StatecraftCRM

STATECRAFTCRM.COM

NOVEMBER 2026

Security & Infrastructure Overview

StatecraftCRM is a relationship, issue, and institutional knowledge platform for government affairs, public affairs, and external affairs teams. This overview summarizes the technical and operational controls Statecraft uses to protect customer workspace information and describes how the service operates today.

CONTENTS

01 Security at a Glance
02 Application & Infrastructure
03 Tenant Isolation & Authorization
04 Identity & Access
05 Data Protection
06 Customer Data Ownership
07 Statecraft Personnel Access
08 Audit & Administrative Records
09 Backup & Recovery
10 Data Export, Termination & Deletion
11 Security Incident Response
12 AI Use
13 Service Providers
14 Support
15 Security Contact

ABOUT THIS DOCUMENT

This document is provided for evaluation and procurement. It is not a third-party certification or audit report, and it does not create contractual commitments. Contractual terms are set by the customer agreement and Statecraft's Terms of Service.

01

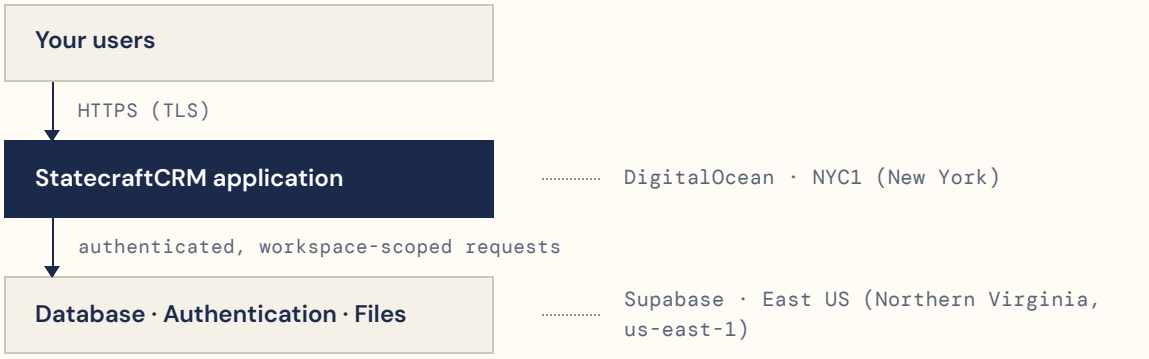
Security at a Glance

TENANT ARCHITECTURE Each customer workspace is a separate tenant. Access is checked against workspace membership on the server and in the database.	**ENCRYPTION IN TRANSIT** All traffic to the service uses HTTPS (TLS), with HTTP Strict Transport Security enforced.
MANAGED INFRASTRUCTURE Managed PostgreSQL database, authentication, and file storage. Cloud application hosting.	**ROLE-BASED ACCESS** Admin, Editor, and Viewer roles in every workspace.
MULTI-FACTOR AUTHENTICATION Authenticator-app (TOTP) MFA. Privileged Admin operations require a verified second factor, enforced on the server.	**SINGLE SIGN-ON** Enterprise SAML SSO for explicitly invited users.
AUDIT RECORDS Server-side records of membership, role, invitation, export, and material deletion events.	**BACKUP AND RECOVERY** Daily database backups, weekly host backups, and documented recovery procedures.
DATA PORTABILITY Workspace Admins can export workspace data in JSON format.	**OFFBOARDING** Documented, verified deletion process. Live workspace data is targeted for deletion within 30 days of a verified request.
PERSONNEL ACCESS No routine access to customer content. Access is limited to defined purposes and named operators.	**AI** Optional and user initiated. Workspace information is not used to train models.

02

Application & Infrastructure

StatecraftCRM is a web application. Users connect over HTTPS to the StatecraftCRM application, which verifies each request and reads or writes data only within the user's workspace.



COMPONENT	PROVIDER	PRIMARY LOCATION
Application hosting	DigitalOcean	NYC1 (New York)
Database (PostgreSQL), authentication, file storage	Supabase	East US, Northern Virginia (us-east-1)
Web server and TLS termination	Nginx with automatically renewed TLS certificates	Application host
Application runtime	Supervised application processes under a dedicated, non-login service account	Application host

Workspace records are stored in the managed database. The application host runs the service and holds operational logs; it is not the system of record for workspace content.

