Sairis LLC Artificial Intelligence Acceptable Use Policy

This Policy was last updated on June 1, 2025.

1. SCOPE

1.1. This Artificial Intelligence Acceptable Use Policy ("AI Policy") applies to Customer's use of all Services provided by Sairis LLC or its affiliates ("Sairis") that incorporate artificial intelligence, including generative AI capabilities, machine learning models, or large language models (collectively, "AI Models"), as well as any third-party products, applications, or functionality that interoperate with such Services (collectively, "Covered AI Services").

1.2. This AI Policy is incorporated into and made part of the Main Services Agreement ("MSA") and applies in addition to the Software Acceptable Use Policy ("Software Use Policy") available at https://sairis.ai/legal and also accessible to users and administrators in 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 AI 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 AI Policy, provided such agreements include appropriate legal, ethical, and operational safeguards.

2. CHANGES TO THIS AI POLICY

2.1. From time to time, Sairis may update this AI Policy to reflect changes in law, regulation, platform capabilities, or to address emerging risks. Sairis will make the updated AI 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. AI POLICY VIOLATIONS

3.1. Any violation of this AI Policy by Customer or its Users may result in enforcement actions in accordance with this AI Policy and the terms of the applicable 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 Main Services Agreement. Sairis employs automated detection and monitoring systems to enforce this AI Policy and may cooperate with law enforcement authorities when violations involve illegal activities or threats to public safety.

4. DISALLOWED USAGE

4.1. Customers may not use Sairis' products, including any Covered AI Services, or permit their users or any third party to use a Covered AI Service, for any of the following:

4.1.1. Automated Decision-Making Processes with Legal Effects

A. As part of an automated decision-making process with legal or similarly significant effects, unless Customer ensures that the final decision is made by a human being. In this case, Customer must take account of other factors beyond the Services' recommendations in making the final decision.

B. As part of an automated decision-making process for payday lending even when the final decision is made by a human being.

4.1.2. Individualized Advice from Licensed Professionals

A. Generating individualized advice that in the ordinary course of business would be provided by a licensed professional. This includes, for example, financial and legal advice.

B. Generating or providing individualized medical advice, treatment, or diagnosis to a consumer or end user.

For clarity, this section does not limit Customer from using Covered AI Services for other purposes, such as customer support in regulated industries, or to assist a licensed professional where Covered AI Services were not leveraged in the generation of individual advice. When a Customer uses such services to assist in providing individualized advice (e.g., summarization), there must be a qualified person reviewing the output.

4.1.3. Explicitly Predicting Protected Characteristics

A. Explicitly predicting an individual's protected characteristic, including, but not limited to, racial or ethnic origin, and past, current, or future political opinions, religious or philosophical beliefs, trade union membership, age, gender, sex life, sexual orientation, disability, health status, medical condition, financial status, criminal convictions, or likelihood to engage in criminal acts.

B. The previous sentence does not limit or prohibit use cases or tools designed specifically to identify security breaches, unauthorized access, fraud, and other security vulnerabilities, or to identify and reduce bias in Sairis AI Services.

C. Additionally, Customer may not submit images of individuals for the purposes of creating or analyzing biometric identifiers, such as face prints or fingerprints or scans of eyes, hands, or facial geometry.

4.1.4. Deceptive Activity

A. Engaging in plagiarism or academic dishonesty.

4.1.5. Child Exploitation and Abuse

A. Creating, sending, uploading, displaying, storing, processing, or transmitting 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).

B. Facilitate the trafficking, sextortion, or any other form of exploitation of a minor.

C. Facilitate minor grooming, including generating content designed to impersonate a minor.

D. Facilitate or depict child abuse of any form, including instructions for how to conceal abuse.

E. Promote or facilitate pedophilic relationships, including via roleplay with the model.

F. Fetishize minors.

Note that Sairis strictly prohibits and will report to relevant authorities and organizations where appropriate any content that exploits or abuses minors.

4.1.6. Compromise Critical Infrastructure

A. Facilitate the destruction or disruption of critical infrastructure such as power grids, water treatment facilities, telecommunication networks, or air traffic control systems.

