

Acceptable Use Policy

VB-AUP | Vera AI | Version 1.0 | Effective July 2026

VendorBenchmark LLC · 1007 N Orange St, 4th Floor, Suite #5951, Wilmington, Delaware 19801, United States

The rules for using Vera AI responsibly: prohibited content and conduct, fair use, AI-feature use, security cooperation, and enforcement. Incorporated into the Master Subscription Agreement.

BACKGROUND

This Acceptable Use Policy (this Policy) is incorporated into the Master Subscription Agreement (the Agreement) and applies to every user of the Service. It exists to keep the Service secure, lawful, and reliable for all customers. Capitalized terms not defined here have the meaning given in the Agreement.

1. PROHIBITED CONTENT

1.1 The Customer will not upload to or process through the Service any content that:

- (a) is unlawful, defamatory, or infringes a third party's intellectual property, privacy, or other rights,
- (b) the Customer has no right or authority to submit, or that violates an obligation of confidence the Customer owes to another,
- (c) contains Malicious Code, or
- (d) consists of special-category personal data that the Service does not require and that the Customer has no lawful basis to process through it.

1.2 The Customer controls what it uploads and is responsible for having the rights and lawful basis to do so.

2. PROHIBITED CONDUCT

2.1 The Customer and its Authorized Users will not:

- (a) attempt to breach tenant isolation or otherwise access data belonging to another organization,
- (b) probe, scan, or test the vulnerability of the Service, or circumvent its security, authentication, or usage limits, except under a testing agreement the Provider has authorized in writing,
- (c) resell, sublicense, rent, time-share, or share access to the Service outside the Customer's organization and its Affiliates without the Provider's written agreement,
- (d) reverse engineer, decompile, or attempt to derive the source code or models of the Service, except to the extent the law permits despite this restriction,
- (e) use automated means to access the Service other than through the APIs the Provider provides and within their documented limits,
- (f) use the Service to build or train a competing benchmarking dataset or product, or to benchmark the Service for a competitor,
- (g) introduce Malicious Code, or interfere with or place an undue load on the integrity or performance of the Service.

3. FAIR USE AND RATE LIMITS

3.1 The Service and its APIs are subject to documented rate limits and fair-use expectations that protect availability for all customers. The Provider may throttle or temporarily limit usage that materially exceeds those limits or

degrades the Service for others, and will work with the Customer on a plan that fits genuine high-volume needs.

4. USE OF AI FEATURES

4.1 The Service includes AI features that produce benchmarks, analyses, and drafts. The Customer will:

- (a) submit only content it has the right to submit and process,
- (b) treat outputs as decision support rather than legal, financial, or professional advice, and apply human review before relying on them,
- (c) not present outputs as the Provider's certification or guarantee of a commercial outcome, and
- (d) not use the Service or its outputs to mislead, or in a way that infringes a third party's rights.

5. SECURITY COOPERATION

5.1 The Customer will keep credentials confidential, enable multi-factor authentication where its security posture requires it, and promptly report any suspected compromise or vulnerability to the Provider. The Customer will not disclose a vulnerability publicly before the Provider has had a reasonable opportunity to address it.

6. ENFORCEMENT

6.1 The Provider may suspend access that presents a security risk, may harm the Service or other customers, or materially breaches this Policy. Where practical the Provider gives notice first and works with the Customer to resolve the issue; where a threat is active the Provider may act first and inform the Customer promptly, limiting the scope and duration of any suspension. Repeated or severe breaches may lead to termination under the Agreement.

7. REPORTING

7.1 Suspected abuse or security issues may be reported to the Provider at security@vendorbenchmark.com. The Provider investigates reports and responds to the reporter where appropriate.

8. CHANGES TO THIS POLICY

8.1 The Provider may update this Policy as the Service and the threat landscape evolve. Material changes are posted with the agreements and take effect on notice; continued use of the Service after the effective date is acceptance.

This Policy forms part of the Master Subscription Agreement and may be updated as the Service evolves.

Any questions about this document go to legal@vendorbenchmark.com.