SSOE, Inc. California Privacy Policy
CPRA PRIVACY POLICY FOR WORK-RELATED INDIVIDUALS

1. DOCUMENT PURPOSE AND SCOPE

SSOE, Inc., its operating groups, parent(s), subsidiaries, and affiliates (collectively, "the Company") are committed to protecting the privacy and security of the personal information of our job applicants, current and former employees and their emergency contacts and beneficiaries, independent contractors, board of directors, and corporate officers who are residents of California ("Work-Related Individuals"). This privacy policy describes how we collect, use, retain, secure, and disclose personal information about you (our "Information Practices"). The Company is responsible for deciding how it collects, uses, retains, secures, and discloses your personal information.

This privacy policy is intended to comply with the California Consumer Privacy Act ("CCPA"), California Privacy Rights Act ("CPRA"), applicable regulations, and other applicable data privacy laws. This Privacy Policy does not form part of any contract of employment or other contract to provide services. We may update this policy at any time.

It is important that you read and understand this privacy policy, together with any other privacy notices we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information. If you have any questions about this privacy policy or how we handle your personal information, please contact us at privacy@ssoe.com or **833-822-7726**.

.

If you wish to access this privacy policy in an alternate format or require an accommodation to access this privacy policy, please contact us at privacy@ssoe.com or **833-822-7726.**

2. DATA PROTECTION PRINCIPLES

We collect, use, retain, and share your personal information in accordance with certain data privacy and data protection principles. Specifically, the personal information we collect about you is: (i) used lawfully, fairly and in a transparent way; (ii) collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes; (iii) reasonably necessary and proportionate to achieve these purposes; (iv) accurate and kept up to date; (v) kept only as long as necessary for these purposes; and (vi) kept securely. If we intend to collect, use, retain, or share your personal information for any purpose that is incompatible with the purposes for which your personal information was collected, we will obtain your consent to do so.

For the purposes of this privacy policy, "personal information" means *information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. "Sensitive personal information" is a subcategory of personal information and means personal information that* : (a) an individual's social security, driver's license, state identification card, or passport number; (b) an individual's account log-in, financial account, (c) an individual's precise geolocation; (d) an individual's racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) the contents of an individual's mail,

email, and text messages unless the Company is the intended recipient of the communication; (f) an individual's genetic data; (g) an individual's biometric information used to uniquely identify the individual; (h) personal information collected and analyzed regarding an individual's health; and (i) personal information collected and analyzed regarding an individual's sexual orientation.

3. PERSONAL INFORMATION WE COLLECT, HOW WE COLLECT IT, USE IT, AND SHARE IT

We collect, receive, use, and share personal information for work-related individuals; job applicants and candidates, current and former employees, contractors, our employee's emergency contacts and beneficiaries, Board of Directors. **We do not:**

- Sell your personal information.
- Share or disclose your personal information to third parties other than the Company's service providers.
- Share or disclose your sensitive information to third parties for purposes other than those listed below or otherwise permitted by the CPRA.
- Share the personal information of consumers under 16 years of age.
- Permit third parties to collect your personal information on our behalf other than the Company's service providers.

(a) **Sources of Personal Information** – Subject to applicable law the Company collects information about you from the following sources:

- "You" in connection with your resume, the application and forms you submit to us when applying for a job, and references you provide.
- Vendor and service providers
- Publicly available sites
- Applicable law enforcement, governmental and administrative agencies
- Third Parties- Job references you provide, professional employer organizations or staffing agencies. your former employer.
- Acquired Company through Merger and Acquisitions.

(b) **The Personal and Sensitive Information – The following are examples of personal and sensitive information we may collect:**

Categories of Personal and Sensitive Information	Example of Personnel Data
Identification Data	Identifiers (e.g., a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers).
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e) Information listed under Cal.Civ. Code	Personal information, such as real name, signature, SSN, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, federal identification authorizing work in the United States, insurance policy number, education, employment, employment history, bank account number, other financial information, medical information, or health insurance information.
Protected classification characteristics under CA or Federal Law	Characteristics of protected classifications under California or federal law, such as age, marital status, gender, sex, race, color, disability, citizenship, immigration status, military/veteran status, disability, request for leave and medical conditions.
Commercial Information	Commercial information, such as transaction information and purchase history (e.g., in connection with expense reimbursements made to employees for business-related purchases, purchases of company store merchandise).
Biometric Information	Behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as sleep, health, or exercise data related to participation in wellness programs.
Internet or other electronic network activity information	Including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application or advertisement.
Geolocation	Such as device location from using the Company's devices.
Sensory Data	Audio, electronic, visual, and similar information.
Professional or employment-related information	Professional or employment-related information, such as work history, prior employers, data submitted in job applications, professional licenses, degrees, and background checks.
Education information	Educational history, academic degrees, and qualifications, certifications, and skills.
Inferences drawn from any of the information	Inferences drawn from any of the personal and sensitive personal information listed to create a profile or summary about, for example, an individual's preferences and characteristics.

