Export Sequence: Security Overview

Document version: 1.4
Last updated: June 5, 2026

1. Purpose of this document

This Security Overview describes how Export Sequence protects customer data and operates securely. It is intended for security reviewers, procurement teams, and IT administrators evaluating the service.

This document is **not** a third-party audit report, SOC 2 attestation, penetration test result, or CSA STAR registry submission. See Section 10 for a list of formal certifications and assessments we do **not** currently hold.

For privacy and legal terms, see our Privacy Policy and Terms of Use.

2. Service summary

Export Sequence is a **read-only** web application that enables Outreach customers to export sequence content (steps, email templates, task notes, metadata) as PDF or DOCX documents.

Attribute	Detail
Service model	SaaS (multi-tenant web application)
User authentication	Outreach OAuth 2.0 (authorization code flow)
Outreach API access	Read-only scopes only
Sequence content storage	**Not persisted** — processed in memory during export, then discarded
Data modification	**None** — the service cannot create, update, or delete Outreach records
Primary use cases	Compliance documentation, stakeholder sharing, archival snapshots

Export Sequence is an independent third-party tool. It is not affiliated with or endorsed by Outreach Corporation. The application requests only the read-only Outreach OAuth scopes required for this integration.

3. Architecture and data flow

3.1 High-level architecture

Diagram omitted in PDF export.

3.2 Authentication flow

1. User clicks **Connect with Outreach** on Export Sequence.
2. User is redirected to Outreach's OAuth authorization server and grants read-only permissions.
3. Export Sequence receives an authorization code and exchanges it for access and refresh tokens.
4. Tokens are **encrypted at rest** (AES-256-GCM) before storage in PostgreSQL.
5. A server-side session is created; the browser receives an **httpOnly, secure** session cookie (`session_id`). The session is valid for **up to 30 days**.
6. **Access tokens** are short-lived (lifetime set by Outreach). They are refreshed automatically when expired, using the stored refresh token — but only while the Export Sequence session is still valid.

7. After **30 days**, on **logout/disconnect**, or when the session is revoked or expired, the user must sign in with Outreach again. When the session ends, stored OAuth tokens are **cleared from the database** (on explicit disconnect, natural expiry, or security-related invalidation). The user profile and export history are retained.

OAuth CSRF protection is implemented via a random `state` parameter validated on callback. Session validity is bound to the user's Outreach organization (`org_guid`); mismatches revoke the session.

3.3 Export flow

1. Authenticated user submits a sequence URL or ID and selects PDF or DOCX format.
2. Export Sequence validates the session and retrieves the decrypted Outreach access token.
3. The application calls Outreach API endpoints (sequences, steps, templates) using the user's token.
4. Sequence data is assembled **in application memory** and passed to the document generator (Puppeteer for PDF, docx library for Word).
5. The generated file is returned to the user's browser as a download.
6. **Sequence body content is not written to disk or database.** Only export metadata (sequence ID, name, format, timestamp) is recorded in export history.

3.4 Outreach API scopes requested

Scope	Purpose
`sequences.read`	Sequence metadata (name, status, dates) and sequence-level aggregate performance statistics (deliveries, opens, clicks, replies)
`sequenceStates.read`	Per-step performance statistics — scope requested for planned functionality; **not yet used** in current exports
`sequenceSteps.read`	Step order, type, timing, task notes
`sequenceTemplates.read`	Links between steps and templates
`templates.read`	Email subject and body content for export

No write, delete, or administrative scopes are requested.

