BiMA·gov Procurement One-Pager

Last updated: 2026-05-06

Identity

Product: BiMA·gov (bi-modeling-automation). Vendor: BiMA·gov — sole proprietor. LLC formation in progress. Primary contact: legal@bimagov.com. Security contact: security@bimagov.com.

Hosting and residency

Fly.io, single region pinned to iad (Ashburn, Virginia, US-East). See /security.

Authentication

OIDC SSO supported (Microsoft Entra, Okta, Google Workspace). MFA enforced via the IdP. Session lifetime configurable per tenant; default 12 hours.

Authorization

RBAC roles: admin, reviewer, contributor, viewer. Entra group claim to BiMA·gov role mapping is on the roadmap (current: roles assigned per-user via the admin UI).

Audit

Hash-chained immutable log. Each row links to the previous via SHA-256. Exports: JSON, CSV, PDF. The PDF cover surfaces chain length, first hash, last hash, and break detection.

Encryption

At rest: AES-XTS-256 (LUKS) on persistent volumes (Fly default). In transit: TLS 1.2 or higher.

Sub-processors

Provider	Purpose	Data
Fly.io	Application hosting	Application data, customer model metadata
AWS	Encrypted backup storage (Fly volume snapshots)	Backup blobs only
Stripe	Billing	Customer billing contact, payment method
Anthropic	LLM fallback (Pro tier and above)	Ticket text, redacted DAX
Crisp	Support widget	Support chat transcripts
Plausible	Analytics	IP (transient, not stored), URL path

Backups

Fly volume snapshots stored in AWS S3, encrypted at rest. Restore tested quarterly (target cadence; not yet at full quarterly cadence — roadmap).

Retention

Audit logs: indefinite. Telemetry: 90 days. Customer model snapshots: 30 days, tenant-configurable.

Incident response

Best-effort 24-hour initial response. Sev-1 30-minute triage target. Postmortem published within 5 business days for any sev-1 or sev-2.

Vulnerability management

Dependency scanning via GitHub Dependabot, weekly updates across pip, npm, and GitHub Actions ecosystems. No formal pen-test cadence yet — roadmap.

Sub-processor change notice

30 days advance notice via /changelog or direct email to security/billing contacts.

Contract templates

Common Paper CSA (/legal/msa) and Common Paper Standard DPA (/legal/dpa).

Out of scope today

SOC2 (see /soc2 — Type 1 in scoping). Formal pen-tests. ISO 27001.