AXION ACCEPTABLE USE POLICY

ENGLISH MASTER — Draft v1

1. Purpose and Scope

This Acceptable Use Policy (“AUP”) sets out the fundamental rules governing permitted and prohibited use of the Axion Service. It should be read together with Axion's Terms and Conditions / Terms of Service, Privacy Policy and other applicable policies.

The AUP applies to all Axion functionality involving AI models, orchestration, web research, document or file processing, code generation or execution, sandbox environments, Connected Services, external integrations or Actions.

The User is responsible for ensuring that their use, Inputs, instructions, integrations, applications and operations performed with Axion comply with applicable law and this AUP.

2. Permitted Use

Axion may be used for lawful and responsible purposes, including research, summarisation and analysis of information, creation and processing of documents, programming and software development, business and creative workflows, education and learning, and other tasks that do not violate this AUP.

Security, cybersecurity, research or testing uses may be permitted where lawful, appropriately authorised, conducted in a controlled environment and not intended to obtain unauthorised access, cause harm, distribute malware or disrupt another person's systems.

The fact that a use falls within a generally permitted category does not make a specific harmful or unlawful implementation acceptable.

3. Illegal, Harmful and Abusive Activities

Axion must not be used to prepare, facilitate, carry out or conceal crime, unlawful activity, fraud, deception, theft, extortion, unlawful trade or harm to persons, organisations or systems.

The Service must not be used to create or operate instructions, workflows, code, documents or automation whose primary purpose is to materially facilitate unlawful or harmful activity.

Axion may restrict or refuse requests where completion would endanger the Service, the User or a third party, or would violate applicable law, this AUP or a mandatory provider policy.

4. Child Sexual Exploitation and Abuse

Creating, obtaining, transforming, distributing, facilitating or concealing content relating to child sexual exploitation or abuse is strictly prohibited, including sexualisation of children and use for grooming.

This prohibition applies whether the content is real, synthetic, altered or AI-generated.

5. Violence, Terrorism and Dangerous Activities

Axion must not be used to materially facilitate, organise or carry out terrorism, violent extremism, targeted physical violence, serious injury or violence against others.

Material facilitation of the creation, acquisition or use of weapons, explosives, chemical, biological, radiological or nuclear weapons or other dangerous devices is prohibited where unlawful or intended to harm persons, organisations or society.

6. Self-Harm and Endangerment

Axion must not be used to encourage, optimise or provide practical facilitation for self-harm, suicide, serious self-endangerment or endangerment of another person.

Axion may support safe preventive, educational or help-seeking uses that do not facilitate harm.

7. Cybersecurity, Malware and System Abuse

Creating, deploying, operating or materially facilitating unauthorised access, credential theft, phishing, malware, ransomware, botnets, destructive payloads, command-and-control infrastructure, denial-of-service attacks or other malicious cyber activity is prohibited.

Unauthorised compromise, surveillance, disruption or damage of another person's system, account, network, data or service is prohibited.

Lawful defensive security, testing of systems you control, authorised penetration testing, CTFs, malware analysis and security education may be permitted where appropriate authorisation, scope and a safe environment are present.

8. Circumvention of Axion and Provider Safeguards

Users must not unlawfully or without authorisation bypass, disable or manipulate Axion's access restrictions, rate limits, security controls, policy enforcement, permission boundaries or other safeguards.

Prompt injection, jailbreaks, tool manipulation or similar techniques must not be used for the purpose of obtaining unauthorised system instructions, secrets, another User's data or resources to which the User has no right of access.

Controlled security testing or vulnerability research may be conducted only within any scope, rules and authorisation made available by Axion.

9. Privacy, Personal Data and Surveillance

Axion must not be used to unlawfully obtain, collect, deanonymise, disclose or use personal data, biometric data, authentication data or other sensitive information.

Tracking, monitoring or profiling persons without consent or another appropriate legal basis is prohibited where applicable law prohibits such activity.

Users may make third-party data, Connected Service data or organisational data available to Axion only where they have appropriate authority and legal basis for the relevant processing.

10. Harassment, Hate and Exploitation

Axion must not be used to facilitate targeted harassment, intimidation, stalking, threats, abuse, exploitation, or hatred or violence against persons or protected groups.

Users must not exploit or manipulate another person's vulnerability in a manner likely to cause significant physical, psychological, financial or other harm.

11. Sexual Content and Non-Consensual Intimate Content

Any sexual content involving children, and the creation, alteration, distribution or facilitation of non-consensual intimate or sexual content, is prohibited.

