

AxiaForce

ACCEPTABLE USE POLICY

AxiaForce, Inc.

Version 1.0 | Effective Date: October 12, 2026

This Acceptable Use Policy ("AUP") establishes the rules for responsible and lawful use of AxiaForce Services. It supplements the AxiaForce Master SaaS Terms and applies to all customers, authorized users, and use of AxiaForce-enabled workflows.

1. Scope

This Acceptable Use Policy ("AUP") applies to Customer's and its users' access to and use of all AxiaForce Services, including AI-enabled agents, communications features, APIs, integrations, automation, voice, messaging, recruiting, sales, customer-engagement, and other functionality.

Customer is responsible for ensuring that its users and anyone acting through its accounts comply with this AUP.

2. Lawful and Authorized Use

The Services may be used only for lawful business purposes and only where Customer has the rights, permissions, consents, and authority required for the applicable activity.

Customer may not use the Services to violate applicable law, regulation, court order, contractual obligation, or the rights of another person.

3. Fraud, Deception, and Impersonation

Customer may not use the Services to commit or facilitate fraud; misrepresent identity or affiliation; deceive recipients about the source or purpose of a communication; impersonate another person or organization without authorization; create deceptive deepfakes or synthetic media; conduct phishing or credential theft; or engage in other misleading or fraudulent practices.

Use of AI-generated personas, voices, or communications must comply with applicable disclosure and consent requirements.

4. Email and Electronic Messaging

Customer may not use the Services to send unlawful spam or other electronic communications in violation of applicable law.

Customer is responsible for maintaining required permissions, opt-outs, suppression lists, unsubscribe mechanisms, sender-identification information, and other requirements applicable to its communications.

Customer may not use false or materially misleading sender identities, subject lines, routing information, or contact information.

Customer must promptly honor valid opt-out and suppression requests.

5. Telephone, Voice, SMS, and Recorded Communications

Customer is responsible for compliance with laws governing calling, texting, prerecorded or artificial voice communications, telemarketing, do-not-call requirements, consent, calling hours, caller identification, and recording of calls or meetings.

Customer must obtain legally required consent before recording, transcribing, monitoring, or using synthetic or AI-generated voice in circumstances where consent or disclosure is required.

Customer may not spoof caller identification or use communications functionality to harass, threaten, or repeatedly contact recipients who have opted out or objected.

6. Recruiting, Employment, and High-Impact Decisions

Customer may not use the Services to unlawfully discriminate or to make decisions prohibited by employment, civil-rights, accessibility, or other applicable laws.

Where law requires notice, assessment, consent, explanation, human review, or other safeguards for automated or AI-assisted employment decisions, Customer is responsible for implementing those requirements.

Unless expressly supported by AxiaForce in writing for the applicable use case, Customer may not rely solely on automated output for final decisions involving employment, credit, housing, insurance, healthcare, legal rights, or other similarly high-impact matters where applicable law requires additional safeguards.

7. Privacy and Personal Data

Customer may not collect, upload, access, enrich, disclose, or Process Personal Data through the Services without a lawful basis and required permissions.

Customer may not use the Services to obtain or infer sensitive Personal Data unlawfully, circumvent privacy choices, defeat consent mechanisms, or combine data in a manner prohibited by applicable law.

Customer must comply with the Agreement, DPA, and applicable privacy and data-protection laws.

8. Security Abuse

Customer may not use the Services to gain unauthorized access to systems, accounts, networks, credentials, or data; distribute malware; conduct denial-of-service attacks; exploit vulnerabilities; perform credential stuffing; conduct phishing; bypass authentication or access controls; interfere with platform operation; or facilitate malicious cyber activity.

Security testing, penetration testing, vulnerability scanning, or similar testing of AxiaForce systems requires AxiaForce's prior written authorization.

9. Unauthorized Data Acquisition and Scraping

Customer may not use the Services to scrape, harvest, obtain, or process data where Customer lacks authorization or where the activity violates applicable law, contractual restrictions, technical access controls, or third-party rights.

