STABILITYLOGIC LLC

Enterprise Security Overview

How StabilityLogic protects applicant, operator, and corporate data across the platform. Written for enterprise security, procurement, and vendor-risk reviewers.

Version	v3.0
Effective date	February 16, 2026
Document owner	StabilityLogic LLC
Distribution	Non-confidential — safe to share with customer legal, security, and procurement teams

Contents

01 Executive Summary

StabilityLogic LLC operates a defense-in-depth security program covering the marketing site, the operator workspace, the Household Stability Index™ (HSI) scoring engine, and the audit trail. This document summarizes the controls a Fortune-500 vendor-risk team typically evaluates during procurement.

The controls described here are engineering commitments. Where an item is a target or a scheduled engagement rather than a completed attestation, it is explicitly labeled. StabilityLogic does not claim any regulatory certification or independent attestation that has not been formally achieved.

02 Architecture Overview

StabilityLogic is a multi-tenant SaaS application composed of a React frontend, a FastAPI backend, and a MongoDB primary datastore. All customer traffic terminates at a managed ingress with TLS 1.2+ enforced end-to-end.

Tenants are isolated at the data layer through per-organization identifiers on every document and enforced at the API layer through role-based access control (RBAC). Cross-tenant reads and writes are rejected before reaching the database.

- Application tier: FastAPI (Python 3.11), stateless request handlers behind a managed ingress.
- Data tier: MongoDB Atlas primary + secondary replicas, encrypted at rest (AES-256), TLS in transit.
- AI tier: HSI scoring engine and Anthropic-backed LLM analytics; no applicant PII is sent to third-party LLMs for scoring.
- Object storage: encrypted at rest; access via signed, time-bound URLs; audit-logged on every read and write.

03 Data Flow

A typical decision flow: (1) the applicant consents in the applicant portal; (2) the intake API stores minimum-necessary data in the tenant's isolated collection; (3) verified financial signals are fetched with explicit consent through the banking connector; (4) HSI computes a score and reason codes; (5) the operator reviews the recommendation and issues the final decision; (6) every state change is written to the audit log.

No applicant data leaves the primary application boundary except (a) transactional email through Resend for pilot notifications and adverse-action delivery, (b) SMS through Twilio under the A2P 10DLC-registered program, and (c) consented banking calls through Plaid. Each is contractually bound by a Data Processing Addendum and listed on the public subprocessors register.

04 Encryption

All customer traffic is protected with TLS 1.2 or higher; older versions are rejected at the ingress. All application secrets (API keys, database URIs, signing keys) are held in the managed secrets store and rotated on personnel change and on discovery of exposure.

- In transit: TLS 1.2+ enforced; older versions rejected at ingress.
- At rest: AES-256 for the primary database and object storage; disk-level encryption on all managed volumes.
- Application secrets: managed secrets store, rotated on personnel change and on discovery of exposure.
- Payment card data: not stored; payment providers handle their own PCI-DSS obligations.

05 Identity & Access Management

Human access to production is restricted to named engineers on the on-call rotation. Every access is auditable through the identity provider and the application audit trail. External customer users authenticate through the application with role-based access enforced at the API boundary.

- Employee access: least-privilege, named roles, MFA required, session-bound tokens.
- Customer users: bcrypt password hashing, JWT session tokens, RBAC (admin / landlord / applicant) with per-property scoping.
- SSO: OIDC available for pilot customers on request; SAML / SCIM on the enterprise roadmap.
- Break-glass: named engineers only; every break-glass event is logged and reviewed within one business day.

06 Logging & Monitoring

Every state change in the application — decision, share, export, admin action — is written to a structured JSON audit log that is retained per policy and available to enterprise customers under NDA. Operational monitoring covers request rates, error rates, latency percentiles, and dependency health.

- Application audit log: structured JSON, one record per state change, tenant-scoped, tamper-evident.
- Operational metrics: request rate, error rate, latency (p50/p95/p99), dependency health.
- Alerting: on-call rotation paged on error-rate and latency-SLO breach; incident classification per the Incident Response section.
- Log retention: aligned to the DPA retention windows; customer-scoped logs delivered on written request.

07 Incident Response

StabilityLogic operates a documented Incident Response Plan (IRP) with defined severity levels, response targets, and customer-communication cadence. Confirmed security incidents involving personal data trigger written customer notice within 72 hours, consistent with GDPR Article 33 and equivalent state statutes.

- P1 · Critical outage or confirmed security event: acknowledge ≤ 15 min; customer notice ≤ 1 hour, hourly updates.
- P2 · Major degradation of a core workflow: acknowledge ≤ 1 hour; customer notice ≤ 4 hours.
- P3 · Localized issue: acknowledge ≤ 4 business hours; next-business-day summary.
- Every P1 and P2 event closes with a written post-incident review sent to impacted customers.

08 Disaster Recovery

The disaster recovery program targets Recovery Point Objective (RPO) ≤ 15 minutes and Recovery Time Objective (RTO) ≤ 4 hours for the primary production environment. Backups are encrypted at rest and in transit; restore exercises are performed at least twice per year.

- RPO target: ≤ 15 minutes (point-in-time recovery on the primary database).
- RTO target: ≤ 4 hours to restore the HSI scoring API, operator application, and audit trail.
- Backup cadence: continuous point-in-time + daily encrypted snapshot retained per policy.
- Validation: restore exercises twice per year, results feed the annual BCP tabletop.

09 Vendor Management

Every subprocessor is contractually bound by a Data Processing Addendum equivalent to or stronger than the customer-facing DPA. StabilityLogic publishes the authoritative subprocessors register at stabilitylogic.com/subprocessors and provides at least thirty (30) days written notice of any material change.

- Onboarding: documented risk review covering data category, jurisdiction, security controls, and business-criticality.
- Ongoing: annual DPA review; SOC 2 / ISO 27001 or equivalent evidence collected where the vendor provides it.
- Objection window: enterprise customers may object to a change during the 30-day notice window per the executed DPA.
- Register: Company · Purpose · Jurisdiction · Data category, updated whenever subprocessors change.

10 Infrastructure Overview

StabilityLogic runs on a managed cloud platform in United States data-center regions. The application tier is deployed on a managed Kubernetes environment with autoscaling; the primary database (MongoDB Atlas) is deployed multi-availability-zone with automatic failover.

Named cloud provider and region details are disclosed to enterprise counterparties under NDA during the pilot scoping conversation. The subprocessors register lists every vendor that participates in the runtime.

11 Security Roadmap

The items below are engineering targets and scheduled engagements. None should be read as achieved certifications until the underlying report or attestation has been published.

- Q1 2026 — Internal control mapping refresh · annual IRP tabletop · backup restore exercise · scheduled.
- Q2 2026 — Third-party penetration test · scheduled. SOC 2 Type I readiness assessment · scheduled (no attestation issued yet).
- Q3 2026 — SOC 2 Type I audit window · target. GDPR / CCPA subject-request portal · target. Bug-bounty program launch · target.
- Q4 2026 — SOC 2 Type II observation window begins · target. Fair-housing external audit · scheduled.

12 Responsible Disclosure

Coordinated disclosure is welcomed from independent security researchers at security@stabilitylogic.com. Acknowledgement within 3 business days; initial triage severity and expected remediation communicated within 10 business days; coordinated public disclosure requires 90 days from initial report or joint agreement.

Good-faith research consistent with this policy will not be pursued through legal action. Out of scope: physical attacks, social engineering, denial-of-service testing, testing against third-party subprocessors. A public bug-bounty program is a planned enhancement; timing appears in the roadmap above.