
Privacy Policy – SSCI-Ops

Effective Date: 04/01/2026

Company: Standing Stone Consulting, Inc.

Standing Stone Consulting, Inc. (“SSCI,” “we,” “our,” or “us”) operates the SSCI-Ops mobile application (the “App”). The App is intended solely for use by authorized employees, contractors, and approved clients of SSCI.

This Privacy Policy explains how SSCI collects, uses, stores, discloses, monitors, logs, and safeguards information obtained through the App and related systems. By creating a profile, accessing, or using the App, the user acknowledges and agrees to the terms of this Privacy Policy.

1. Scope of Use

The SSCI-Ops App is a restricted-access internal platform used for operational coordination, workforce management, communication, scheduling, assignment tracking, reporting, compliance support, and administrative oversight.

Access to the App is limited to individuals expressly authorized by SSCI. Unauthorized access or use is prohibited.

Use of the App constitutes acknowledgment and acceptance of SSCI’s policies and practices concerning system monitoring, audit logging, location tracking, administrative oversight, data retention, and information security.

2. Company-Owned System; No Expectation of Privacy

The App and all related systems, data, communications, and records are company-owned or company-controlled systems.

By using the App, each user acknowledges and agrees that:

- the App is provided for authorized business and operational purposes;
- there is **no expectation of personal privacy** when using the App or any SSCI-related systems;
- all communications, data, messages, uploaded materials, location-related records, activity logs, and other information created, transmitted, received, stored, or maintained within the App may be accessed, monitored, reviewed, copied, retained, disclosed, or used by SSCI for legitimate business purposes;

- SSCI reserves the right, to the fullest extent permitted by law, to monitor and review App usage, communications, and records at any time, with or without further notice.

Users should not use the App for personal, private, or non-business communications or content.

3. Information We Collect

SSCI may collect, receive, generate, store, and process several categories of information through the App.

A. Account and Identity Information

We may collect account and identity information, including:

- full name;
- email address;
- mobile phone number;
- employee, contractor, or client identifier;
- job title, role, division, department, or assignment;
- account status and permissions;
- username or other profile identifiers.

B. Profile and Employment-Related Information

Where applicable, we may collect profile and workforce-related information, including:

- division or team assignment;
- supervisor or reporting relationship information;
- work eligibility or assignment status;
- scheduling and availability information;
- internal classification information necessary for workforce coordination.

C. Communications and Messaging Data

We may collect and retain communications conducted through the App, including:

- direct messages;
- group messages;

- announcements;
- comments or replies;
- attached documents, images, files, or media;
- metadata associated with communications, such as sender, recipient, time sent, time viewed, and related activity.

All such communications are considered company communications when conducted through the App.

D. Operational and Usage Data

We may collect operational and usage data, including:

- schedules;
- assignments;
- work-related task information;
- check-in and check-out records;
- reports, forms, and responses submitted through the App;
- feature usage;
- timestamps of actions taken;
- interactions with system functions.

E. Uploaded Content

We may collect and store content uploaded or submitted by users, including:

- photographs;
- profile images;
- reports;
- forms;
- PDFs;
- spreadsheets;
- documents;
- attachments;

- other files or content submitted through the App.

F. Device and Technical Information

We may collect technical and device-related information, including:

- IP address;
- device type;
- device identifiers;
- operating system;
- browser type;
- app version;
- login timestamps;
- session data;
- crash or diagnostic information;
- network and access information;
- approximate device configuration information needed for security or functionality.

G. Authentication and Access Data

We may collect authentication and access information, including:

- account creation date;
- login and logout history;
- password reset activity;
- authentication provider data;
- profile creation records;
- role assignment records;
- account enablement, disablement, or restriction records.

H. Location Information

Where enabled, permitted, or required for App functionality, SSCI may collect:

- real-time location data;

- periodic location data;
- approximate location data;
- location associated with check-in, clock-in, clock-out, or attendance verification;
- site presence data associated with operational assignments.

Location information may be collected through GPS, network-based methods, device location services, or similar technical means.

I. Acknowledgment and Consent Records

SSCI may collect and retain records relating to acceptance of this Privacy Policy and related notices, including:

- user identity;
- date and time of acknowledgment;
- policy version accepted;
- device or browser information;
- IP address or related technical information;
- record of checkbox, selection, or other affirmative acceptance action.

4. Location Tracking for Operational Purposes

The App may collect location information for legitimate operational purposes.

