Last Updated: October 6th, 2026

Acceptable Use Policy

1. **Application**. This Acceptable Use Policy ("**AUP**") forms part of the Agreement. Customer shall comply, and ensure that its Users, Guests, and anyone else using its account comply, with this AUP. The examples below are not exhaustive, and Airia will determine violations in its sole discretion. Undefined capitalized terms have the meaning given in the Airia Service Terms at https://trust.airia.com/resources.

2. **Prohibited Uses.** Customer shall not use the Airia Services unlawfully or as follows:

2.1. **AI Law Prohibited Practices** - practices prohibited by Article 5 of the EU AI Act (as amended) or similar laws, including any AI system that:

a) uses subliminal, manipulative, or deceptive techniques to materially distort a person's behavior, causing or likely to cause significant harm;
b) exploits vulnerabilities due to age, disability, or social or economic situation to distort behavior, causing or likely to cause significant harm;
c) scores individuals based on their social behavior or personal characteristics, leading to detrimental treatment that is unjustified, disproportionate, or in unrelated contexts;
d) predicts the risk of an individual committing a criminal offense based solely on profiling or personality traits;
e) builds facial recognition databases by untargeted scraping of facial images from the internet or CCTV;
f) infers emotions in workplaces or education, except for medical or safety reasons;
g) uses biometric data to infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation;
h) performs real-time remote biometric identification in public spaces for law enforcement, except as permitted by law; or
i) can foreseeably generate non-consensual intimate imagery or child sexual abuse material without adequate safeguards.

2.2. Safety, Security, and Critical Infrastructure - including:

a) developing or deploying weapons designed to harm people;
b) disrupting or damaging critical infrastructure or military systems;
c) generating malware or other malicious code;
d) circumventing safety or security controls without authorization; or
e) inciting, facilitating, or promoting violence, terrorism, or self-harm.

2.3. Privacy and Surveillance - including:

a) unlawful surveillance or tracking of individuals; or
b) processing children's personal data without legally required parental or legal guardian consent.

2.4. Harmful, Abusive, or Exploitative Content - including:

a) child sexual abuse material or other content exploiting minors;
b) non-consensual intimate imagery, including deepfakes;
c) content that is excessively violent, cruel, or gory; or
d) harassment, threats, or hateful content targeting any person or group.

2.5. Fraud, Deception, and Misrepresentation - including:

a) impersonating any person, entity, or AI system without authorization;
b) misleading deepfakes or other deceptive content;
c) fraud, phishing, or other financial crime;

Copyright © Airia LLC 2026

d) spam or unsolicited bulk communications;
e) plagiarism or facilitating academic dishonesty; or
f) interfering with elections or political campaigns through deceptive means.

2.6. Discrimination, Exploitation, and Unlawful Profiling - including:

a) unlawful discrimination based on protected characteristics;
b) facilitating human trafficking or trafficking in illegal substances; or
c) infringing the intellectual property rights of third parties.

2.7. Platform Integrity and Compliance - including:

a) creating accounts to evade any suspension or restriction imposed by Airia;
b) enabling access in breach of export controls, sanctions, or other applicable law; or
c) extracting or reverse-engineering Model weights, training data, or methodologies.

3. **Security Testing**. Section 2 does not restrict lawful, good-faith security testing or red-teaming of Customer's own AI systems.

4. **Transparency.** Customer shall comply with all applicable AI transparency obligations (including under Article 50 of the EU AI Act), including telling individuals when they are interacting with AI.

5. **High-Risk Uses**. High-Risk Uses are permitted only if Customer complies with all applicable laws. A "**High-Risk Use**" is any use of the Airia Services for an AI system that is high-risk under applicable law (including Article 6 of the EU AI Act) or that makes or materially influences decisions with legal or similarly significant effects on individuals, such as in employment, education, credit, insurance, housing, healthcare, essential services, law enforcement, migration, or justice.

5.1. Customer is responsible for determining its role under applicable law and for meeting all requirements for the AI system and its development and use, not only its Output (for example, risk management, documentation, logging, human oversight, conformity assessment, and incident reporting).

5.2. Customer may become the provider of a high-risk AI system (including under Article 25 of the EU AI Act). Airia does not represent that the Airia Services meet the requirements for any such system. Except as required by applicable law, Airia's compliance support is limited to the Documentation and any assistance agreed in writing.

6. **Third-Party Services**. Customer's use of any Third-Party Service (including AI Models) is subject to, and Customer shall comply with, that provider's terms and policies, including where Customer uses its own credentials. The stricter of those terms and this AUP applies. Airia may restrict access to a Third-Party Service where its provider requires.

7. **Reporting**. Customer shall promptly report suspected violations to notices@airia.com. Airia may investigate and suspend or restrict access under the Agreement.

8. **Change.** Airia may update this AUP by posting it at https://trust.airia.com/resources, and continued use of the Airia Services after an update constitutes acceptance.

Copyright © Airia LLC 2026