

Acceptable Use Policy

Version 1.0

Approved publication

Effective Date: April 15, 2026

1. Overview

This Acceptable Use Policy ("AUP") governs your use of the mAlvn Developer Platform (the "Service") provided by mAlvn, LLC ("mAlvn," "we," "us," or "our"). This AUP supplements our [Terms of Service](#) and is incorporated therein by reference.

The Service orchestrates AI agents across multiple large language model (LLM) providers. Your use of the Service is subject not only to this AUP but also to the acceptable use policies, terms of service, and usage policies of each upstream LLM provider whose models you access through the Service. Violations of upstream provider policies may result in immediate suspension or termination of your access.

2. Upstream LLM Provider Policies

The Service currently integrates with the following LLM providers. You are responsible for reviewing and complying with each provider's usage policies for any models you use through the Service:

2.1 OpenAI

Models: GPT-4.1 series, GPT-5 series, o3, o4-mini, Codex models. Your use of OpenAI models through the Service is subject to the [OpenAI Usage Policies](#). Key restrictions include prohibitions on generating content that exploits minors, developing weapons, conducting surveillance, and generating deceptive content.

2.2 Anthropic

Models: Claude Haiku 4.5, Claude Sonnet 4/4.5/4.6, Claude Opus 4.5/4.6. Your use of Anthropic models through the Service is subject to the [Anthropic Acceptable Use Policy](#). Key restrictions include prohibitions on generating CSAM, creating biological or chemical weapons, conducting cyberattacks, and undermining AI safety mechanisms.

2.3 Google (Gemini)

Models: Gemini 2.0/2.5/3/3.1 Flash and Pro series. Your use of Google models through the Service is subject to the [Google Gemini API Terms of Service](#) and the [Google Generative AI Prohibited Use Policy](#). Key restrictions include prohibitions on generating misleading content, facilitating illegal activities, and creating harmful or deceptive applications.

2.4 Mistral AI

Models: Mistral Small 3.1, Mistral Medium 3, Mistral Large, Codestral. Your use of Mistral AI models through the Service is subject to the [Mistral AI Terms of Use](#). Key restrictions include prohibitions on generating illegal content, infringing intellectual property rights, and creating deceptive or manipulative systems.

2.5 xAI (Grok)

Models: Grok 3 Mini, Grok 4 series, Grok 4.1 series, Grok 4.20 Beta, Grok Code Fast. Your use of xAI models through the Service is subject to the [xAI Terms of Service](#). Key restrictions include prohibitions on generating harmful content, facilitating illegal activities, and circumventing safety measures.

2.6 Future Providers and Models

The providers and models listed above reflect the Service's current integrations. We may add, remove, or replace LLM providers and models at any time without amending this AUP. **When you access any model through the Service, you are automatically bound by that model's provider usage policies, whether or not the provider is explicitly named in this document.** This includes providers added after the effective date of this AUP.

It is your responsibility to identify which LLM providers power the models you use through the Service, to review their respective usage policies, and to monitor those policies for changes. mAlvn is not responsible for notifying you of changes to upstream provider policies.

If an upstream provider's usage policies conflict with this AUP, the more restrictive policy applies. If you are uncertain whether a specific use case is permitted under an upstream provider's policies, you should refrain from that use or contact us for guidance.

3. Universally Prohibited Uses

Regardless of which LLM provider or model you use through the Service, the following uses are strictly prohibited. You shall not use the Service to:

3.1 Illegal Activities

- Violate any applicable federal, state, local, or international law or regulation;
- Facilitate or promote any criminal activity, including fraud, money laundering, terrorism financing, or human trafficking;
- Generate, distribute, or facilitate access to child sexual abuse material (CSAM) or any content that sexually exploits minors;
- Violate U.S. export control laws, sanctions programs, or other trade restrictions.

3.2 Weapons and Violence

- Develop, improve, or proliferate biological, chemical, nuclear, or radiological weapons or related materials;
- Create instructions for manufacturing weapons, explosives, or dangerous materials;
- Generate content that promotes, glorifies, or incites violence against individuals or groups;
- Plan, coordinate, or facilitate acts of terrorism or mass violence.

3.3 Deception and Manipulation

- Generate deepfakes, synthetic media, or other content intended to deceive or mislead;
- Create or operate bots or agents that impersonate real individuals without their explicit consent;
- Conduct influence operations, disinformation campaigns, or election interference;
- Generate fraudulent academic work, fake reviews, or deceptive testimonials;
- Create phishing content, social engineering attacks, or scam communications.

3.4 Privacy and Surveillance

- Conduct unauthorized surveillance, tracking, or monitoring of individuals;
- Build facial recognition systems or biometric identification tools without proper authorization and consent;
- Aggregate, correlate, or deanonymize personal information without authorization;
- Scrape, harvest, or collect personal data in violation of applicable privacy laws.

