Coastline CRM security questionnaire

Last updated 2026-07-30 · coastlinecrm.com/security · security@coastlinecrm.com

The questions vendor security reviews ask most often, answered in advance. Every answer describes a control that exists in the product today. Where a control does not exist yet, this document says so rather than leaving the question out.

COMPANY AND PRODUCT

What does the product do, and who uses it?

Coastline CRM is a web application for service businesses to manage customers, jobs, estimates, invoices, scheduling, and communication. Users are the business's own staff, plus limited-scope portal access for their customers and subcontractors.

Where is the application hosted?

On managed cloud infrastructure operated by providers holding SOC 2 Type II attestations, running on Amazon Web Services. Coastline does not operate physical servers.

Is there a published list of subprocessors?

Yes, at coastlinecrm.com/security, naming every provider that processes customer data and what each one can see.

TENANT ISOLATION

How is one customer's data kept separate from another's?

By row-level security enforced in the database engine, not by filters in application code. Every table carries policies scoping rows to the owning workspace, and those policies apply even to the database owner account. A query that omits a workspace filter returns nothing rather than another tenant's rows.

What prevents a developer from accidentally creating an unprotected table?

A database-level event trigger enables row-level security on every newly created table automatically. A table with no policy written for it is fully locked rather than fully open, so the failure mode of forgetting is denial of access, not disclosure.

Is the database shared between customers?

Yes, this is a multi-tenant application on shared infrastructure, with isolation enforced as described above.

ENCRYPTION

Is data encrypted in transit?

Yes. All traffic is served over TLS, and the application is available over HTTPS only.

Is data encrypted at rest?

Yes. Databases, file storage, and backups are encrypted at rest with AES-256 by the infrastructure providers.

How are third-party credentials protected?

OAuth tokens for connected email, calendar, and accounting accounts are encrypted with AES-256-GCM using a key held outside the database before being stored, so a database copy alone does not yield usable tokens. Integration API secrets are held in a dedicated secrets vault rather than in ordinary application tables.

How are API keys stored?

As SHA-256 hashes. The plaintext key is shown once at creation and never stored, so it cannot be recovered from the database.

AUTHENTICATION AND ACCESS CONTROL

Is multi-factor authentication supported?

Yes. Time-based one-time password (TOTP) two-factor authentication works with any standard authenticator app, is available to every user on every plan at no additional cost, and is backed by single-use recovery codes stored as keyed hashes.

Can MFA be enforced for all users in an organization?

Yes. An administrator can require two-factor authentication workspace-wide; users without it are required to enroll before they can continue working. Administrators can see how many users have not yet enrolled.

Is single sign-on supported?

Google and Microsoft sign-in are supported. SAML-based enterprise SSO is not currently offered.

How granular is the permission model?

Over 110 individually-controlled permissions, assembled into roles that each organization defines. Access checks test for a specific permission rather than a role name, so renaming or adding a role cannot inadvertently widen access.

How quickly is access revoked when someone leaves?

Immediately. Removing a member blocks sign-in and invalidates sessions already open; the database-level policies stop returning that user any workspace data at the same moment.

What is the password policy?

Passwords are handled by the managed authentication platform, stored using industry-standard one-way hashing, with a minimum length requirement and rate limiting on failed sign-in attempts. Coastline staff cannot read user passwords.

PAYMENT DATA

Does the vendor store cardholder data?

No. Card numbers, security codes, and bank account numbers are never stored; no such field exists in the database schema.

How are payments processed?

By Stripe, a PCI DSS Level 1 service provider. Payment details are captured by Stripe's own hosted components, so sensitive values do not pass through Coastline systems.

LOGGING AND MONITORING

Are administrative actions logged?

Yes. Changes to roles, permissions, member access, and security settings are written to an append-only audit log that the application has no ability to update or delete, and which administrators can review in-product.

Is there tamper-evident logging anywhere?

Yes. Electronic signature audit trails are cryptographically hash-chained: each event incorporates the hash of the preceding event, and the chain is verified on read, so a modified or removed event is detectable rather than silent.

Is application error monitoring in place?

Yes, via a third-party error monitoring service that receives technical diagnostics and an account identifier, not record contents.

SECURE DEVELOPMENT

Is there a code review process?

Yes. Changes land through pull requests with review, automated type checking, and an automated build gate before merge.

Are security reviews performed?

Yes. Periodic internal security audits are run against the codebase, with findings tracked to remediation. The most recent full review produced 30 findings, all of which were remediated and deployed.

Has a third-party penetration test been performed?

Not to date. This is planned but has not happened, and we would rather state that than imply otherwise.

Are incidents documented?

Yes. Production incidents receive written post-incident reports retained internally, including root cause and the specific controls added to prevent recurrence.

DATA HANDLING AND RETENTION

Can customers export their data?

Yes, while the account is active.

What happens when an account is deleted?

Deletion runs on a 30-day grace period during which it can be reversed, protecting against accidental or malicious deletion. After that window personal information is permanently anonymized.

Is customer data used to train AI models?

No. AI features process only the specific record or text a user invokes them on, at the moment of the request. Workspace contents are not used for model training.

Is customer data sold or shared with advertisers?

No.

COMPLIANCE STATUS

Does Coastline hold a SOC 2 attestation?

Not currently. The underlying infrastructure providers (cloud hosting, database platform, payment processor) each maintain SOC 2 Type II attestations, but Coastline has not completed its own audit. We state this directly rather than relying on the infrastructure's certifications to imply our own.

Is a Data Processing Agreement available?

Not yet. One is being prepared. If you need a DPA to complete a vendor review, contact security@coastlinecrm.com and we will work with you on timing.

How are vulnerability reports handled?

Reports go to security@coastlinecrm.com and are acknowledged within two business days. Good-faith researchers who allow a reasonable remediation window and avoid accessing other customers' data will not face legal action.

SUBPROCESSORS

Every company that processes customer data on Coastline's behalf.

Used for every workspace

PROVIDER	PURPOSE	DATA IT CAN SEE
Supabase	Database, authentication, and file storage	All workspace records and uploaded files
Vercel	Application hosting and content delivery	Requests in transit; no persistent copy of workspace records
Amazon Web Services	Underlying cloud infrastructure for the services above	Encrypted storage and compute for the platforms built on it
Stripe	Subscription billing and customer payment processing	Billing contact details and payment instruments; card numbers are held by Stripe and never by Coastline
Resend	Delivery of automated email such as notifications and receipts	Recipient address and the contents of the message being sent
Anthropic	AI assistance features, reached through Vercel AI Gateway	Only the specific record or text you invoke an AI feature on; not used to train models
Sentry	Application error monitoring	Technical error diagnostics and an account identifier; not record contents

Used only when the related feature is enabled

PROVIDER	PURPOSE	DATA IT CAN SEE
Unipile	Connecting your email and calendar accounts (only if you connect one)	Messages and events in the mailbox or calendar you connect
Nylas	Calendar synchronization for existing connections	Events in the calendar you connect
Twilio	Text messaging and calling (only with messaging or voice enabled)	Phone numbers and message or call contents
xAI	AI voice agent (only with the voice add-on enabled)	Audio and transcripts of calls handled by the voice agent

Intuit QuickBooks	Accounting synchronization (only if you connect it)	Invoices, payments, and customer billing records you choose to sync
Google	Maps and address lookup, and calendar access if you connect a Google account	Addresses being looked up; calendar events if connected
Regrid	Property parcel data lookup	Property addresses being looked up
RoofScope	Measurement reports (only if you order one)	The property address the report is ordered for