SiteRecord

Security & Procurement Overview

SiteRecord · Version 1.0 · Reviewed 2026-11-01 · siterecord.io/security

Product overview

SiteRecord is a SaaS web application for website accessibility monitoring and remediation management. It helps organizations identify accessibility findings, assign and track remediation, record verification, and maintain exportable evidence of their work.

Security controls

- **Data protection:** HTTPS/TLS is enforced in transit. Nightly backups are stored as encrypted archives. Customer evidence attachments are restricted to authorized users only.
- **Identity & authentication:** Email/password plus Google and Microsoft sign-in. Enterprise SSO (OIDC) is available on the Organization plan. Passwords are stored hashed.
- **Access controls:** Workspace and website roles (owner, member, viewer) gate every data access. External auditor access is read-only, optionally expiring, and revocable.
- **Application security:** CSRF protection on state-changing requests, prepared SQL statements, output escaping, file-upload validation, and scan-target validation that blocks private/reserved network addresses (SSRF protection).
- **Monitoring & auditability:** Accessibility work history (assignments, corrections, verifications) is appended per finding. Security-relevant events are logged for administrator review.
- **Backup & recovery:** Nightly encrypted backup bundles of application data. Restoration procedures exist as part of deployment operations.

Data processing and retention

- SiteRecord stores account details (name, email), workspace and website configuration, monitored page lists, scan results and findings, finding history, uploaded evidence attachments, subscription and billing status (card details are handled by Stripe, not stored by SiteRecord).
- Scan results are generated from the pages you choose to monitor. Imported findings (Siteimprove, Tenon, or generic JSON/CSV) are reviewed before they count and are distinguished from SiteRecord-generated scans.
- Uploaded evidence is stored as files with access limited to authorized workspace users and included in exports you generate.
- Reports, evidence packages, and ZIP exports can be generated by authorized users; paid plans include advanced reports and PDF/ZIP evidence exports.
- When a website or account is deleted, its records are removed from active use. Retention and deletion specifics are described in the Privacy Policy.
- The Ask SiteRecord assistant may send the text of your question and selected finding context to the AI provider to generate an answer. Customer data is not used to train models operated by SiteRecord; refer to the AI provider's API data-use terms.

Service providers (subprocessors)

Hosting	Linux cloud virtual server (Ubuntu 24.04, nginx, PHP-FPM, MySQL). Application data is stored on that host.
Email delivery	Resend (transactional email; receives recipient addresses and message content for delivery).
Payment processing	Stripe (billing for paid plans; receives billing contact and payment details; SiteRecord does not store card numbers).
Authentication	Google and Microsoft sign-in (OAuth; receive authentication assertions for users who sign in that way). Optional enterprise OIDC on the Organization plan.
AI assistant	OpenAI (Ask SiteRecord questions and selected finding context are sent to generate answers; not used by SiteRecord to train models).

Access and accountability

- Website roles: owners manage the site, members work findings, viewers read only.
- Workspace administration: Organization plan adds member/role administration and optional SSO.
-

External auditor access: read-only invitations to selected websites, with optional expiry and instant revocation.
- Activity history: per-finding records of assignment, correction, and verification. These document accessibility work; they are not a substitute for security audit logs.

Accessibility and conformance documentation

Accessibility is a core product consideration. An Accessibility Conformance Report (ACR/VPAT) has not yet been completed; documentation requests can be sent to security@siterecord.io.

Procurement reference

Legal entity	Pacolet Studios LLC
Business address	PO Box 1, Tryon, NC 28782, United States
Product name	SiteRecord
Product website	https://siterecord.io
Product category	Cloud-based website accessibility monitoring and remediation management software
Service delivery model	SaaS
Deployment model	Web-based application
Subscription structure	Free, Pro, and Organization
Public pricing	https://siterecord.io/#pricing
Privacy Policy	https://siterecord.io/privacy
Terms of Use	https://siterecord.io/terms
Security & procurement contact	security@siterecord.io

Frequently asked questions

Where is customer data hosted?
On a cloud-hosted Linux server running the SiteRecord application (Ubuntu 24.04), with encrypted nightly backups stored by the application.

Is data encrypted in transit and at rest?
In transit: HTTPS/TLS is enforced. At rest: nightly backups are encrypted; live database storage relies on host disk encryption at the infrastructure level.

Does SiteRecord support MFA?
Optional multi-factor authentication is available on all plans using an authenticator app (TOTP) plus one-time recovery codes. Enrollment is voluntary — existing users are not required to enable it. SSO on the Organization plan can also enforce your identity provider's MFA.

Does SiteRecord support SSO?
Yes — enterprise OIDC single sign-on is available on the Organization plan, and Google/Microsoft sign-in on every plan.

Can access be restricted by user role?
Yes. Website roles (owner, member, viewer) and external auditor read-only access control what each user can see and do.

Can customers export their data?
Yes. Authorized users can generate reports and evidence exports; paid plans add advanced reports and PDF/ZIP evidence packages.

What happens to data after account deletion?
Deleted records are removed from active use. See the Privacy Policy for retention details.

Does SiteRecord use subprocessors?
Yes — hosting, email delivery (Resend), payments (Stripe), OAuth sign-in (Google/Microsoft), and the AI assistant (OpenAI) are listed on this page with the data each handles.

Are backups performed?
Yes — nightly encrypted backup bundles of application data.

How are security incidents handled?
Issues can be reported to security@siterecord.io or support@siterecord.io; we investigate and remediate confirmed issues, deploying fixes through our normal change process.

Is a SOC 2 report available?

No — SiteRecord does not currently have a SOC 2 report. This page describes verified implemented controls instead.

Is an Accessibility Conformance Report (VPAT) available?
An ACR has not yet been completed. Accessibility of the SiteRecord application is a product consideration; documentation requests can be made via the contact below.

Can our procurement team request additional documentation?
Yes — use the request form on this page or email security@siterecord.io. Available items include this overview, policies, and answers to specific questions.

This document describes implemented controls verified on 2026-11-01. It is not a certification, audit report, or contractual commitment. Confidential vendor documents (W-9, insurance certificates) are available on request where they exist. Questions: security@siterecord.io.