3.5 Harm and Abuse

- Generate content that promotes self-harm, suicide, or eating disorders;
- Create content that harasses, bullies, intimidates, or threatens individuals;
- Generate hate speech or content that discriminates against protected groups;
- Produce non-consensual intimate imagery or sexually exploitative content;
- Provide unqualified medical, legal, or financial advice presented as professional guidance.

3.6 System Integrity

- Attempt to circumvent, disable, or interfere with safety measures, content filters, or usage restrictions of the Service or any upstream LLM provider;
- Engage in prompt injection attacks, jailbreaking, or other techniques designed to bypass model safety guardrails;
- Reverse-engineer, extract training data from, or attempt to replicate the models or algorithms of any LLM provider;
- Use the Service to develop tools or techniques for circumventing AI safety measures;
- Transmit malware, viruses, or malicious code through the Service;
- Conduct denial-of-service attacks or deliberately degrade service performance.

3.7 High-Risk Applications

- Use AI-generated outputs as the sole basis for decisions with significant legal, financial, or safety consequences without human review;
- Deploy AI agents in safety-critical systems (medical devices, autonomous vehicles, industrial control systems) without appropriate human oversight;
- Use the Service for automated decision-making that determines eligibility for credit, employment, housing, insurance, or education without human review and in violation of applicable laws;
- Deploy AI agents that autonomously execute financial transactions without appropriate human authorization and oversight.

4. AI Agent-Specific Requirements

Because the Service orchestrates autonomous AI agents, the following additional requirements apply:

- **Transparency:** You must clearly disclose to end users when they are interacting with an AI agent rather than a human;
- **Human Oversight:** You must implement appropriate human oversight mechanisms for any AI agent that takes consequential actions;

- **Scope Limitation:** You must configure agents with appropriate scope limitations to prevent unintended actions beyond their intended purpose;
- **Error Handling:** You must implement appropriate error handling and fallback mechanisms for agent failures;
- **Data Minimization:** Agents should only access and process the minimum data necessary for their intended function;
- **Audit Trail:** You should maintain adequate records of agent actions for accountability and debugging purposes;
- **Testing:** You must adequately test agents before deploying them in production environments where they interact with real users or data.

5. Content and Output Responsibilities

You are responsible for all content you submit to and all outputs generated through the Service. Specifically:

- You must review AI-generated outputs before publishing, distributing, or relying on them;
- You must not represent AI-generated content as being created by a human when doing so would be deceptive;
- You must ensure that AI-generated content complies with applicable intellectual property laws and does not infringe third-party rights;
- You are responsible for the accuracy and appropriateness of any AI-generated content you publish or distribute;
- You must not use the Service to generate content that violates the content policies of any platform where you intend to publish or distribute it.

6. Rate Limits and Fair Use

To ensure fair access for all users:

- You must comply with all rate limits, usage quotas, and resource restrictions associated with your subscription plan;
- You must not attempt to circumvent rate limits through multiple accounts, key rotation, or other evasive techniques;
- You must not use the Service in a manner that disproportionately consumes shared resources or degrades service quality for other users;
- Automated usage patterns that constitute abuse (e.g., excessive polling, unnecessary redundant requests) are prohibited.

7. Reporting Violations

If you become aware of any violation of this AUP, whether by yourself or another user, you should promptly report it to us at hello@maivn.io. We investigate all reports and take appropriate action, which may include content removal, account suspension, or termination.

8. Enforcement

We reserve the right to investigate and take appropriate action in response to violations of this AUP, including but not limited to:

- Issuing warnings for minor or first-time violations;
- Temporarily suspending your access to specific models or features;
- Permanently suspending or terminating your account;
- Removing content that violates this AUP;
- Reporting violations to law enforcement or upstream LLM providers as appropriate;
- Pursuing legal remedies for violations that cause harm to mAlvn, its users, or third parties.

Upstream LLM providers may also independently enforce their usage policies, which may result in loss of access to specific models regardless of mAlvn's enforcement actions.

9. Changes to This Policy

We may update this AUP from time to time to reflect changes in upstream provider policies, applicable laws, or our own practices. Material changes will be communicated through the Developer Portal or via email. Your continued use of the Service after changes take effect constitutes acceptance of the updated AUP.

We strongly recommend periodically reviewing the usage policies of the upstream LLM providers listed in Section 2, as those policies may change independently of this AUP.

10. Contact Information

For questions about this Acceptable Use Policy, to report violations, or for guidance on whether a specific use case is permitted, please contact us:

mAlvn, LLC

3368 100th St

Urbandale, IA 50322

United States

Email: hello@maivn.io