Boomi AI Acceptable Use Policy

Effective Date: April 3, 2026

Scope and purpose

This Acceptable Use Policy (AUP) applies to all users of Boomi AI, including Boomi Agentstudio, and covers the building, configuration, deployment, and use of AI-enabled capabilities and agents through the Boomi platform. This AUP forms part of your agreement with Boomi. A breach of this AUP constitutes a breach of the Boomi Master Services Agreement.

Third-party model providers

Boomi AI may use or provide access to models, tools, and services supplied by third-party providers. Where this is the case, your use is also subject to the applicable usage policies of those providers, including restrictions on using inputs or outputs to train, fine-tune, distil, or improve any AI model without the relevant provider's prior authorisation, and restrictions on systematic prompting or collection of outputs intended to replicate model behaviour. For Boomi's foundational model, such policies are made available at anthropic.com/legal/aupor such other location as Boomi specifies from time to time. Where those policies impose stricter requirements than this AUP, the stricter requirement applies.

Prohibited uses

The following uses of Boomi AI are prohibited. They reflect requirements under applicable law, including Regulation (EU) 2024/1689 (the EU AI Act), and apply regardless of the deployment context or sector in which you operate.

You must not use Boomi AI to:

(a) Manipulate or deceive. Deploy subliminal or manipulative techniques that materially distort a person's behaviour by impairing their ability to make an informed decision, where this causes or is reasonably likely to cause significant harm.

(b) Exploit vulnerabilities. Exploit vulnerabilities such as those arising from age, disability, or social or economic circumstances in a way that distorts a person's behaviour and causes or is reasonably likely to cause significant harm.

(c) Social scoring. Evaluate or classify individuals or groups based on social behaviour or predicted personal characteristics in ways that lead to detrimental treatment in unrelated contexts or to unjustified or disproportionate harm.

(d) Predictive criminal risk. Assess or predict the risk of a person committing a criminal offence, or engage in predictive policing or similar profiling.

(e) Facial recognition databases. Create or expand facial recognition databases through untargeted scraping of images from the internet or CCTV footage.

(f) Emotion recognition. Infer the emotions of individuals in workplace or educational settings, except where permitted by law for medical or safety purposes.

(g) Biometric categorisation. Deduce or infer sensitive attributes including race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation from biometric data.

(h) Real-time biometric identification. Conduct real-time remote biometric identification in publicly accessible spaces for law enforcement purposes.

(i) Harmful, abusive, or exploitative content. Generate, distribute, or facilitate content that is illegal, abusive, or exploitative, including child sexual abuse material ("CSAM"), content that incites or facilitates violence or terrorism, content that harasses or targets individuals on the basis of protected characteristics, and non-consensual intimate imagery. Where Boomi detects suspected CSAM, Boomi may take immediate action including suspension of access and reporting to competent authorities where required or appropriate.

(j) Autonomous commitments. Automatically commit an organisation to a legal or financial obligation without an appropriate human approval step.

(k) Data fabrication. Fabricate data used to make business-critical decisions.

Your role under the EU AI Act

Depending on how you use Boomi AI, you may be considered a provider or a deployer under the EU AI Act. Different obligations apply to each role. You are responsible for determining which role applies to your use and for meeting the obligations that come with it.

High-risk AI systems

Boomi AI is not classified as a high-risk AI system under the EU AI Act and is not designed or intended for high-risk use. If an agent you build or deploy using Boomi AI constitutes, or functions as, a high-risk AI system within the meaning of Article 6 of the AI Act, this will be treated as a modification of the intended purpose of Boomi AI.

Boomi does not determine whether your specific deployment qualifies as high-risk. That assessment is your responsibility. Where your deployment does fall within a high-risk classification, you carry the applicable legal obligations as provider under the AI Act and other applicable law, and you are responsible for meeting those obligations before the system is put into service.

Operating in a regulated sector does not, by itself, make a deployment high-risk. Classification depends on the specific intended purpose and deployment context of the AI system.

Transparency and human oversight

Where Boomi AI is used in a context that directly affects and/or interacts with individuals, you must:

- inform those individuals that they are interacting with an AI system, and not present outputs as human-generated where the intent is to mislead, at the start of each session where the agent is interactive or consumer-facing;

- where Boomi AI is used to provide tailored advice that would ordinarily require a professional licence, such as legal or medical advice, ensure that a licensed professional is appropriately involved before that advice is disseminated; and

- where you deploy Boomi AI to generate or manipulate image, audio, or video content that constitutes a deepfake, or to generate text published for the purpose of informing the public on matters of public interest, disclose that the content has been artificially generated or manipulated, subject to any exceptions permitted under applicable law.

Your responsibilities as a user

You are responsible for your use of Boomi AI and for the agents you build and deploy, whether you are acting as a provider or a deployer. When building or deploying an agent, you should consider its intended purpose, where it will be used, and how it might affect the people who interact with it. You should use appropriate change control, testing, monitoring, and access controls before and after deployment. You should ensure that staff operating agents on your behalf have a sufficient understanding of AI for their role. Where you expose tools, connectors, APIs, or Model Context Protocol (MCP) servers to an agent, you should ensure that such tooling is authorised and monitored.

Reporting

If you become aware of suspected misuse of Boomi AI, or a material safety incident arising from your use of an agent, you must promptly notify Boomi. You must also notify Boomi of any request or notice received from a regulator that relates to your use of Boomi AI, and cooperate reasonably with Boomi in responding to it, to the extent permitted by law.

Enforcement

Boomi may implement monitoring to detect misuse and enforce this AUP. Violations may result in suspension of access to Boomi AI in accordance with the terms of the Master Services Agreement.

Changes

Boomi may update this AUP from time to time. The updated version will apply from the effective date stated in the revised AUP, or as otherwise specified in the applicable terms.