech has no liability for loss, corruption, deletion, or unavailability of Subscriber Data or Service Output regardless of cause.
- Obtaining any legally required consents or authorizations prior to transmitting Subscriber Data to Licensor-Facilitated AI Providers through the AI Features.
- Reviewing and understanding the terms, policies, and data handling practices of any applicable Licensor-Facilitated AI Provider. Just-Tech makes no representations or warranties regarding the terms or practices of any such provider.

Just-Tech does not monitor Subscriber Data as a matter of course but reserves the right to investigate suspected violations of this AUP.

4. Authorized User Oversight

Subscriber is responsible for ensuring that all Authorized Users are aware of and comply with this AUP and the Agreement. Subscriber shall:

- Provide adequate training and guidance to Authorized Users on the appropriate and compliant use of the Service, including the limitations of AI-generated output.
- Maintain appropriate internal policies, access controls, and oversight mechanisms to prevent unauthorized or non-compliant use of the Service.
- Promptly revoke Service access for any individual who is no longer an Authorized User, including upon termination of employment or engagement.
- Promptly investigate and remediate any suspected violation of this AUP by an Authorized User.
- Promptly notify Just-Tech of any known or suspected violation of this AUP or the Agreement at support@jtai.law.

5. Enforcement

Just-Tech may investigate suspected violations of this AUP. If Just-Tech determines, in its reasonable judgment, that Subscriber or any Authorized User has violated this AUP, Just-Tech may take one or more of the following actions:

- Issue a written warning to Subscriber.
- Suspend or restrict Subscriber's or an Authorized User's access to all or any portion of the Service.
- Remove or disable access to specific Subscriber Data.
- Terminate access to the Service in accordance with the Agreement.
- Report unlawful conduct to appropriate governmental or regulatory authorities.

Just-Tech may take immediate action without prior notice where necessary to protect the security, integrity, or availability of the Service or Just-Tech Systems, or to comply with applicable Law. Just-Tech shall have no liability for any damages or losses resulting from enforcement actions taken in good faith under this AUP.

6. Reporting Violations

Suspected violations of this AUP, security vulnerabilities, or other concerns related to the Service should be reported to Just-Tech as follows:

Email: support@jtai.law
Address: Just-Tech, LLC, 1345 Avenue of the Americas, 2nd Floor, New York, NY 10105
Hours: 9:00 AM – 5:00 PM Eastern Time, Monday through Friday (excluding U.S. federal holidays)

Just-Tech does not guarantee a specific response time. Reports should include a description of the suspected violation, the affected system or data (if known), and contact information for follow-up.

7. Modifications

Just-Tech may update this AUP from time to time by posting a revised version to the applicable URL specified in the Agreement. Updates become effective upon posting or such later date as specified in the updated AUP. Just-Tech will use commercially reasonable efforts to provide advance notice of material changes. Continued use of the Service following the effective date of any update constitutes Subscriber's acceptance of the revised AUP.

— *End of Acceptable Use Policy* —