---

4. Data inventory

4.1 Data processed but not stored

Data type	Handling
Sequence step content	Fetched from Outreach API, held in memory during export, discarded after response
Email template subject/body	Same as above
Task notes	Same as above
Generated PDF/DOCX files	Streamed to user; not stored on our servers after delivery

4.2 Data stored

Data type	Storage	Encryption	Retention
Outreach OAuth access token	PostgreSQL	AES-256-GCM at application layer	Stored only while connected; short-lived (Outreach-defined); auto-refreshed during active session; **cleared when session ends** (disconnect, expiry, or invalidation)
Outreach OAuth refresh token	PostgreSQL	AES-256-GCM at application layer	Stored only while connected; usable only during an active session (max

Data type	Storage	Encryption	Retention
			30 days); **cleared when session ends**; replaced on re-login
User identifier (Outreach user ID, org ID, email, org shortname)	PostgreSQL	Database-level encryption at rest (hosting provider)	Active account; **policy target** of ~12 months after inactivity (see Section 9)
Session records (session ID, org binding, expiry)	PostgreSQL	Provider encryption at rest; opaque session ID sent to browser via **httpOnly cookie only** (not accessible to client-side JavaScript; OAuth tokens are not stored in cookies)	**30 days maximum**; revoked on logout/disconnect; re-login required after expiry
Export history (sequence ID, name, format, timestamp)	PostgreSQL	Database-level encryption at rest	Retained for user reference; deletable on request
Bulk export job metadata	PostgreSQL	Database-level encryption at rest	Job status and sequence ID list only

4.3 Data we do not collect

- Outreach account passwords (authentication is delegated entirely to Outreach OAuth)
- Payment or billing information (service is free)
- Sequence content in persistent storage

---

5. Security controls

5.1 Encryption

Layer	Control
Data in transit	TLS/HTTPS for all browser and API communication
OAuth tokens at rest	AES-256-GCM with random IV and authentication tag; key from environment variable (`ENCRYPTION_KEY` — 32-byte base64-encoded value or strong passphrase, derived to 32 bytes)
Database	PostgreSQL hosted on Render; TLS required via `sslmode=require` in the deployment `DATABASE_URL` connection string; provider-managed encryption at rest

5.2 Authentication and session management

- OAuth 2.0 authorization code flow via Outreach (industry-standard delegated authentication)
- **Session model:** server-side session records (user ID, Outreach org binding, expiry, revocation status) stored in PostgreSQL; the browser receives only an opaque `session_id` — OAuth tokens remain in the database (encrypted) and are never written to cookies
- **Session lifetime:** 30-day maximum (`session_id` cookie and server-side session record); user must re-authenticate with Outreach after expiry
- Session cookies: `httpOnly` , `secure` (production), `sameSite=lax` — session identifier is not exposed to client-side JavaScript
- **Access tokens:** short-lived; automatically refreshed via stored refresh token while the session is valid
- **Session end:** logout/disconnect, natural expiry (30 days), or security invalidation revokes the session and **clears stored OAuth tokens**; user profile and export history are retained
- New login revokes prior sessions for the same user and stores fresh tokens
- Token refresh with org-scoping validation — session revoked if token org does not match session org
- Users can revoke Export Sequence access at any time via Outreach authorized applications

5.3 Access control

- All export API endpoints require a valid authenticated session
- Application accesses Outreach data **only** with the authenticated user's token — no shared service account with broad org access
- Users can only export sequences they have read access to in Outreach (enforced by Outreach API permissions)
- Production secrets (OAuth client secret, encryption key, database credentials) stored as environment variables, not in source code

5.4 Application security

- OAuth state parameter validation (CSRF protection on auth callback)
- Input validation on export requests (sequence ID/URL format, supported formats)
- Read-only API integration — no endpoints that modify customer Outreach data
- Dependency updates applied as part of regular development and deployment

5.5 Organizational controls

- Operator: Sequently s.r.o. (Prague, Czech Republic)
- Access to production infrastructure limited to authorized personnel
- Privacy Policy aligned with GDPR and CCPA requirements
- Data subject requests (access, correction, deletion) handled **manually** via support@exportsequence.com; we aim to respond within 30 days

5.6 Operational policies (not automated controls)

The following are **documented operational policies**. They are not fully automated in the application today:

- **Inactive account cleanup (~12 months):** performed manually during periodic reviews, not by a scheduled deletion job
- **Account deletion requests:** fulfilled manually by authorized personnel; no self-service deletion endpoint
- **Incident response (Section 8):** documented procedure carried out by the operator team; no formal 24/7 security operations center

---

6. Subprocessors

Export Sequence uses the following third-party services to operate. Each processes data only as necessary to provide the service.

