AITY DOCUMENTS

AITY CLOUD SRL

Acceptable Use Policy

Version 1.0 · effective from 15 August 2026 · aity.tech/documents

DENUMIRE / ENTITY	AITY CLOUD SRL
CUI	39458128 (RO39458128)
NR. REG. COM.	J2018000824245
EUID	ROONRC.J2018000824245
CORESPONDENȚĂ / CORRESPONDENCE	Str. Heliade Între Vii nr. 35, cod 023382, Sector 2, București, România
CONTACT	office@aity.ro · support@aity.ro · aity.ro · aity.tech

Table of contents

Acceptable Use Policy

VERSION 1.0 · EFFECTIVE FROM 15 AUGUST 2026 · AITY CLOUD SRL

Romanian version · Download PDF

This policy (the "**AUP**") forms part of the Terms of Service provided by **AITY CLOUD SRL**, a Romanian limited liability company, with its registered office at SACEL no. 1003, Săcel Village, Săcel Commune, Maramureș County, postal code 437290, Romania, tax ID 39458128 (VAT RO39458128), Trade Register J2018000824245, EUID ROONRC.J2018000824245, subscribed and paid-up share capital RON 5,000, correspondence address Str. Heliade Între Vii no. 35, postal code 023382, Sector 2, Bucharest, Romania, telephone +40735850896 (Monday-Friday, 09:00-18:00 Romanian time), e-mail office@aity.ro ("**aity**"), and applies to any use of the aity Platform and aity Cloud services. The Customer is responsible for its End Users' compliance with the AUP. The Romanian and English versions are both official; in case of divergence, the Romanian version prevails.

1. General prohibitions

The Services must not be used for:

- activities that violate the law or third-party rights, including intellectual property rights, privacy, and human dignity;
- storing or distributing illegal content, including child sexual abuse material (CSAM), content inciting hatred or violence, or content violating data protection law;
- creating, transmitting, or distributing malware, ransomware, viruses, or other harmful components;
- phishing, deception, identity theft, fraud, or misrepresenting the origin of communications;
- cyberattacks of any kind: unauthorized access, interception, hostile port scanning, denial-of-service attacks, or circumventing the security measures of any system;
- any activity likely to affect the security, integrity, or availability of aity's infrastructure or services provided to other Customers.

2. E-mail-specific rules (aity Platform)

- **Spam prohibited**: sending unsolicited commercial messages is prohibited. Commercial messages may be sent only to recipients who have given prior consent (opt-in) or under the conditions permitted by article 12 of Romanian Law no. 506/2004, using the sender's real identity, accurate headers, and a functional unsubscribe mechanism that is honored promptly.
- Sending limits (number of messages, recipients, rate) are those published in the product documentation; aity may temporarily throttle traffic exhibiting a pattern of abuse.
- The following are prohibited: harvesting addresses without consent, using purchased lists, snowshoe spamming, open relaying, and sender identity forgery (spoofing).

3. Cloud-specific rules (aity Cloud)

- Cryptocurrency mining is prohibited on free and trial offers and, on paid resources, is permitted only within the contracted resources;
- operating services that facilitate abuse is prohibited: open resolvers, open proxies, and amplification/reflection services usable in DDoS attacks;
- data traffic includes 4 TB per month per instance; consumption that systematically exceeds this limit is subject to the fair-use policy: aity may propose a dedicated solution or limit excess traffic, with prior notice;
- the Customer is responsible for securing its own workloads; compromised instances attacking third parties may be isolated immediately.

4. Other restrictions

Without aity's written agreement, it is prohibited to: resell the Services as your own service; use accounts shared by several natural persons to circumvent per-user pricing; use automated account-creation mechanisms; test the security of the Services (penetration testing) without prior written authorization.

5. Points of contact and reporting illegal content (DSA)

5.1. Recipients of the Services may contact aity directly and rapidly through the electronic form at aity.tech/documents/report-illegal-content or at office@aity.ro. Authorities use office@aity.ro. Communication is available in Romanian and English and does not rely solely on automated tools. These are the points of contact under articles 11-12 of Regulation (EU) 2022/2065.

5.2. A notice must allow submission of: (a) a sufficiently substantiated explanation of why the information is considered illegal; (b) the exact electronic location, including the URL and any additional data necessary to identify it; (c) the name and e-mail address of the person submitting the notice, except for notices concerning the offenses referred to in articles 3-7 of Directive 2011/93/EU; and (d) a statement of good faith concerning the accuracy and completeness of the information.

5.3. aity acknowledges receipt without undue delay, reviews the notice in a timely, diligent, objective, and non-arbitrary manner, and communicates the decision and avenues for redress. The acknowledgement and decision are sent to the electronic address provided. If automated means are used for detection, prioritization, or decision-making, that fact is communicated.

5.4. aity has no general obligation to monitor hosted information and does not actively conduct general investigations. A sufficiently precise notice may give rise to actual knowledge within the meaning of the law and will be handled under this article.

6. Enforcement

6.1. In the event of an AUP breach, aity may, proportionately to its seriousness: request remediation within 24 hours, limit functionality or visibility, suspend the affected Services or Accounts, remove illegal content or disable access to it, terminate the contract for serious or repeated breaches, and notify competent authorities. When selecting the measure, aity takes into account seriousness, frequency, impact, intent, cooperation, and the rights of all affected persons.

6.2. In serious cases (ongoing attacks, manifestly illegal content, risk to third parties or infrastructure), aity may act immediately without prior notice, informing the Customer as soon as reasonably possible.

6.3. Recurring fees remain due during a suspension attributable to the Customer, under the Terms.

6.4. Statement of reasons for restrictions. No later than when a measure is imposed, aity sends the affected recipient, if it knows the recipient's electronic contact details, a clear, specific, and easily understandable statement of reasons stating: the measure, its territorial scope and duration; the facts and circumstances, including the source of the notice or investigation; the use of automated means; the legal ground and reasons why the information is illegal, or the contractual clause and reasons why it is incompatible; and the available internal, out-of-court, and judicial avenues for redress, as applicable. Exceptions apply only under the conditions of article 17 of Regulation (EU) 2022/2065.

6.5. Moderation and challenges. Anti-spam and anti-malware filters and security mechanisms may detect, prioritize, temporarily quarantine, or technically stop an attack. A material restriction of the Account or termination involves human review. The Customer or affected recipient may challenge the measure at office@aity.ro, identifying the decision and reasons; where practicable, a person who did not make the initial decision reviews the case and communicates the outcome on a durable medium. This avenue does not limit out-of-court or judicial mechanisms available under the law.

6.6. Safety of persons. If aity becomes aware of information giving rise to a suspicion that an offense involving a threat to a person's life or safety has taken place, it promptly informs the competent authorities under article 18 of Regulation (EU) 2022/2065 and retains a record of the decision and information transmitted.

7. Vulnerability reporting

Vulnerabilities that may affect the Services may be reported confidentially to security@aity.ro, under the policy published at aity.tech/documents/security and the `/.well-known/security.txt` file. The report should identify the Service, vulnerability, reproduction steps, and the reporter's contact details. aity acknowledges receipt, protects responsible reporting carried out in good faith within the policy's limits, and communicates a reasonable remediation timeline, without requesting access to or disclosure of other persons' data.

Version history

VERSION	DATE	CHANGES
1.0	15 August 2026	First published version.