

AxiaForce

SLA / SUPPORT POLICY

AxiaForce, Inc.

Version 1.0 | Effective Date: October 12, 2026

This Policy establishes AxiaForce's standard support channels, severity classifications, response objectives, support scope, and service-level framework. It is designed to provide clear customer expectations without creating availability or service-credit commitments unless those commitments are expressly purchased or agreed in writing.

1. Scope and Relationship to the Agreement

This Service Level and Support Policy ("Policy") describes the standard support process and service-level objectives for paid AxiaForce Services.

This Policy supplements the AxiaForce Master SaaS Terms. If an Order Form or separately executed service-level agreement provides different support hours, response targets, availability commitments, or service credits, that document controls for the affected Services.

2. Support Channels

Customers may submit support requests through available in-application support functionality or by emailing support@axiaforce.ai.

AxiaForce may add customer portals, ticketing systems, chat, or other support channels over time. Where a support ticket or case number is assigned, Customer should use that reference for follow-up communications concerning the same issue.

3. Support Availability

Support requests may be submitted twenty-four (24) hours a day, seven (7) days a week.

Standard human support is provided during AxiaForce business support hours unless the applicable Order Form includes enhanced support. Business support hours are 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding U.S. federal holidays.

AxiaForce may use automated or AI-enabled support outside business support hours. Monitoring and incident-response processes may operate outside standard support hours for material production incidents.

4. Severity Levels

Severity 1 - Critical: A production issue causing a widespread or material inability to access or use a core paid Service, material cross-tenant or security risk, or a critical production function that is unavailable with no reasonable workaround.

Severity 2 - High: A substantial degradation of important production functionality affecting Customer operations where a reasonable workaround is unavailable or materially burdensome.

Severity 3 - Normal: A non-critical defect, limited degradation, configuration issue, integration issue, or product problem for which a workaround exists or the impact is not materially business-critical.

Severity 4 - Low / Request: General questions, documentation requests, cosmetic issues, feature requests, product guidance, or other non-urgent matters.

AxiaForce may reasonably adjust severity based on actual impact, scope, reproducibility, availability of a workaround, and whether Customer has provided information necessary to investigate.

5. Initial Response Objectives

AxiaForce will use commercially reasonable efforts to provide an initial substantive response within the following targets:

Severity 1: 4 hours. Severity 2: 1 business day. Severity 3: 3 business days. Severity 4: 5 business days.

These are initial response objectives, not guaranteed resolution times. Response measurement begins when AxiaForce receives a support request containing sufficient information to begin investigation. For requests submitted outside business support hours, Severity 2 through Severity 4 response measurement begins at the start of the next business support period.

For a Severity 1 incident involving a confirmed material production outage or security incident, AxiaForce will use commercially reasonable efforts to begin response outside business support hours when detected through monitoring or properly escalated by Customer.

6. Resolution and Restoration

Resolution time depends on the nature of the issue, architecture, third-party dependencies, Customer cooperation, severity, and whether code, configuration, infrastructure, provider, or integration changes are required.

AxiaForce does not guarantee a specific resolution time unless an applicable Order Form expressly states one.

For material production incidents, AxiaForce may prioritize restoration, containment, workaround, or service stabilization before permanent root-cause remediation.

7. Customer Responsibilities

Customer will provide information reasonably necessary to investigate support requests, which may include the affected tenant, users, workflows, timestamps, steps to reproduce, relevant screenshots, business impact, integration information, and other diagnostic details.

Customer will make appropriate personnel available when testing, approvals, credentials, integration changes, or Customer-controlled systems are necessary to resolve an issue.

Delays caused by incomplete information, unavailable Customer personnel, Customer-controlled systems, or third parties selected or controlled by Customer may pause applicable response or investigation objectives.

8. Support Scope

Standard support covers reasonable assistance with use of paid AxiaForce Services, suspected product defects, account or access issues, supported integrations, and technical issues within AxiaForce-controlled Services.

Standard support does not include unlimited implementation, custom development, data cleansing, business-process consulting, training, migration work, Customer network administration, administration of Customer-controlled third-party systems, or creation of new product features. Those services may require an Order Form, Statement of Work, professional-services engagement, or other separate agreement.

9. Third-Party Services and Customer Integrations

AxiaForce Services may depend on cloud, AI/model, communications, payment, email, voice, customer-authorized integration, and other third-party services.

AxiaForce will use commercially reasonable efforts to investigate issues involving dependencies used to provide the Services, but AxiaForce is not responsible for outages, delays, rate limits, defects, changes, or failures caused solely by third-party systems outside AxiaForce's reasonable control.

Customer-selected or Customer-controlled integrations are subject to the availability, permissions, configuration, and terms of those third parties.

10. Maintenance and Changes

AxiaForce may perform planned maintenance, updates, releases, security changes, infrastructure changes, migrations, or other work necessary to operate and improve the Services.

Where planned work is reasonably expected to cause material customer-facing disruption, AxiaForce will use commercially reasonable efforts to provide advance notice through email, the AxiaForce Notices system, in-application messaging, or another reasonable channel.

Emergency security, reliability, or provider-related maintenance may be performed without advance notice where reasonably necessary.

11. Availability

AxiaForce designs the Services for reliable production use but does not provide a standard contractual uptime percentage under this Policy.

Any guaranteed availability percentage, excluded downtime rules, service credits, recovery objectives, or other availability remedies apply only where expressly stated in an applicable Order Form or separately executed SLA.

Marketing statements, status information, or historical performance do not create a contractual availability commitment.

12. Service Credits

No service credits are provided under this standard Policy unless the applicable Order Form or separately executed SLA expressly provides for service credits.

Where service credits are expressly provided, they are calculated and administered solely under the applicable written terms and are not automatically cash refunds.

13. Escalation

Customers may request escalation of a material unresolved support matter through support@axiaforce.ai.

AxiaForce may escalate issues internally based on severity, customer impact, security implications, duration, provider dependencies, or other relevant factors.

14. Ticket Closure

AxiaForce may close a support request when the issue is resolved, a reasonable solution or workaround has been provided, the issue is determined to be outside AxiaForce's support scope, or Customer does not provide requested information or respond after reasonable follow-up.

A closed support request may be reopened or a new request submitted if the issue recurs or materially new information becomes available.

15. Security and Privacy Incidents

Security and privacy incidents are handled under AxiaForce's incident-response process and applicable contractual or legal requirements.

Suspected security issues may be reported to security@axiaforce.ai. Privacy or data-protection matters may be directed to privacy@axiaforce.ai.

16. Changes to this Policy

AxiaForce may update this Policy as support operations, Services, support tooling, or service tiers evolve.

Material changes will be communicated using the notice mechanisms described in the Master SaaS Terms. Plan-specific or negotiated support commitments in an Order Form remain governed by that Order Form during the applicable committed term unless otherwise agreed.

17. Contact

Support requests: support@axiaforce.ai

Security matters: security@axiaforce.ai

Privacy matters: privacy@axiaforce.ai

END OF SLA / SUPPORT POLICY