B. Obtain unauthorized access to critical systems such as voting machines, healthcare databases, and financial markets.

C. Interfere with the operation of military bases and related infrastructure.

4.1.7. Compromise Computer or Network Systems

A. Discover or exploit vulnerabilities in systems, networks, or applications without authorization of the system owner.

B. Gain unauthorized access to systems, networks, applications, or devices through technical attacks or social engineering.

C. Create or distribute malware, ransomware, or other types of malicious code designed to harm, disrupt, or gain unauthorized access to computer systems.

D. Develop tools for denial-of-service attacks or managing botnets designed to overwhelm or compromise network resources.

E. Create tools designed to intercept communications or monitor devices without authorization of the system owner.

F. Develop persistent access tools designed to operate below normal system security levels, including firmware modifications or hardware implants.

G. Create automated tools designed to compromise multiple systems at scale for malicious purposes.

H. Bypass security controls such as authenticated systems, endpoint protection, or monitoring tools without proper authorization.

4.1.8. Incite Violence or Hateful Behavior

A. Incite, facilitate, or promote violent extremism, terrorism, or hateful behavior.

B. Depict support for organizations or individuals associated with violent extremism, terrorism, or hateful behavior.

C. Facilitate or promote any act of violence or intimidation targeting individuals, groups, animals, or property.

D. Promote discriminatory practices or behaviors against individuals or groups on the basis of one or more protected attributes such as race, ethnicity, religion, nationality, gender, sexual orientation, or any other identifying trait.

4.1.9. Compromise Someone's Privacy or Identity

A. Compromise security or gain unauthorized access to computer systems or networks, including spoofing and social engineering.
B. Violate the security, integrity, or availability of any user, network, computer, device, or communications system, software application, or network or computing device.
C. Violate any person's privacy rights as defined by applicable privacy laws, such as sharing personal information without consent, accessing private data unlawfully, or violating any relevant privacy regulations.
D. Misuse, collect, solicit, or gain access to private information without permission such as non-public contact details, health data, biometric or neural data (including facial recognition), or confidential or proprietary data.
E. Impersonate a human by presenting results as human-generated, or using results in a manner intended to convince a natural person that they are communicating with a natural person when they are not.

4.1.10. Intellectual Property Violations

A. Infringe, misappropriate, or violate the intellectual property rights of any third party, including but not limited to copyrights, trademarks, patents, or trade secrets.
B. Generate content that substantially reproduces copyrighted works without proper authorization or fair use justification.
C. Violate any other applicable laws or regulations in your jurisdiction.

4.1.11. Disclosures

A. Customers must disclose to end users when they are interacting directly with automated systems, such as AI Assistants, AI Agents, Blueprints, or similar features, unless there is a human in the loop, and when required by law, provide a means for end users to interact with a human instead of an automated system.

4.1.12. Weapons Development

A. Developing, advertising, marketing, distributing, or selling weapons, weapon accessories, or explosives, as enumerated by the United States Munitions List.
B. Produce, modify, design, market, or distribute weapons, explosives, dangerous materials or other systems designed to cause harm to or loss of human life.
C. Engage in or facilitate any illegal activity, such as the use, acquisition, or exchange of illegal and controlled substances, or the facilitation of human trafficking and prostitution.

4.1.13. Create Psychologically or Emotionally Harmful Content

A. Facilitate or conceal any form of self-harm, including disordered eating and unhealthy or compulsive exercise.
B. Engage in behaviors that promote unhealthy or unattainable body image or beauty standards, such as using the model to critique anyone's body shape or size.
C. Shame, humiliate, intimidate, bully, harass, or celebrate the suffering of individuals.
D. Coordinate the harassment or intimidation of an individual or group.
E. Generate content depicting animal cruelty or abuse.
F. Generate content depicting sexual violence.
G. Generate violent or gory content that is inspired by real acts of violence.
H. Promote, trivialize, or depict graphic violence or gratuitous gore.
I. Develop a product, or support an existing service that facilitates deceptive techniques with the intent of causing emotional harm.

