Parable Security

DOCUMENT
Security Overview

Built for security teams. Multi-tenant by design.

Parable handles sensitive employee data and runs on behalf of security teams. This document summarizes the controls that protect customer data — from tenant isolation and SSO, through input handling and webhook integrity, to audit logging and deletion.

SOC 2 Type II — audit in progress | WorkOS-backed SSO / SCIM | GDPR-aligned data handling

ARCHITECTURE & DATA PROTECTION

Multi-tenant isolation, defense in depth

Postgres row-level security on every tenant table. All reads and writes are filtered by organization_id server-side, regardless of client. Dedicated isolation tests run on every build.

Identity & SSO

WorkOS-backed SSO and SCIM support Okta, Microsoft Entra, Google Workspace, OneLogin, and any SAML IdP. Role-based access (admin/member) per organization. Platform-admin access is restricted to an explicit allowlist.

Encryption

TLS 1.2+ in transit. AES-256 at rest via managed Postgres. Database backups are encrypted and retained per the provider's standard policy.

Audit log

Every privileged action — member invites, role changes, campaign sends, template edits — is recorded with actor, target, IP, and metadata. One-year retention by default, enforced by a scheduled purge. Longer retention available on request.

Secrets & data handling

No secrets in source code or the client bundle. Only public anon keys and URLs are exposed to the browser. Server-side keys are environment-scoped per deployment.

Data deletion

Cascade deletes ensure removing an organization removes all child records. Customer-initiated data deletion supported on request.

APPLICATION & OPERATIONAL SECURITY

Webhook integrity

All inbound webhooks — Twilio, Resend, WorkOS — verify HMAC signatures with timing-safe comparison and replay-window enforcement. Unsigned requests are rejected.

Rate limiting

Per-endpoint limits on authentication, AI generation, and outbound dispatch. Per-organization concurrency caps prevent abuse. Distributed (Redis-backed) where deployed; in-memory fallback otherwise.

Input handling

Parameterized database queries throughout. All user-supplied HTML passes through a strict DOMPurify allowlist before render. No eval, no string-built SQL.

HTTP hardening

Strict-Transport-Security (1 year, includeSubDomains), Content-Security-Policy, X-Frame-Options: DENY, X-Content-Type-Options: nosniff, strict Referrer-Policy, restrictive Permissions-Policy.

Outbound safety

Server-side egress is restricted to an HTTPS allowlist (SSRF mitigation). Internal IP ranges and metadata endpoints are blocked at the request layer.

Build & code quality

TypeScript in strict mode. Dedicated security test suite covering authorization, tenancy isolation, input validation, and rate limiting. Dependency audit on every build.

COMPLIANCE ROADMAP

Parable is undergoing a SOC 2 Type II audit. Our posture is informed by the frameworks our customers operate under — HIPAA, PCI DSS, NIST CSF 2.0, ISO 27001, CMMC, and GDPR. A vendor security questionnaire and DPA are available on request.

How Parable maps to customer compliance frameworks →

RESPONSIBLE DISCLOSURE

Found a security issue? We welcome reports from researchers and customers. Please email us with details and reproduction steps; we acknowledge within one business day.

security@parablesecurity.ai