

AxiaForce

SECURITY FRAMEWORK

AxiaForce, Inc.

Version 1.0 | Effective Date: October 12, 2026

AxiaForce is designed to help businesses operate with AI-enabled software and agentic workflows while protecting the systems, data, identities, and integrations those workflows depend on. This Security Framework explains the security model and shared responsibilities at a customer-appropriate level without exposing sensitive internal architecture.

1. Purpose and Scope

This Security Framework describes the security principles, control categories, and shared responsibilities used to protect AxiaForce Services and Customer Data. It supports customer security reviews and explains AxiaForce's security approach at a level appropriate for public disclosure.

This Framework is informational and does not create service levels, certifications, or contractual commitments beyond those expressly stated in the applicable Agreement, Data Processing Addendum, Order Form, SLA, or separately executed Security Addendum.

2. Security Governance

AxiaForce applies a risk-based approach to security that considers the confidentiality, integrity, and availability of systems and data; the sensitivity of Customer Data; AI-enabled and agentic workflows; and dependencies on cloud infrastructure and Subprocessors.

Security controls are reviewed as the Services, architecture, threat environment, and legal requirements evolve.

3. Shared Responsibility

AxiaForce is responsible for security controls within systems and infrastructure under its control. Customer is responsible for secure administration of Customer accounts, authorized users, connected systems, credentials, permissions, data governance, and Customer-selected integrations.

Security outcomes depend on both parties configuring and operating their respective environments appropriately.

4. Identity and Access Management

AxiaForce uses identity and access controls designed to restrict access to systems and Customer Data to authorized users and personnel based on legitimate business need.

Controls may include unique identities, role-based access, least-privilege principles, multi-factor authentication for privileged access, session controls, access revocation, and periodic review of administrative access where applicable.

5. Tenant Isolation and Authorization

Each AxiaForce customer tenant is provisioned with its own separate database. Customer Data from different tenants is not stored together in a shared customer database.

Tenant-specific authorization controls, credentials, application context, and access boundaries are designed to restrict each tenant to its own database, configuration, users, integrations, and Customer Data.

Database-level separation is supplemented by application-level authorization and access controls designed to prevent cross-tenant access. Customer-configured permissions and integrations remain part of the shared-responsibility model.

6. Encryption and Data Protection

AxiaForce uses encryption in transit and encryption at rest where supported by the applicable service and underlying infrastructure.

Secrets, tokens, credentials, and integration keys are handled using security controls appropriate to their sensitivity and should not be exposed through user interfaces, logs, or customer-facing diagnostics except where specifically required and appropriately protected.

7. Secure Development and Change Management

AxiaForce incorporates security into software development and change processes through practices appropriate to the size, architecture, and risk of the Services.

These practices may include code review, dependency management, access-controlled source repositories, environment separation, testing, controlled deployments, configuration review, and remediation of identified security defects.

8. AI and Agentic Security

AxiaForce recognizes that AI-enabled and autonomous or semi-autonomous agents create security risks beyond traditional SaaS applications.

Security design for agentic workflows may include permission boundaries, tenant-scoped context, configurable approval and autonomy levels, restricted tool access, logging of agent actions, safeguards around credentials and connected systems, and controls designed to reduce unauthorized or unintended execution.

Customers are responsible for selecting autonomy levels, permissions, human-review requirements, and connected systems appropriate to their risk profile.

9. Logging, Monitoring, and Detection

AxiaForce maintains logging and monitoring capabilities appropriate to the Services to support operational visibility, security investigation, incident response, troubleshooting, and auditability.

Logging is designed to balance operational and security needs with data-minimization principles and protection of sensitive information.

10. Vulnerability and Patch Management

AxiaForce uses processes designed to identify, assess, prioritize, and remediate security vulnerabilities in systems under its control.

The timing and method of remediation depend on severity, exploitability, affected systems, provider dependencies, and operational risk. Third-party infrastructure and software may also be subject to the patching and vulnerability-management practices of the applicable provider.

11. Incident Response

AxiaForce maintains an internal incident-response process for identifying, triaging, containing, investigating, remediating, and learning from material security and privacy incidents.

Where an incident triggers customer-notification obligations, AxiaForce will provide notice in accordance with the applicable Agreement, Data Processing Addendum, and Applicable Data Protection Law.

12. Business Continuity and Recovery

AxiaForce uses backup, recovery, redundancy, and operational-resilience practices appropriate to the applicable Services and underlying infrastructure.

Recovery capabilities may depend on third-party cloud, database, storage, communications, and other infrastructure providers. Specific uptime, recovery-time, or recovery-point commitments apply only where expressly stated in an applicable SLA or Order Form.

13. Subprocessors and Vendor Security

AxiaForce relies on third-party providers for portions of its technology and service delivery. Material providers that Process Customer Personal Data on behalf of AxiaForce are managed as Subprocessors under the Data Processing Addendum.

AxiaForce maintains or is implementing vendor-review practices appropriate to the provider's role and risk.

AxiaForce maintains its material Subprocessor list as confidential operational and compliance information and makes it available to customers upon reasonable request. AxiaForce does not publicly disclose its complete provider stack or Subprocessor list.

14. Customer-Directed Integrations

Customers may connect AxiaForce to Microsoft 365, Google Workspace, CRM, ATS, telephony, storage, data, and other third-party systems.

Customer is responsible for authorizing these integrations, configuring permissions appropriately, and assessing third-party systems selected or controlled by Customer. A Customer-selected integration is not automatically an AxiaForce Subprocessor.

15. Payment Security

AxiaForce may use third-party payment processors for credit card, ACH, and recurring billing.

Payment-card information is intended to be handled through the designated payment processor's payment environment rather than stored as full payment-card credentials by AxiaForce unless expressly disclosed otherwise. Applicable payment-card compliance obligations of the payment processor remain subject to that provider's services and controls.

16. Data Minimization and Retention

AxiaForce seeks to limit Processing and retention of Customer Personal Data to what is reasonably necessary to provide, secure, support, and operate the Services, subject to the Agreement, Data Processing Addendum, legal requirements, and technical retention schedules.

Customer-controlled systems remain the primary systems of record where the applicable AxiaForce workflow is designed to synchronize results back to those systems.

17. Physical and Infrastructure Security

AxiaForce primarily relies on professional cloud and infrastructure providers for physical data-center security, environmental controls, network infrastructure, and related facilities protections.

AxiaForce does not represent that it directly operates the physical data centers used by the Services unless expressly stated otherwise.

18. Security Reviews and Customer Assurance

AxiaForce may provide reasonable security information to customers and prospects, including this Framework, the Data Processing Addendum, Subprocessor information, security questionnaires, and other documentation appropriate to the request.

Certifications, third-party audit reports, penetration-test reports, and similar materials will be represented only when they actually exist and apply to the relevant Services.

19. Security Reporting

Customers and security researchers may report suspected security issues to security@axiaforce.ai.

AxiaForce may request information reasonably necessary to investigate a reported issue. No authorization to conduct penetration testing, vulnerability scanning, or other intrusive testing is granted by this Framework.

20. Changes to this Framework

AxiaForce may update this Security Framework as the Services, security controls, architecture, providers, or risk environment evolve.

Material contractual security commitments are governed by the Agreement, DPA, Order Form, SLA, or separately executed Security Addendum rather than this informational Framework.

END OF SECURITY FRAMEWORK