4.1.14. Do Not Spread Misinformation

A. Create and disseminate deceptive or misleading information about a group, entity or person.
B. Create and disseminate deceptive or misleading information about laws, regulations, procedures, practices, standards established by an institution, entity or governing body.
C. Create and advance conspiratorial narratives meant to target a specific group, individual or entity.
D. Create and disseminate deceptive or misleading information with the intention of targeting specific groups or persons with the misleading content.
E. Impersonate real entities or create fake personas to falsely attribute content or mislead others about its origin without consent or legal right.
F. Provide false or misleading information related to medical, health or science issues.

4.1.15. Undermine Democratic Processes or Engage in Targeted Campaign Activities

A. Targeting, creating, or distributing political campaign materials for external public or semi-public audiences. Political campaign material refers to material: i. That may influence a political process, such as an election, passage of legislation, regulation or ballot measure, judicial ruling, and content for campaigning purposes; or

ii. Soliciting financial support for material that may influence a political process, such as an election, passage of legislation, regulation or ballot measure, judicial ruling, and content for campaigning purposes.

B. Promote or advocate for a particular political candidate, party, issue or position. This includes soliciting votes, financial contributions, or public support for a political entity.

C. Engage in political lobbying to actively influence the decisions of government officials, legislators, or regulatory agencies on legislative, regulatory, or policy matters. This includes advocacy or direct communication with officials or campaigns to sway public opinion on specific legislation or policies.

D. Engage in campaigns, including political campaigns, that promote false or misleading information to discredit or undermine individuals, groups, entities or institutions.

E. Incite, glorify or facilitate the disruption of electoral or civic processes, such as targeting voting machines, or obstructing the counting or certification of votes.

F. Generate false or misleading information on election laws, procedures and security, candidate information, how to participate, or discouraging participation in an election.

G. Engage in personalized vote or campaign targeting based on individual profiles or data.

H. Create artificial or deceptive political movements in which the source, scale or nature of the campaign or activities is misrepresented.

I. Generate automated communications to public officials or voters at scale that conceal their artificial origin, or engage in systematic vote solicitation that could undermine election integrity.

J. Create political content designed to deceive or mislead voters, including synthetic media of political figures.

K. Create content designed to suppress voter turnout or discourage legitimate political participation through deception or intimidation.

4.1.16. Criminal Justice, Law Enforcement, Censorship or Surveillance Purposes

A. Make determinations on criminal justice applications, including making decisions about or determining eligibility for parole or sentencing.

B. Target or track a person's physical location, emotional state, or communication without their consent, including using our products for facial recognition, battlefield management applications or predictive policing.

C. Utilize Sairis to assign scores or ratings to individuals based on an assessment of their trustworthiness or social behavior.

D. Build or support emotional recognition systems or techniques that are used to infer people's emotions.

E. Analyze or identify specific content to censor on behalf of a government organization.

F. Utilize Sairis as part of any biometric categorization system for categorizing people based on their biometric data to infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

G. Use Sairis for any official local, state or national law enforcement application. Except for the following permitted applications by law enforcement organizations: i. Back office uses including internal training, call center support, document summarization, and accounting; ii. Analysis of data for the location of missing persons, including in human trafficking cases, and other related applications, provided that such applications do not otherwise violate or impair the liberty, civil liberties, or human rights of natural persons.

4.1.17. Engage in Fraudulent, Abusive, or Predatory Practices

A. Facilitate the production, acquisition, or distribution of counterfeit or illicitly acquired goods.

B. Promote or facilitate the generation or distribution of spam.

C. Generate content for fraudulent activities, schemes, scams, phishing, or malware that can result in direct financial or psychological harm.

D. Generate content for the purposes of developing or promoting the sale or distribution of fraudulent or deceptive products.

E. Generate deceptive or misleading digital content such as fake reviews, comments, or media.

F. Engage in or facilitate multi-level marketing, pyramid schemes, or other deceptive business models that use high-pressure sales tactics or exploit participants.

G. Promote or facilitate payday loans, title loans, or other high-interest, short-term lending practices that exploit vulnerable individuals.