Customer is responsible for determining whether data obtained from third-party providers, websites, APIs, or other sources may lawfully be used for Customer's intended purpose.

10. Intellectual Property and Proprietary Rights

Customer may not use the Services to infringe, misappropriate, or unlawfully exploit copyrights, trademarks, patents, trade secrets, rights of publicity, privacy rights, or other proprietary rights.

Customer may not use AxiaForce to reproduce or distribute content where Customer lacks the necessary rights.

11. Platform Integrity and Usage Controls

Customer may not circumvent usage limits, rate limits, license controls, approval workflows, safety controls, authentication measures, or technical restrictions.

Customer may not intentionally overload the Services, generate abusive or wasteful traffic, use automation to degrade service for others, or create multiple accounts or identities to evade limits, suspension, or pricing.

Customer may not resell, sublicense, or provide unauthorized shared access to the Services.

12. Reverse Engineering and Competitive Use

Customer may not reverse engineer, decompile, disassemble, extract, copy, discover, or attempt to derive AxiaForce source code, prompts, orchestration, model configurations, non-public architecture, algorithms, or other proprietary technology except where such restriction is prohibited by applicable law.

Customer may not use the Services or outputs from systematic testing of the Services to build, train, benchmark, validate, or improve a competing product or service without AxiaForce's prior written consent.

Customer may not publicly publish comparative performance or benchmark results concerning the Services without AxiaForce's prior written consent.

13. Prohibited Content and Conduct

Customer may not use the Services to create, store, send, or distribute content or communications that are unlawful; threatening; intentionally harassing; defamatory; fraudulent; malicious; designed to facilitate criminal conduct; or that unlawfully exploits, targets, or endangers individuals.

AxiaForce may restrict specific content or conduct where reasonably necessary to comply with law, protect users or third parties, preserve platform integrity, or address a material security or abuse risk.

14. Regulated and Restricted Activities

Customer is responsible for determining whether its industry or intended use is subject to special regulatory requirements.

Customer may not use the Services for a regulated or restricted activity where the applicable AxiaForce Service has not been configured or contractually approved for that activity.

Customer must not submit data subject to specialized legal restrictions, including protected health information, payment-card data, government-classified information, or similarly sensitive regulated data, unless AxiaForce has expressly agreed in writing that the applicable Service supports that data type.

15. Export Controls and Sanctions

Customer may not access or use the Services in violation of applicable export-control, trade-sanctions, or embargo laws, or for the benefit of a person or entity prohibited from receiving the Services under applicable law.

16. Third-Party Services and Integrations

Customer may use only integrations and third-party services that Customer is authorized to access.

Customer may not direct AxiaForce to violate a third party's terms, technical restrictions, privacy rights, or security controls.

Customer remains responsible for actions performed through Customer-configured third-party integrations and for permissions granted to the Services.

17. Reporting Abuse and Violations

Suspected abuse, unlawful communications, security misuse, or other violations involving the Services may be reported to support@axiaforce.ai.

AxiaForce may request information reasonably necessary to investigate a reported violation.

18. Investigation and Enforcement

AxiaForce may investigate suspected violations of this AUP and may use automated and manual methods to protect the Services, customers, recipients, and third parties.

Where reasonably practicable, AxiaForce may provide Customer an opportunity to cure a violation. AxiaForce may immediately restrict, suspend, or terminate affected functionality where necessary to address unlawful conduct, material security risk, fraud, abuse, harm to third parties, repeated violations, or a credible threat to the Services.

A violation of this AUP constitutes a breach of the Agreement.

19. Changes to this AUP

AxiaForce may update this AUP from time to time. Notice of material changes will be provided using the notice methods described in the Agreement.

Changes required by law, security, abuse prevention, or technical operation may become effective on the stated effective date. Continued use of the Services after the applicable effective date constitutes acceptance of the updated AUP as provided in the Agreement.

20. Contact

Questions regarding this AUP may be directed to:

AxiaForce, Inc. support@axiaforce.ai

END OF ACCEPTABLE USE POLICY