StabilityLogic Enterprise Security Overview

Version 2.0 · Published July 07, 2026 · Non-confidential.
Prepared for enterprise vendor-risk intake by security, procurement, and legal reviewers. For a full vendor-security questionnaire (SIG, CAIQ, or a custom template): aqueelah@stabilitylogic.com.

This document describes the information-security posture of the StabilityLogic decision-infrastructure platform, including the Household Stability Index™ (HSI) engine, the AI Decision Support layer, and the operator workspace where housing providers review recommendations and issue the final rental decision. Roadmap items are explicitly labeled and represent engineering commitments — not certifications already obtained. StabilityLogic does not claim any regulatory certification or independent attestation that has not been formally achieved.

1. Security architecture

The StabilityLogic platform is a modern web application composed of a Python/FastAPI backend, a React frontend served over HTTPS, and a MongoDB persistence layer. The backend is deployed on the Emergent Cloud Platform behind a managed ingress terminating TLS. Application code, configuration, and infrastructure definitions are stored under version control with reproducible deployment pipelines. Third-party services are integrated only through a documented provider-abstraction layer to keep vendor coupling explicit and auditable.

2. Encryption

Encryption is enforced at every layer where customer data traverses or is stored.

- In transit: TLS 1.2 or higher on all public endpoints; HTTPS is required for the marketing site, application API, and operator workspace.
- At rest: encryption is enabled on the primary MongoDB data store and on backup volumes.
- Application secrets: API keys, provider tokens, and JWT signing keys are stored outside application code, injected at runtime through the environment, and never committed to source control.
- Client-side storage: session tokens are held in browser storage with short expiries; no applicant data is persisted client-side.

3. Authentication

Authentication is credential-based for humans and token-based for API calls.

- Passwords are hashed with bcrypt before storage; plaintext passwords are never persisted or logged.
- Session tokens are JSON Web Tokens (JWT) with configurable expiry and rotation-capable signing keys.
- Rate-limit and lockout protections apply to authentication endpoints to reduce brute-force exposure.
- Enterprise Single Sign-On (SAML/SCIM) is scoped as a roadmap item — see Section 12. Interim OIDC integration is available under pilot terms.

4. Authorization

Access to platform functionality is granted through explicit role and scope checks.

- Role-based access control (RBAC) across three primary roles: Administrator, Landlord/Operator, and Applicant.

- Every authenticated route asserts role or membership before returning data; unauthorized calls return HTTP 401/403 without leaking existence.
- The internal Pilot CRM, Executive Brief, and AI Opportunity Brief endpoints are restricted to Administrator role.
- Operator actions (score view, override, note, tag change, status transition) are scoped to the operator's organization membership.

5. Audit logging

The audit log is a first-class product surface, not an afterthought.

- Every scoring decision is stamped with the HSI model version and weight configuration used to produce it — recommendations are reproducible weeks or years later.
- Every override of an HSI recommendation, and the rationale entered by the operator, is written to the audit log.
- Every internal note, tag change, pipeline-status transition, and export in the operator workspace is written to the audit log.
- The audit log is queryable for compliance review and is retained for the duration required to defend a rental decision under applicable federal, state, and local law.

6. Infrastructure overview

The platform runs on the Emergent Cloud Platform, a managed Kubernetes environment operating in the United States. Persistent data is stored in MongoDB (managed cluster, encrypted at rest). Application traffic is fronted by a managed ingress that terminates TLS and applies rate limiting. Automated pipelines rebuild and redeploy the application on every merge to the main branch; infrastructure changes are reviewed and applied declaratively. A limited number of named engineers hold production access; production access is logged.

7. Incident response

StabilityLogic maintains a written incident-response runbook that covers detection, triage, containment, notification, and post-incident review. On confirmation of a data incident affecting a specific customer, StabilityLogic will notify that customer without undue delay and in any event within seventy-two (72) hours of confirmation, providing the information reasonably necessary for the customer to meet its own notification obligations under applicable law. A written post-incident summary is delivered to affected enterprise customers with the corrective actions taken.