H. Engage in deceptive, abusive behaviors, practices, or campaigns that exploits people due to their age, disability or a specific social or economic situation.

I. Promote or facilitate the use of abusive or harassing debt collection practices.

J. Develop a product, or support an existing service that deploys subliminal, manipulative, or deceptive techniques to distort behavior by impairing decision-making.

K. Plagiarize or engage in academic dishonesty.

4.1.18. Abuse Our Platform

A. Coordinate malicious activity across multiple accounts to avoid detection or circumvent product guardrails or generating identical or similar inputs that otherwise violate this AI Policy.
B. Utilize automation in account creation or to engage in spammy behavior.
C. Circumvent a ban through the use of a different account, such as the creation of a new account, use of an existing account, or providing access to a person or entity that was previously banned.
D. Access or facilitate account or API access to Sairis services to persons, entities, or users in violation of applicable export controls or sanctions regulations.
E. Intentionally bypass capabilities, restrictions, or guardrails established within our products for the purposes of instructing the model to produce harmful outputs (e.g., jailbreaking or prompt injection) without prior authorization from Sairis.
F. Utilization of inputs and outputs to train an AI model (e.g., "model scraping" or "model distillation") without prior authorization from Sairis.
G. Engage in actions or behaviors that circumvent the guardrails or terms of other platforms or services.

4.1.19. Adult and Sexually Explicit Content

A. Creating, sending, uploading, displaying, storing, processing, or transmitting sexually explicit material.
B. Creating, sending, uploading, displaying, storing, processing, or transmitting sexual chatbots or engaging in erotic chat.
C. Depicting or requesting sexual intercourse or sex acts.
D. Generate content related to sexual fetishes or fantasies.
E. Facilitate, promote, or depict incest or bestiality.
F. Engage in erotic chats.

5. HIGH-RISK USE CASE REQUIREMENTS

5.1. Certain Use Cases involving our products and services may carry heightened potential for impact because they operate in domains that are vital to public welfare, human safety, and social equity. For the purpose of this section, a "Use Case" refers to the specific business process, decision, or function in which Sairis' services are deployed to inform or automate tasks. "High-Risk Use Cases" may require additional safeguards and include, but are not limited to, the following:

5.1.1. **Legal:** Use Cases related to legal interpretation, legal guidance, or decisions with legal implications.
5.1.2. **Healthcare:** Use Cases affecting healthcare decisions, medical diagnosis, patient care, or medical guidance. General wellness advice – such as content related to sleep, stress, nutrition, or fitness – is not considered a High-Risk Use Case, provided it is not positioned as a substitute for professional medical judgment.
5.1.3. **Insurance:** Use Cases related to health, life, property, disability, or other types of insurance underwriting, claims processing, or coverage decisions.
5.1.4. **Finance:** Use Cases related to financial decisions, including investment advice, loan approvals, and determining financial eligibility or creditworthiness.
5.1.5. **Employment and Housing:** Use Cases related to decisions about the employability of individuals, resume screening, hiring tools, or other employment determinations or decisions regarding eligibility for housing, including leases and home loans.
5.1.6. **Academic Testing, Accreditation, and Admissions:** Use Cases related to standardized testing companies that administer school admissions (including evaluating, scoring or ranking prospective students), language proficiency, or professional certification exams; agencies that evaluate and certify educational institutions.
5.1.7. **Media or Professional Journalistic Content:** Use Cases related to using our products or services to automatically generate or significantly assist in generating factual reporting, opinion articles, or other editorial content that is published externally and intended for broad public consumption. This does not include internal communications, marketing materials, or private content workflows.
5.1.8. **Industrial Safety and Operational Procedures:** Use Cases involving AI-generated outputs that directly support or inform decisions related to physical operations, safety procedures, equipment handling, hazardous material protocols, explosives management, or other frontline activities in high-risk industrial environments (such as mining, manufacturing, construction, or energy). These Use Cases may present elevated risk to human safety and must include clearly defined human-in-the-loop processes and safeguards to verify critical outputs before execution.
5.1.9. **Aerospace, Aviation, and Space Systems:** Use Cases that involve the development, operation, testing, or support of systems related to air travel, aerospace engineering, or space exploration. This includes but is not limited to flight planning, autopilot systems, aircraft diagnostics, satellite communications, launch operations, and mission-critical spaceflight procedures. Due to the potential for catastrophic consequences, all outputs from Covered AI Services in these domains must be reviewed and validated by appropriately certified aerospace or aviation professionals prior to any implementation or reliance.