Axion may also restrict other explicit sexual or pornographic uses based on Service safety requirements and applicable upstream provider policies.

12. Fraud, Deception, Impersonation and Spam

Axion must not be used to create or facilitate fraud, scams, phishing, false identities, deceptive impersonation, false documents or other deceptive practices intended to mislead others, violate their rights or obtain an unlawful advantage.

Axion must not be used to create or distribute unsolicited bulk communications, spam or deceptive automated communications.

AI-generated content must not be deceptively represented as exclusively human-generated where doing so is intended to mislead others or where applicable law or product policy requires disclosure.

13. Intellectual Property and Rights of Others

Axion must not be used to knowingly infringe or circumvent copyright, trademark, trade-secret, personality, privacy or other third-party rights.

The User is responsible for having the rights necessary to use Inputs, files, data, code and other content provided to Axion and for using Outputs lawfully.

14. High-Impact and Regulated Decisions

Axion must not be used without appropriate human oversight to make solely or substantially automated decisions that may have a significant detrimental effect on a natural person's rights, legal position, life opportunities or fundamental interests.

This is particularly relevant in employment, credit and finance, insurance, healthcare, housing, education, legal services, social welfare and other high-risk domains.

The User is responsible for necessary professional review, human oversight, legal basis, transparency, auditability and compliance with applicable AI and sector-specific requirements.

15. Connected Services, Actions and External Systems

Users may connect Axion only to a Connected Service, account, mailbox, file, calendar, repository, API or other external system they are appropriately authorised to use.

Axion Actions or other execution capabilities must not be used to cause unauthorised messaging, file modification, data extraction, transactions, account operations or other external effects.

Where Axion requests confirmation or other User approval for an externally consequential operation, Users must not attempt to bypass that control through deception or technical means.

16. Code, Sandboxes and User-Operated Applications

Code, workflows and User-operated applications created or executed with Axion must not be used to circumvent this AUP. The same restrictions apply where a prohibited operation is performed by generated code, automation, an agent or an external application rather than by a direct prompt.

The User is responsible for reviewing and testing generated code and applications before production use and for their permissions, data processing and secure configuration.

Sandbox or code-execution environments must not be used to attack other systems without authorisation, abuse computing resources, run malware for harmful purposes or provide infrastructure for prohibited activity.

17. Safety, Educational, Scientific and Public-Interest Contexts

Analysis of an otherwise sensitive topic may be permitted where the purpose is clearly lawful security, educational, documentary, scientific, journalistic or other public-interest use and the request does not provide practical assistance that materially increases the ability to cause harm.

Axion may limit, transform into a safer form or refuse such requests where the risk, context or an applicable provider policy warrants doing so.

18. Provider Policies and Feature-Specific Restrictions

Axion may use multiple external AI, cloud, search, sandbox and other technology providers. Particular functionality may therefore also be subject to mandatory use or safety requirements imposed by the relevant provider.

Where an Axion feature is subject to a stricter provider restriction for technical or contractual reasons, Axion may apply that stricter restriction to the feature even if the same use would not generally be prohibited in another Axion function.

Users may not use Axion to circumvent provider policies, safety filters or other mandatory restrictions.

19. Enforcement and Measures

To prevent, detect and investigate AUP violations, Axion may apply automated and manual security, abuse-prevention and policy-enforcement controls in accordance with applicable law and the Privacy Policy.

Depending on the nature, severity and recurrence of a violation or risk, Axion may refuse or restrict a request or feature, issue a warning, temporarily limit access, suspend or terminate an Account, or take other measures required or permitted by law or contract.

In the case of a serious or urgent security risk, Axion may apply immediate protective measures without prior notice where permitted by applicable law and the Terms.

20. Reporting, Changes and Precedence

Suspected abuse, security issues or AUP violations may be reported to support@axionaiapp.com.

Axion may update this AUP as the Service, technical capabilities, law, threat environment or provider requirements change. The current version will be published through the legal interface associated with the Service.

If this AUP conflicts with mandatory law, mandatory law prevails. If a mandatory provider policy imposes a stricter restriction on a particular Axion feature, Axion may apply the stricter rule to that feature.

[LAUNCH REQUIREMENT: before publication, compare this AUP against Axion's final Terms, the policies of AI/cloud providers actually used in production, applicable EU AI Act prohibited-practice requirements, and Axion's enforcement and appeal/support process. Remove all internal markers from the public version.]

Last updated: [DATE]
Effective date: [DATE]
Version: [VERSION]