

# Sairis LLC Software Acceptable Use Policy

This Policy was last updated on June 1, 2025.

## 1. SCOPE

- 1.1. This Software Acceptable Use Policy ("Usage Policy") applies to Customer's use of all Services provided by Sairis LLC or its affiliates ("Sairis"), including web-based applications, platform tools, system interfaces, and any external-facing deployment of Services. Capitalized terms used but not defined in this Software Use Policy have the meaning set forth in the Main Services Agreement ("MSA").
- 1.2. This Software Use Policy is incorporated into and made part of the MSA and governs general use of the Sairis platform and software applications. For specific rules and restrictions relating to the use of artificial intelligence features, including generative AI and large language models, Customers must also comply with the Sairis Artificial Intelligence Acceptable Use Policy ("AI Policy"), available at <https://sairis.ai/legal> and within the Sairis User Help Center.
- 1.3. Sairis may enter into agreements with certain governmental or specialized commercial customers that include tailored use restrictions aligned to the customer's public mission, legal authorities, or regulatory obligations, provided that, in Sairis' reasonable judgment, such restrictions and associated safeguards are sufficient to mitigate the potential harms addressed in this Software Use Policy. Where applicable, these exceptions will be documented in the customer's contract or Order Form and must be approved by Sairis' legal or compliance team. In cases involving national security or law enforcement, Sairis reserves the right to enter into separate agreements that may supersede specific provisions of this Software Use Policy, provided such agreements include appropriate legal, ethical, and operational safeguards.

## 2. CHANGES TO THIS SOFTWARE USE POLICY

- 2.1. From time to time, Sairis may update this Software Use Policy to reflect changes in law, regulation, platform capabilities, or to address emerging risks. Sairis will make the updated Software Use Policy available at <https://www.sairis.ai/legal> and within the Sairis User Help Center accessible by users and administrators, and such updates will be effective upon posting.

## 3. VIOLATIONS

- 3.1. Any violation of this Software Use Policy by Customer or its Users will be considered a material breach of the MSA and may result in enforcement actions in accordance with this Software Use Policy and the terms of the MSA, including but not limited to warnings, temporary suspension of access, permanent suspension of user accounts, or termination of Services. Sairis will determine the appropriate enforcement action at its sole discretion based on the severity and frequency of the violation and in accordance with the applicable MSA. Sairis employs automated monitoring systems to detect policy violations and may cooperate with law enforcement authorities when violations involve illegal activities or threats to public safety.

## 4. PROHIBITED MATERIAL

- 4.1. Customer may not, and may not allow any third party (including its users) to use the Services to create, send, upload, display, store, process, or transmit any of the following content, nor may Customer permit others to do so using the Services:
  - A. Material that infringes or misappropriates a third party's intellectual property or proprietary rights;
  - B. Hate-related content or material that advocates discrimination against individuals or groups;
  - C. Material that advocates or promotes violence, terrorism, or violent extremism;
  - D. Obscene, excessively profane material or otherwise objectionable content;
  - E. Content that advocates or facilitates criminal hacking, cracking, or phishing activities;
  - F. Material related to illegal drugs or paraphernalia;
  - G. Malicious or deceptive content intended to harm, deceive, or mislead others;
  - H. Malicious code, such as viruses, worms, Trojan horses, time bombs, or other harmful scripts, agents, or programs;
  - I. Unlawful software or software designed for unauthorized surveillance or access; or
  - J. Content that violates, encourages, or furthers conduct that would violate any applicable laws or regulations, including criminal laws and third-party rights (such as privacy, publicity, or intellectual property rights).
- 4.2. Customers may not, and may not allow any third party, including its Users, to:
  - A. Deceive or mislead others by presenting AI-generated or automatically generated content as if it were authored by a human or an authoritative source, without clear disclosure;
  - B. Impersonate any person, company, organization, or entity, or misrepresent an affiliation with any of the foregoing;

- C. Publish, distribute, or promote false or misleading information about safety procedures, critical operations, legal or medical guidance, or other topics where reliance could cause harm to individuals, property, or public welfare;
- D. Use Services to generate or disseminate synthetic media (text, images, video, or audio) without appropriate context, disclosures, or legal rights to do so.