5.1.10. **Autonomous Systems, Drones, and Robotics:** Use Cases involving the development, deployment, or operation of autonomous systems, including but not limited to drones, self-driving vehicles, industrial robots, robotic surgical tools, and other AI-controlled or non-human controlled machinery. These systems often interact directly with people, environments, or physical assets in ways that carry potential risk. Any outputs or instructions derived from Covered AI Services in these contexts must be subject to rigorous human oversight and validated by qualified technical professionals prior to real-world execution.

5.2. If your Use Case is listed above, we require that you implement the additional safety measures listed below:

5.2.1. **Human-in-the-loop:** when using our products or services to provide advice, recommendations, or subjective decisions that directly impact individuals, human safety, public safety, or outcomes in high-risk domains, a qualified professional in that field must review the content or decision prior to dissemination or finalization. This requirement applies specifically to content or decisions that are provided to consumers or the general public, or that may affect physical safety, operational performance, property or asset integrity, or human life. Your business is responsible for the accuracy and appropriateness of that information. For other types of content generation or interactions with users that do not involve direct advice, recommendations, or subjective decisions, human review is strongly encouraged but not mandatory.

5.2.2. **Disclosure:** you must disclose to your customers or end users, at or before the point of interaction, that they are interacting with an AI system or receiving AI-assisted outputs, such as those generated by Generative AI. This disclosure must be clear, understandable, and get prominently displayed, particularly in contexts where it may influence trust, legal compliance, decision-making, or the rights of individuals or consumers.

5.2.3. **Fallback Access and Offline Safety Protocols:** For High-Risk Use Cases where real-time access to AI-generated outputs is necessary for operational decisions (e.g., in frontline industrial environments), Customer must ensure that users in remote, offline, or low-bandwidth conditions have access to pre-validated procedures or fallback protocols. These protocols must not rely solely on dynamic AI responses and should be designed to ensure safety and continuity during connectivity disruptions.

6. AI INTERACTION DISCLOSURE REQUIREMENTS

6.1. The following Use Cases – regardless of whether they qualify as High Risk Use Cases – must include clear and timely disclosure to users that they are interacting with an AI system and not a human:

6.1.1. All customer-facing AI interfaces, including external-facing chatbots, AI assistants, or interactive agents intended to simulate human interaction.

6.1.2. Customers must not misrepresent AI-generated content as being authored or created by a human, or otherwise conceal the automated nature of the content, especially where such misrepresentation may influence trust, decisions, or regulatory compliance.

6.1.3. Products serving minors: Organizations providing minors with the ability to directly interact with products that incorporate Sairis Software, AI services, Generative AI services, or API(s). Note: These organizations must also comply with the following guidelines and implement the following safeguards:

A. **Additional Technical Measures:** Organizations must implement safety features tailored to their product's use by minors, including but not limited to: i. Age verification systems to ensure only intended users can access the product. ii. Content moderation and filtering to block inappropriate or harmful content. iii. Educational resources and guidance for minors on safe and responsible use of the product. iv. Monitoring and reporting mechanisms to identify and address potential issues.

In addition to these organization-specific measures, Sairis may make available technical measures intended to tailor product experiences for certain end users, including minors. For example, we may provide a child-safety system prompt, which organizations serving minors should implement as part of a comprehensive suite of safety measures. These technical safeguards are supportive but not foolproof, and should be combined with the organization's own safety protocols to ensure comprehensive protection for minors.

B. **Regulatory Compliance**: Organizations must comply with all applicable child safety and data privacy regulations, including COPPA in the United States and similar laws in other jurisdictions. It is the responsibility of organizations to comply with all applicable regulations.