Location tracking may be used for purposes that include:

- verifying presence at an assigned work site or approved location;
- workforce coordination;
- operational deployment and supervision;
- attendance verification;
- timekeeping support;
- confirming service delivery requirements;
- supporting safety, accountability, and incident review.

Location tracking is intended for business and operational purposes only. By using the App and enabling or using features that rely on location, the user consents to the collection and use of location data as described in this Privacy Policy.

5. Communications Subject to Monitoring

All communications conducted through the App are company communications systems and are subject to monitoring, review, logging, retention, and retrieval.

SSCI may monitor, access, review, disclose, or retain communications and related content for legitimate business purposes, including:

- operational management;
- quality assurance;
- supervision;
- compliance review;
- policy enforcement;
- workplace investigations;
- incident response;
- legal and contractual compliance;
- protection of SSCI personnel, clients, contractors, property, and business interests.

This includes messages, chats, attachments, uploaded content, and related metadata. Users should have no expectation that communications within the App are private or personal.

6. Audit Logging and System Monitoring

SSCI maintains audit logs and system monitoring records relating to App use and system activity.

Audit logs may include, without limitation:

- login and logout events;
- account creation events;
- profile changes;
- data changes;

- messages sent;
- file uploads;
- feature usage;
- location-related events;
- administrative access events;
- actions performed by users;
- time and date of actions;
- device or technical metadata associated with those events.

These records may be used for:

- security monitoring;
- fraud prevention;
- system integrity;
- policy enforcement;
- internal audits;
- compliance reviews;
- investigations;
- incident response;
- operational accountability;
- legal or administrative proceedings.

7. Internal Data Access and Administrative Oversight

Authorized SSCI personnel, including administrators, supervisors, managers, executive leadership, HR, compliance personnel, or other designated representatives, may access user data within the App where necessary for legitimate business purposes.

Such purposes may include:

- operational management;
- workforce coordination;
- supervision;

- schedule and assignment administration;
- compliance and policy enforcement;
- training and quality review;
- incident response;
- investigative review;
- legal or administrative review;
- protection of SSCI's rights, people, clients, systems, or operations.

Access is intended to be based on business need, role, and responsibility. SSCI reserves the right to determine appropriate access and oversight consistent with operational, administrative, and legal requirements.

8. How We Use Information

SSCI may use collected information for lawful business purposes, including to:

- create and manage user accounts and profiles;
- operate, maintain, improve, and secure the App;
- manage internal communications and announcements;
- coordinate staffing, assignments, and schedules;
- verify attendance, check-ins, and site presence;
- facilitate operational reporting and workforce management;
- administer roles, permissions, and access controls;
- monitor system use and compliance with company policies;
- conduct audits, investigations, and reviews;
- respond to safety, security, misconduct, or compliance concerns;
- troubleshoot technical issues and maintain system integrity;
- comply with contractual, regulatory, administrative, or legal obligations;
- document acknowledgments, policy acceptance, and user consent.

9. Data Sharing and Disclosure

SSCI does **not sell personal information**.

SSCI may share, disclose, or permit access to information in the following circumstances:

- with authorized SSCI personnel for legitimate business purposes;
- with service providers, vendors, or contractors that support hosting, authentication, communications, storage, security, analytics, maintenance, or App functionality;
- with clients or authorized representatives where necessary for service delivery, reporting, or contractual compliance, to the extent appropriate;
- when required by law, court order, subpoena, legal process, governmental request, or regulatory obligation;
- when SSCI believes disclosure is necessary to protect the safety, rights, property, systems, personnel, contractors, clients, or operations of SSCI or others;
- in connection with internal investigations, audits, disciplinary matters, or enforcement actions;
- in connection with a business transaction, restructuring, or organizational transition, where legally appropriate.

10. Third-Party Services and Data Infrastructure

The App may use third-party providers and infrastructure to support functionality and operations, which may include:

- cloud hosting providers;
- databases;
- authentication services;
- file and media storage providers;
- messaging or notification systems;
- analytics or monitoring services;
- technology providers supporting App performance, maintenance, or security.

These providers may store, transmit, process, or maintain data on SSCI's behalf. SSCI selects such providers based on business, security, operational, or technical considerations, but SSCI does not control every aspect of a third party's internal systems or independent policies.

Users acknowledge that information processed through the App may be handled through third-party systems supporting SSCI operations.