Subprocessor	Role	Data processed	Location
Render.com	Application hosting, managed PostgreSQL	Application traffic, user/session/export metadata (OAuth tokens only while connected)	United States (primary)
Outreach Corporation	OAuth identity provider and data source API	User identity, sequence data (transient during export)	Per Outreach infrastructure
Google (Google Analytics 4)	Optional website analytics	Page views, anonymized usage events (if `NEXT_PUBLIC_GA_MEASUREMENT_ID` is configured)	Per Google infrastructure

We do not sell customer data. We do not use third-party advertising trackers.

Customers may request an updated subprocessor list by contacting support@exportsequence.com.

---

7. Shared responsibility model

Responsibility	Export Sequence	Customer (Outreach org)
Outreach account credentials	—	Customer
OAuth authorization and scope approval	—	Customer
Revoking application access	Provides disconnect (revokes session, clears stored tokens); customer can revoke in Outreach	Customer
Sequence content accuracy and compliance	—	Customer
Securing exported documents after download	—	Customer
Application security, token encryption, hosting	Export Sequence	—
Outreach platform security	—	Outreach / Customer

---

8. Incident response and breach notification

This section describes our **documented operational incident response procedure**. Export Sequence does not operate a formal 24/7 security operations center or dedicated security monitoring platform. Our incident response process includes:

1. **Detection** - Monitoring application errors and infrastructure alerts from hosting provider
2. **Assessment** - Authorized personnel evaluate scope and impact
3. **Containment** - Revoke compromised sessions, rotate secrets, patch vulnerabilities as applicable
4. **Notification** - Notify affected customers and relevant authorities as required by applicable law (including GDPR breach notification timelines where applicable)
5. **Review** - Post-incident review and remediation

Report security concerns to: **support@exportsequence.com**

---

9. Data retention and deletion

Retention and deletion practices below include **operational policy targets** fulfilled manually (see Section 5.6), unless otherwise noted as enforced in application code.

Data	Retention policy
Active user accounts	Retained while account is active
Inactive accounts	**Policy target:** data may be deleted after ~12 months of inactivity during manual periodic reviews (not automated)
OAuth tokens	Stored encrypted **only while connected**; used **only during an active session** (max 30 days). **Cleared when the session ends** — disconnect, expiry, or invalidation (user profile and export history retained). Fresh tokens stored on re-login. Outreach may revoke tokens independently. User record and export history removed on account deletion request.
Export history	Retained for user reference; included in deletion requests
Sequence content	Never retained

Users may request full data deletion by emailing support@exportsequence.com. Deletion is performed **manually** by authorized personnel; we aim to complete it within 30 days, subject to legal retention requirements.

---

10. Formal assessments and certifications

The following are **not currently available**:

Requested artifact	Status
SOC 2 Type I or Type II report	Not available
ISO 27001 certification	Not available
Third-party security audit	Not available
Annual penetration test report	Not available
CSA STAR registry listing	Not submitted

We provide this Security Overview and a CAIQ Lite–style self-assessment questionnaire as transparency documents. We are happy to respond to customer-specific vendor security questionnaires.

---

11. Related documents

Document	URL / location
Privacy Policy	https://exportsequence.com/privacy
Terms of Use	https://exportsequence.com/terms
FAQ (security section)	https://exportsequence.com/faq
CAIQ Lite self-assessment	Available on request

---

12. Document maintenance

This document is reviewed and updated at least annually, or when material changes are made to the service architecture, data handling, or subprocessors.

Questions: support@exportsequence.com