C. **Disclosure Requirements**: Organizations must disclose to minor users and their parents or guardians that the user is interacting with an AI system rather than a human, and obtain appropriate parental or guardian authorization where required by law.

D. Sairis reserves the right to determine thresholds for acceptable usage and violation rates, and may take enforcement action where necessary to preserve the integrity, safety, and trustworthiness of the Services. If your organization has a high violation rate and has not implemented these safety recommendations, we may ask you to implement them.

Failure to implement these recommendations when requested, or a continued high violation rate, may lead to the suspension or termination of your account in accordance with the applicable Main Services Agreement.

7. NOTICES AND DISCLAIMERS

7.1. NOTICE OF HIGH-RISK USE. AI TECHNOLOGY, INCLUDING GENERATIVE AI, IS EVOLVING RAPIDLY AND MAY PRODUCE UNEXPECTED, INACCURATE, OR INAPPROPRIATE RESULTS. CUSTOMER ACKNOWLEDGES THIS RISK AND IS SOLELY RESPONSIBLE FOR DETERMINING WHETHER ITS USE OF AI TECHNOLOGIES IS SAFE, LEGALLY COMPLIANT, AND APPROPRIATE FOR ITS INTENDED BUSINESS PURPOSES AND OPERATIONAL ENVIRONMENT.

7.2. CUSTOMER RESPONSIBILITIES. CUSTOMER AGREES TO REVIEW AND VERIFY ALL AI-GENERATED OUTPUTS BEFORE RELYING ON THEM FOR ANY BUSINESS-CRITICAL DECISIONS, COMMUNICATIONS, OR OUTPUTS MADE AVAILABLE TO THIRD PARTIES. CUSTOMER IS RESPONSIBLE FOR ENSURING THAT ITS USE OF AI TECHNOLOGY COMPLIES WITH ALL APPLICABLE LAWS, REGULATIONS, AND ITS OWN INTERNAL POLICIES AND PROCEDURES. FOR USE CASES WHERE AI-GENERATED OUTPUTS SUPPORT OPERATIONAL DECISIONS IN FRONTLINE OR INDUSTRIAL ENVIRONMENTS, CUSTOMER IS RESPONSIBLE FOR ENSURING THAT APPROPRIATE FALLBACK PROTOCOLS OR PRE-VALIDATED PROCEDURES ARE AVAILABLE TO USERS IN LOW-BANDWIDTH OR OFFLINE CONDITIONS, WHERE ACCESS TO REAL-TIME AI RESPONSES MAY BE DISRUPTED.

7.3. LIMITATIONS OF LIABILITY. LIMITATIONS OF LIABILITY, DISCLAIMERS, AND INDEMNIFICATION OBLIGATIONS RELATED TO THE USE OF AI-GENERATED OUTPUTS ARE SET FORTH IN THE SAIRIS MAIN SERVICES AGREEMENT (MSA). THIS AI POLICY DOES NOT ALTER OR EXPAND THOSE CONTRACTUAL LIMITATIONS.

7.4. CUSTOMER RESPONSIBILITY FOR EMERGING USES. AI TECHNOLOGY, INCLUDING GENERATIVE AI, WILL CONTINUE TO BE USED IN NEW AND INNOVATIVE WAYS. CUSTOMER IS RESPONSIBLE FOR DETERMINING WHETHER ANY NEW OR EVOLVING USE CASES INVOLVING AI TECHNOLOGIES ALIGN WITH APPLICABLE LAWS, INDUSTRY-SPECIFIC REGULATIONS, PROFESSIONAL STANDARDS, OR CUSTOMER'S OWN COMPLIANCE REQUIREMENTS. SAIRIS DOES NOT MONITOR OR CONTROL HOW CUSTOMER IMPLEMENTS OR DEPLOYS AI TECHNOLOGIES WITHIN ITS ORGANIZATION AND DISCLAIMS RESPONSIBILITY FOR UNAUTHORIZED OR NON-COMPLIANT USES.

Version: 06012025 Sairis LLC Artificial Intelligence Acceptable Use Policy