## 5. PROHIBITED ACTIONS

5.1. Customers may not use a service to, nor allow its users or any third party to use a service to:

5.1.1. Generate or facilitate unsolicited commercial email and other forms of commercial communications (spam).

Such prohibited activity includes, but is not limited to:

- A. Sending communications or email in violation of the CAN-SPAM Act or any other applicable anti-spam law or regulation;
  - B. Imitating or impersonating Sairis, another person or his, her, or its email address, or creating false accounts for the purpose of sending spam;
  - C. Mining data or harvesting any web property (including any External-Facing Service) to find email addresses or other user account information;
  - D. Sending unauthorized mail via open, third-party servers;
  - E. Sending email to users who have requested to be removed from a mailing list;
  - F. Selling to, exchanging with, sharing with, or distributing to a third party personal information, including the email addresses of any person without such person's knowing and continued consent to such disclosure; or
  - G. Sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no preexisting relationship;
- 5.1.2. Create, send, upload, display, store, process, or transmit material that is unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, excessively profane, hateful, violent, or otherwise objectionable, or use the Services to send, display, or transmit sexually explicit material;
  - 5.1.3. Create, send, upload, display, store, process, or transmit highly deceptive manipulated or synthetic digital media that is fabricated or false but presented as authentic or fact-based and intended to deliberately sway audiences toward a specific interest or agenda, including, but not limited to, deepfakes;
  - 5.1.4. Promote, support, or facilitate unlawful, hateful, discriminatory, or violent causes, including terrorism or violent extremism;
  - 5.1.5. Intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;
  - 5.1.6. Conduct or forward multi-level marketing, such as pyramid schemes and the like;
  - 5.1.7. Generate or facilitate SMS, MMS, other text messages, push notifications, or other uninvited communications in violation of the Telephone Consumer Protection Act, the Do-Not-Call Implementation Act, or any other applicable law including anti-spam, telemarketing, robocalling, caller ID spoofing, or telephone consumer protection laws or regulations;
  - 5.1.8. Use the Services in any manner that violates applicable industry standards, third-party policies, or requirements that Sairis may communicate to its users, including all applicable guidelines published by the CTIA, the Mobile Marketing Association, the Self-Regulatory Principles as directed by the Digital Advertising Alliance and the Network Advertising Initiative, or other generally accepted industry associations, carrier guidelines, or other industry standards;
  - 5.1.9. Create, send, upload, display, store, process, or transmit material that may be harmful to minors including, but not limited to, for any purposes related to child exploitation or abuse, such as real or artificial Child Sexual Abuse Material (CSAM);
  - 5.1.10. Illegally send, upload, display, store, process, or transmit another's intellectual property or other proprietary information without such owner's or licensor's permission;
  - 5.1.11. Impersonate another person, entity, or Sairis (via the use of an email address or otherwise) or otherwise misrepresent themselves or the source of any communication;
  - 5.1.12. Facilitate or engage in coordinated inauthentic behavior for the purposes of manipulating public debate;
  - 5.1.13. Violate the rights (such as rights of privacy or publicity) of others;
  - 5.1.14. Promote, facilitate, or encourage illegal activity;
  - 5.1.15. Intentionally or unintentionally interfere with the availability of the service for other users, including, but not limited to, engaging in usage practices prohibited by the Documentation;
  - 5.1.16. Mislead people about voting processes or census processes;
  - 5.1.17. Engage in activity in connection with illegal peer-to-peer file sharing;
  - 5.1.18. Engage in or promote gambling, or run a gambling operation;
  - 5.1.19. "Mine" bitcoins and other cryptocurrencies;
  - 5.1.20. Sell, distribute, or export illegal or prescription drugs or other controlled substances or paraphernalia;
  - 5.1.21. Operate an "open proxy" or any other form of Internet proxy service that is capable of forwarding requests to any end user or third-party-supplied Internet host;