The locations above describe Statecraft's primary infrastructure. Supporting providers listed in Section 13 operate their own infrastructure under their own terms.

03

Tenant Isolation & Authorization

Every customer workspace is a separate tenant. Statecraft enforces that separation at several layers:

- **Membership is the boundary.** Access to a workspace requires a membership record in that workspace. The server derives each user's identity from a verified session and never relies on workspace identifiers supplied by the browser.
- **Database row-level controls.** Database policies limit what a signed-in user can read and write to rows belonging to their own workspace.
- **Independently scoped server operations.** Operations that run with elevated database privileges, such as workspace export, AI briefings, and administrative actions, verify the user's membership and role first and then query only that workspace.
- **Validated relationships.** Links between records, such as a contact and its organization, are validated so that a record cannot be connected to another workspace's records.
- **Controlled deletion.** Deletion of core records (contacts, organizations, issues, interactions, and policy items) runs through server-side operations that verify role and workspace before acting.

These controls are covered by Statecraft's automated test suite, including tests that attempt cross-workspace access.

04

Identity & Access

SIGN-IN OPTIONS

- Email and password
- Enterprise SAML single sign-on for explicitly invited users. SAML SSO has been verified with Microsoft Entra ID.

MULTI-FACTOR AUTHENTICATION

Users can enroll an authenticator app (TOTP). Privileged Admin operations require a session verified with MFA, and this is enforced on the server rather than only in the interface. These operations include:

- inviting members and revoking invitations
- changing roles and removing members
- exporting workspace data
- managing billing and seats

Admins who sign in through SSO complete the same second-factor step before performing these operations.

INVITATION-CONTROLLED MEMBERSHIP

Membership and role are set by invitation from a workspace Admin. Authenticating through an organization's identity provider does not, by itself, create an account or grant access to a workspace. A user who authenticates through SSO without an invitation is not admitted.

ROLES

ROLE	ACCESS
Admin	Manages members, roles, invitations, export, and billing. Full record access.
Editor	Creates and edits workspace records.
Viewer	Reviews workspace records without editing them.

The service also prevents a workspace from losing its last Admin through removal or demotion.

REMOVING ACCESS

When an Admin removes a member, the member's workspace authorization ends on the server.

> **Current scope.** Membership and roles are managed within StatecraftCRM. Automatic provisioning, deprovisioning, or role and group synchronization from an identity provider is not currently offered.

05

Data Protection

In transit. All connections to StatecraftCRM use HTTPS (TLS). HTTP Strict Transport Security instructs browsers to connect only over HTTPS. Authentication cookies are marked Secure. The application connects to its database, authentication, and storage services over encrypted connections.

At rest. Supabase provides Statecraft's managed PostgreSQL database, Auth, and Storage services and documents encryption of hosted customer data at rest. Supabase security documentation

APPLICATION SAFEGUARDS.

- Server-side authorization on every workspace operation
- MFA required for privileged Admin operations
- Request validation and rate limits on sensitive and resource-intensive operations
- Browser security protections, including a Content Security Policy and clickjacking protection
- Application secrets held in protected server configuration, outside source code
- Operational logs designed to exclude passwords, tokens, and request bodies

Payments. Payment card details are processed by Stripe. Statecraft does not store complete payment card numbers.

06

Customer Data Ownership

> Customers own the content they place in StatecraftCRM. Statecraft does not claim ownership of customer workspace content.

Statecraft uses customer content to provide, support, secure, and recover the service, as described in its Terms of Service.

A workspace Admin can download a JSON export of the workspace's supported records at any time.

07

Statecraft Personnel Access

> *Can Statecraft see our data?*

Statecraft personnel do not routinely access customer workspace content. Access occurs only when necessary to:

- provide support a customer has requested
- operate or secure the service
- investigate a security incident
- perform recovery
- satisfy a legal obligation

When access is needed, it is limited to the minimum scope and duration required and is performed by named Statecraft operators using protected accounts. For discretionary support inspection, Statecraft obtains customer authorization where practical. Emergency access during an outage or security event is documented and reviewed afterward. Operator access is recorded in a restricted internal record that captures purpose and scope without copying customer content.

08

Audit & Administrative Records

Statecraft maintains server-side audit records for security- and administration-relevant workspace actions, including:

- membership and role changes
- workspace data exports
- invitation lifecycle events
- material record deletions
- MFA enrollment changes

Audit records are written by the server and typically capture the acting user, the action, the time, and the affected item. Workspace users cannot create, edit, or delete audit records through the application.