11. Data Storage and Security

SSCI implements administrative, technical, and organizational safeguards intended to protect information processed through the App.

Such measures may include:

- role-based access restrictions;
- password and authentication controls;
- account management controls;
- restricted administrative permissions;
- encryption in transit where applicable;
- monitoring and logging controls;
- system access controls;
- vendor and infrastructure safeguards where available.

Despite reasonable efforts, no method of transmission, storage, or electronic security is completely secure. SSCI cannot guarantee absolute security, uninterrupted service, or prevention of all unauthorized access, misuse, loss, or disclosure.

12. Data Retention

SSCI retains information for as long as necessary or appropriate for legitimate business purposes, including:

- operation of the App;
- workforce and account management;
- communications and recordkeeping;
- audits and compliance;
- incident review and investigations;
- enforcement of company policies;
- contractual obligations;

- legal, regulatory, administrative, or evidentiary requirements.

Data may be retained after the end of employment, contract status, client access, or account deactivation where SSCI determines retention is necessary or appropriate.

13. User Responsibilities

Users are responsible for:

- using the App only for authorized business and operational purposes;
- providing accurate information where required;
- maintaining the security and confidentiality of login credentials;
- promptly reporting suspected unauthorized access or misuse;
- complying with SSCI policies, rules, and standards applicable to App use;
- avoiding use of the App for personal, unlawful, inappropriate, or non-business purposes;
- submitting only appropriate, work-related, and authorized content through the App.

14. User Rights

To the extent required by applicable law, users may have the right to request:

- access to certain personal data maintained by SSCI;
- correction of inaccurate personal data;
- deletion of certain personal data, subject to business, legal, operational, investigative, compliance, and retention requirements.

Any such request may be limited, denied, or deferred where SSCI determines retention, access restriction, or continued processing is necessary for legitimate business purposes or legal obligations.

Requests may be submitted through SSCI using the contact information below.

15. Children's Privacy

The App is not intended for individuals under the age of 18. SSCI does not knowingly provide access to the App for children or knowingly collect personal information from individuals under 18 through the App for general use.

16. Changes to This Privacy Policy

SSCI may revise, amend, or update this Privacy Policy at any time.

When changes are made, SSCI may update the effective date and may require renewed acknowledgment before continued access or use. Continued use of the App after any update may constitute acceptance of the updated policy, except where SSCI requires a new express acknowledgment.

17. Contact Information

Standing Stone Consulting, Inc.

Email: webadmin@sscsecurity.com

Address: 826 Pennsylvania Ave, Huntingdon, PA 16652

18. User Acknowledgment, Consent, and Record of Acceptance

As a condition of creating a profile, obtaining access to the App, and continuing to use the App, users are required to provide an explicit acknowledgment of this Privacy Policy.

By creating a profile, selecting the acknowledgment option, checking an acknowledgment box, clicking to accept, or otherwise affirmatively accepting within the App, the user:

- confirms that the user has read, understood, and agreed to this Privacy Policy;
- acknowledges that the App is a company-owned and company-controlled system;
- acknowledges that there is **no expectation of privacy** in communications, data, files, system activity, or other use of the App;
- consents to the monitoring, review, logging, retention, and administrative access described in this Privacy Policy;
- acknowledges that communications through the App are subject to monitoring and retention;
- consents to the collection and use of location data for operational purposes;
- acknowledges that use of the App is subject to audit logging, system oversight, and policy enforcement.

SSCI maintains a record of each user's acknowledgment and acceptance. That record may include:

- user identity;
- date and time of acceptance;
- version of the Privacy Policy accepted;

- profile or account information;
- IP address;
- device or browser information;
- technical metadata associated with the acceptance event.

These records serve as evidence of consent and acceptance and may be used by SSCI for:

- policy enforcement;
- account administration;
- compliance documentation;
- internal investigations;
- disciplinary review;
- administrative proceedings;
- legal proceedings or defense of claims.

Users who do not provide the required acknowledgment will not be permitted to create a profile, access the App, or continue use where acknowledgment is required.

19. Policy Versioning and Re-Acknowledgment

SSCI may assign a version number, effective date, or similar identifier to this Privacy Policy. SSCI reserves the right to require users to provide a new acknowledgment whenever SSCI determines that an updated policy, revised practice, new feature, legal requirement, or operational change warrants renewed acceptance.

Failure or refusal to provide a required re-acknowledgment may result in denial, suspension, or restriction of access to the App.