- 5.1.22. Perform significant load or security testing without first obtaining Sairis' written consent;
- 5.1.23. Remove any copyright, trademark, or other proprietary rights notices contained in or on the service or reformat or frame any portion of the web pages that are part of the service's administration display;
- 5.1.24. Access a third-party web property for the purposes of web scraping, web crawling, web monitoring, or other similar activity through a web client that does not take commercially reasonable efforts to identify itself via a unique User Agent string describing the purpose of the web client and obey the robots exclusion standard (also known as the robots.txt standard), including the crawl-delay directive;
- 5.1.25. Use a service in any manner that would disparage Sairis;
- 5.1.26. Directly manage, as the primary operator, private, for-profit prison facilities or detention centers in the United States. For-profit prisons and detention centers refer to privately owned facilities in which persons are incarcerated or otherwise involuntarily confined for purposes of execution of a punitive sentence imposed by a court or detention pending a trial, hearing, or other judicial or administrative proceeding;
- 5.1.27. Engage in high risk activity where the use or failure of a service may result in the death or serious bodily harm of a person, or in significant damage to property;
- 5.1.28. Abuse platform infrastructure or technical resources, including but not limited to:
  - A. Exceed documented API rate limits or usage quotas without prior authorization;
  - B. Engage in resource consumption patterns designed to degrade platform performance for other users;
  - C. Attempt to reverse engineer platform functionality, proprietary algorithms, or system architecture;
  - D. Systematically extract data for competitive intelligence purposes or unauthorized bulk data exports;
  - E. Circumvent technical limitations or platform restrictions through automated means.

## 5.2. Firearms Restrictions

- 5.2.1. Worldwide, customers may not use a service to commercially advertise or sell any of the following firearms and/or related accessories to private citizens, including:
- 5.2.2. **Firearms:** automatic firearms; semi-automatic firearms that have the capacity to accept a detachable magazine and any of the following: thumbhole stock, folding or telescoping stock, grenade launcher or flare launcher, flash or sound suppressor, forward pistol grip, pistol grip (in the case of a rifle) or second pistol grip (in the case of a pistol), barrel shroud; semi-automatic firearms with a fixed magazine that can accept more than 10 rounds; ghost guns; 3D printed guns; firearms without serial numbers; .50 BMG rifles; firearms that use .50 BMG ammunition.
- 5.2.3. **Firearm Parts:** magazines capable of accepting more than 10 rounds; flash or sound suppressors; multi-burst trigger devices; grenade or rocket launchers; 80% or unfinished lower receivers; blueprints for ghost guns; blueprints for 3D printed guns; barrel shrouds; thumbhole stocks; threaded barrels capable of accepting a flash suppressor or sound suppressor.

## 6. U.S. DIGITAL MILLENNIUM COPYRIGHT ACT OR SIMILAR STATUTORY OBLIGATIONS

- 6.1. To the extent a customer uses the services for hosting, advertising, sending electronic messages, or for the creation and hosting of, or for posting material on, websites, each customer must:
  - 6.1.1. Comply with any notices received under Title II of the Digital Millennium Copyright Act of 1998 (Section 512 of the U.S. Copyright Act) or similar statute in other countries (the "DMCA");
  - 6.1.2. Set up a process to expeditiously respond to notices of alleged infringement that comply with the DMCA and to implement a DMCA-compliant repeat infringers policy;
  - 6.1.3. Publicly display a description of its notice and takedown process under the DMCA on its instance of the services; and
  - 6.1.4. Comply with its published notice-and-takedown process and repeat infringer policy.
  - 6.1.5. When using Covered AI Services, Customers must take reasonable steps to ensure that AI-generated outputs do not infringe, misappropriate, or otherwise violate any third party's intellectual property rights, including copyrights, trademarks, or publicity rights.
- 6.2. It is Sairis' policy to respond expeditiously to valid notices of claimed copyright infringement compliant with the DMCA. In appropriate circumstances, Sairis will terminate the accounts of customers who Sairis reasonably believes to be repeatedly or blatantly infringing copyrights.
- 6.3. If Sairis receives a notice alleging that material on a customer's instance of a service infringes another party's intellectual property, Sairis may disable that customer's instance of the service or remove the allegedly infringing material. If Sairis receives more than one such notice for the same Customer, Sairis reserves the right to immediately terminate that Customer's subscriptions to the Services if necessary to maintain safe harbor protection under the DMCA or to prevent ongoing violations of law or third-party rights and in accordance with the applicable MSA.