



## Acceptable Use Policy

THIS ACCEPTABLE USE POLICY CONTAINS LEGALLY BINDING TERMS APPLICABLE TO YOUR USE OF ALL SOFTWARE, PRODUCTS, AND SERVICES OFFERED BY JAMA SOFTWARE, INC. ("JAMA"). IF YOU DO NOT AGREE TO THESE TERMS, YOU MAY NOT USE THESE PRODUCTS.

This Acceptable Use Policy ("AUP") applies to all Jama customers (each a "Customer," "you," or "your") use of any software, products, and services offered by Jama, whether directly or through a reseller (collectively "Products"). This AUP is incorporated by reference into your Agreement with Jama. Jama may update this AUP at any time by posting a revised version at [www.jamasoftware.com/legal](http://www.jamasoftware.com/legal), effective immediately upon posting. Violation of this AUP constitutes a material breach of your Agreement with Jama. Jama's suppliers, including without limitation, Oracle Corporation, are third-party beneficiaries of this AUP and your Agreement.

Customer shall use the Products only in compliance with applicable laws and regulations, including without limitation, export and import laws and regulations. The prohibited uses described below are general guidelines regarding improper conduct and use of the Products and should not be interpreted as exhaustive. Any capitalized terms not defined herein have the meaning given in your Agreement.

### PROHIBITED USES AND CONTENT

Customer may not, and may not allow any third party, including its Users, to use the Product(s) to upload, display, distribute, retrieve, store, process or transmit:

- Material that infringes or misappropriates a third party's publicity, privacy, or proprietary rights;
- Hate-related, violent, discriminatory, harassing, defamatory, or abusive material, or material advocating the foregoing against individuals or groups;
- Obscene, excessively profane, or otherwise objectionable material;
- Fraudulent material or material advocating or advancing criminal hacking, cracking, or phishing;
- Material related to illegal drugs or paraphernalia;
- Unlawful software or material that violates applicable laws, including export control laws;
- Malicious material or code, such as viruses, worms, time bombs, Trojan horses, spyware, malware, corrupted files, hoaxes and other harmful or malicious files, scripts, agents or programs or other items of a destructive or deceptive nature;
- Health information, including, without limitation, information protected under the privacy or security regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 or subject to the Health Information Technology for Economic and Clinical Health Act;
- Financial information, including, without limitation, bank, checking, credit card, debit card, financial, or other personal account numbers; or
- Other sensitive personal data, including without limitation, drivers license, passport, social security, tax ID or similar numbers.

Customer may not use a Product to, nor allow its Users or any third-party to use a Product to:

- Generate or facilitate unsolicited commercial email (spam), including but not limited to:
  - violating anti-spam laws (including CAN-SPAM Act), sending to users who requested removal, or sending unsolicited emails to recipients with whom you have no preexisting relationship;
  - data mining or harvesting any web property to find email addresses or account information; OR
  - sending unauthorized mail via open third-party servers;
- Conduct or forward multi-level marketing, such as pyramid schemes and the like;
- Solicit a customer from, or collect replies to messages sent from, another Internet Service Provider where those messages violate this AUP or terms of service of any such provider;
- Generate or facilitate SMS, MM.S, or other text messages or push notifications in violation of the Telephone Consumer Protection Act, the Do-Not-Call Implementation Act, or any other applicable law including anti- spam, telemarketing or telephone consumer protection laws or regulations;
- Engage in activity or transmit material that may be harmful to minors, including content that promotes child sexual exploitation or abuse;

- Violate security, integrity or availability of any user, system, computer, software application, network or computing device, including without limitation: gaining unauthorized access to, or attempting to compromise the normal functioning, operation or security of any account, password, network, system, computing facility, equipment, data or information; engaging in any activities or behavior that may interfere with the ability of others to access or use the Product(s) or the Internet; monitoring any data, information or communications on any network or system not owned by you without authorization; attempting to intercept, redirect or otherwise interfere with communications intended for others; collecting or using email addresses, screen names or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting).
- Fraudulently conceal, forge, or otherwise falsify your identity, alter your source IP address or use forged headers or otherwise misrepresent the source of any communication;
- Violate applicable law or promote, facilitate or encourage illegal activity;
- Interfere with other users' enjoyment of a service;
- Engage in prohibited financial activities, including gambling operations or cryptocurrency mining;
- Access (including through any interfaces provided with a Product), any Product or other service or website, in a manner that violates the terms for use of or access to such Product, service or website;
- Engage in automated access activities, including operating open proxies or web scraping/crawling without proper identification and robots.txt compliance;
- Perform load, benchmarking, penetration, vulnerability, probing, scanning, or security testing without first obtaining Jama's written consent, and if Jama consents the results of such tests may not be published without express written consent;
- Remove any copyright, trademark or other proprietary rights notices contained in or on the Product or reformat or frame any portion of the web pages that are part of the Product;
- Threaten, incite, promote, or actively encourage violence, terrorism, or other serious harm;
- Decompile, disassemble, reverse engineer or otherwise attempt to discover the source code of or trade secrets embodied in the Product or to circumvent license control mechanisms;
- Distribute, lend, lease, sell, transfer, grant sublicenses to, or otherwise make available the Product (or any portion thereof) to parties other than authorized Users;
- Create modifications to or derivative works of the Product(s);
- Develop, promote, distribute, sell or support any product or service that is competitive with any Product; or
- Use a Product in any manner that would disparage Jama.

### THIRD-PARTY TOOL INTEGRATION

Any non-Jama software that accesses the Software through API integration or any other means must be assigned a dedicated Named User license. Any artificial intelligence tool (meaning artificial intelligence software, service, application, bot or similar technology) that is not provided by Jama which Customer integrates with the Software requires: (a) a separate Named User license for each such artificial intelligence tool; (b) a separate Named User license for each individual User who access, uses, or interacts with the Software through such integration, regardless of whether such access is direct or indirect. Customer is responsible for ensuring proper license allocation and compliance.

### USAGE DATA

Jama may monitor, collect and use data pertaining to use of the Products. No such data will be disclosed to a third party except in anonymous, aggregated form.

### COOPERATION WITH INVESTIGATIONS

Jama may investigate suspected AUP violations and remove or disable violating content or Users. You agree to cooperate with investigations and assist when requested. Jama will not disclose your data to third parties without your consent, except as required by law. Jama will cooperate with law enforcement and governmental agencies investigating illegal activity and has no liability for such cooperation.

### VIOLATIONS

Jama may take down, delete and/or block access to any Customer Content within the Cloud Software that violates this AUP. You must immediately notify Jama via e-mail at [legal@jamasoftware.com](mailto:legal@jamasoftware.com) of any AUP violation.

If you have questions or concerns related to this AUP, please contact us at [legal@jamasoftware.com](mailto:legal@jamasoftware.com).