8. Disaster recovery

Business-continuity objectives are scoped per pilot in the operator success plan and documented in the executed order form.

- Automated database backups are taken on a defined cadence and stored encrypted; restore procedures are tested on a regular schedule.
- Application code, configuration, and infrastructure definitions are stored under version control; deployments are reproducible from source.
- Target recovery-time and recovery-point objectives (RTO/RPO) are agreed with each pilot partner in writing before go-live.

9. Data retention

Retention is calibrated to the minimum period necessary to defend a rental decision under applicable law, plus any additional period expressly requested by the housing provider. On termination of the underlying agreement, customer data is returned or hard-deleted per the executed Data Processing Agreement (DPA), subject to ongoing legal-hold obligations where they apply. Applicant-facing deletion requests are routed through the housing provider, who acts as the Controller.

10. Tenant isolation

The platform is multi-tenant with logical isolation enforced at the application layer.

- Every organization holds a unique organization identifier; every applicant, decision, note, tag, and audit record is stamped with that identifier at write time.
- All read paths filter by the requesting user's organization membership; cross-tenant reads are impossible through the public API.
- Administrator-role access can span tenants only through explicit administrative endpoints, which are themselves logged.
- Dedicated infrastructure (single-tenant hosting) is available on request under enterprise terms.

11. Vulnerability management

Security posture is maintained continuously, not annually.

- Dependency scanning: application dependencies are monitored for known vulnerabilities, and critical advisories are patched on an expedited cadence.
- Static analysis and lint gates run on every merge to the main branch.
- A third-party penetration test is scheduled as part of the roadmap in Section 12; findings will be tracked to closure and summarized to enterprise customers under NDA.
- Responsible disclosure — see Section 13 — provides an external reporting channel for security researchers.

12. Planned SOC 2 readiness timeline

The following items reflect engineering intent. Target windows will be updated as engagement letters are signed. None of the items below should be read as an achieved certification until the underlying report or attestation has been published.

- SOC 2 Type I readiness assessment — target window Q2 2026. Auditor engagement to be disclosed upon signature.
- Third-party penetration test — target window Q2 2026.
- SOC 2 Type I attestation — target window Q3 2026.
- Enterprise SSO (SAML / SCIM) — target window Q4 2026; interim OIDC integration available under pilot terms.
- Public status page with historical uptime — shipped; live at stabilitylogic.com/status.
- SOC 2 Type II attestation — under evaluation for 2027, contingent on completion of the Type I cycle.

13. Responsible disclosure

StabilityLogic welcomes reports from security researchers acting in good faith.

- Reports may be sent to **security@stabilitylogic.com**. Please include reproduction steps, affected endpoint, and expected impact.
- StabilityLogic will acknowledge receipt within two (2) business days and will provide status updates as remediation progresses.
- Researchers who follow responsible-disclosure practice — no data exfiltration, no service disruption, no public disclosure prior to remediation — will not be pursued through legal channels for the report itself.
- A formal public bug-bounty program is under evaluation and, if launched, will be linked from the Trust Center.

14. Contact information

For any security, privacy, or compliance question raised during vendor-risk review, please contact us using the addresses below. Every legitimate inquiry receives a response.

- Security reports: **security@stabilitylogic.com**
- Privacy, data-subject requests: **privacy@stabilitylogic.com**
- Vendor-risk / procurement: **aqueelah@stabilitylogic.com**
- General: **aqueelah@stabilitylogic.com** · (818) 805-0068
- Mailing address: StabilityLogic LLC, 3411 W Stanton Ave, Fullerton, CA 92833, United States.

This overview is non-confidential and may be shared internally with a buyer's security, risk, procurement, and legal teams. Under an executed NDA, extended architecture diagrams, detailed control mappings, and completed vendor-security questionnaires (SIG, CAIQ, or a custom template) are available on request. The current authoritative sub-processors register is published at stabilitylogic.com/subprocessors.