09

Backup & Recovery

Statecraft maintains documented recovery procedures for host loss, database loss or corruption, faulty releases, and credential compromise.

LAYER	CURRENT CONFIGURATION	APPROXIMATE RECOVERY CHARACTERISTICS
Database (Supabase)	Daily physical backups.	Recovery point up to about 24 hours
Application host (DigitalOcean)	Weekly host backups, with 28-day retention observed	Recovery point up to about 7 days; restoration in about 2 to 4 hours
Application releases	Automated rollback to the previous release	Rollback in minutes

Because workspace records live in the database, the database backup schedule is the primary measure for customer data. Database backups and uploaded-file storage are handled separately.

These figures describe current operational configuration and internal recovery estimates. They are not contractual service levels unless separately agreed.

10

Data Export, Termination & Deletion

Before leaving. A workspace Admin can export workspace data at any time. Statecraft offers the export again as part of offboarding.

DELETION PROCESS.

01	A workspace Admin requests deletion. Statecraft verifies the requester's identity and current Admin role.
02	Statecraft offers the workspace export and agrees an access end date with the customer.
03	Outstanding support matters, and any security, legal, billing, or dispute holds, are reviewed before deletion.
04	Access ends at the agreed time.
05	Live workspace data is targeted for deletion within 30 days of the verified request, subject to documented exceptions for those holds.

Backups. Historical backups are not selectively purged. They expire on the providers' established rotation schedules after live deletion.

Retained records. Statecraft may retain limited audit and security evidence for 12 months after termination or deletion by default, subject to documented security, legal, dispute, or business-record requirements. Billing records are retained separately as required.

11

Security Incident Response

Statecraft maintains an operational incident process covering:

- investigation and severity assessment
- containment
- scope determination
- evidence preservation
- customer impact assessment
- customer communication

If a confirmed incident materially affects customer data, Statecraft will notify affected customers without undue delay, consistent with applicable contractual and legal obligations. Notifications describe what is known, the data and dates affected, containment steps, any recommended customer actions, and a point of contact, with updates as the investigation develops.

12

AI Use

AI in StatecraftCRM is **optional** and **user initiated**. Nothing is sent to an AI provider unless a user chooses to generate a briefing.

Contact briefings. When a user requests a briefing on a contact, StatecraftCRM sends selected, relevant workspace context to Anthropic's commercial API. Depending on the record, this can include:

- contact and organization details, and relationship attributes
- notes
- recent interaction summaries, outcomes, and next actions
- linked issues
- the meeting details the user provides

Only context relevant to the requested briefing is sent. Free-text notes may contain any information users have entered.

HANDLING.

- The generated briefing is streamed to the user and is not stored as a StatecraftCRM record.
- Statecraft does not use workspace information to train AI models.
- Anthropic states that inputs and outputs from its commercial API are not used for model training by default.
- Briefing requests verify workspace membership and are rate limited per user.

13

Service Providers

PROVIDER	PURPOSE	INFORMATION INVOLVED
Supabase	Database, authentication, file storage	Workspace content, account and membership information, audit and operational records
DigitalOcean	Application hosting	Workspace data as it is processed by the application; operational logs
Google Workspace	Support and business correspondence	Support email, related correspondence, and limited internal operational records
Resend	Transactional and support email delivery	Recipient addresses, message content, delivery metadata
Anthropic	Optional AI contact briefings	Selected workspace context when a user requests a briefing
Stripe	Payments and subscriptions	Billing contacts, subscription and transaction information
Mapbox	Map display and address geocoding	Contact address text when a location must be geocoded

Mapbox. When a contact address needs a map location, StatecraftCRM sends the address text to Mapbox and stores the resulting coordinates for display within the product.

14

Support

Customers can submit support requests from within StatecraftCRM, and each request is recorded. Email support is available at **support@statecraftcrm.com**.

STATECRAFT'S CURRENT SUPPORT COMMITMENT:

Initial response within one business day. Critical service issues are prioritized immediately.

15

Security Contact

Security questions, suspected vulnerabilities, and suspected account compromise:

support@statecraftcrm.com

Statecraft can complete customer security questionnaires and provide additional architecture or security detail during procurement.