(c) **How your personal and sensitive person information is used.** We may use personal and sensitive information for the following purposes:

- Recruiting and retaining employees and processing employment applications.
- Collecting and processing employment applications, including confirming eligibility for employment, background, and related checks.
- Employee pre-boarding, onboarding, and off-boarding.
- Maintaining personnel records and complying with records retention requirements
- Leaves of absence administration.
- Compensation administration and compliance, including payroll, bonuses, reimbursement etc.
- Booking employee travel.
- Employee benefit plans and program administration.
- Employee activation initiatives and communications.
- Facilitating diversity and inclusion programs.
- Administering training and education programs.
- HR and IT system management, administration, and security.
- Performance management.
- Workplace health and Safety compliance
- Security (including network and physical security)
- As required by law.
- Communication with employees and/or employee's emergency contacts and plan beneficiaries.
- Facilitating and administering the use of the company's property and resources, including the company's information systems, electronic devices, network and data, and preventing unauthorized access of such.
- Ensuring employee productivity and adherence to Company policies.
- Investigating complaints, grievances, and suspected violations of policy.
- Complying with applicable state and federal laws, including labor, employment, tax, benefits, workers compensation, disability, equal employment opportunity, workplace safety and related laws
- Exercising and defending legal claims.
- To investigate, prevent, or take action if we think someone might be using information for illegal activities, fraud, or in ways that may threaten someone's safety or violate our policies or legal obligations.
- As part of an acquisition, merger, asset sale, or other transaction where another party assumes control over all or part of our business.

(d) **Categories of Entities with whom we share the Personal Information** – SSOE may share "Personal Data in the following ways:

- Company personnel that have a business need to know based on their role with the Company.
- Vendor or Service providers that perform services on behalf of the Company**.**
- Clients of the Company.
- Other Third Parties

- Where required by law.
- Where SSOE determines it is lawful and appropriate.
- To protect SSOE legal rights or to protect its employees, resources, and workplaces.
- In an emergency where health or security are at stake.
- Public security and Law Enforcement.

4. PRIVACY RIGHTS

As a California resident, you have the following privacy rights regarding your personal information:

- The right to know and right to access the personal information we have collected about you, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer.

- The right to delete personal information that we have collected from you, subject to certain exceptions.

- The right to correct inaccurate personal information that we maintain about you.

- The right of portability, or right to have us transfer your personal information to other persons or entities upon your request.

- The right to limit the use of your sensitive information if we decide in the future to use such information for purposes other than the purposes listed above.

- The right not to be discriminated against or retaliated against for exercising your privacy rights.

You can exercise your privacy rights by submitting a request to us by emailing us at privacy@ssoe.com calling us at **833-822-7726** or asking our Human Resources Department for a written request form. To protect the security of your personal information, we will require you to provide us with identifying information such as personal email address, personal telephone number, employee identification number, and/or other information that we can match with the personal information we have collected about you to verify your identity.

You may use an authorized agent to request access to or deletion of your personal information. We will require your authorized agent to provide us with either (1) a power of attorney authorizing the authorized agent to act on your behalf or (2) your written authorization permitting the authorized agent to request access to your personal information on your behalf. Further, we will require you or your authorized agent to provide us with identifying information to verify your identity. We may also require you to either verify your own identity directly with us or directly confirm with us that you provided the authorized agent permission to submit the request.

Within **10 days** of receiving your request to know, we will confirm receipt of your request and provide information about how we will process your request. Generally, we will respond to your request within

45 days. If we need more time to respond, we will provide you with notice and an explanation of the reason we need more time to respond. We may deny your request if we cannot verify your identity or are legally permitted to deny your request. If we deny your request, we will explain the basis for the denial, provide or delete any personal information that is not subject to the denial, and refrain from using the personal information retained for any purpose other than permitted by the denial. We will maintain a record of your request and our response for 24 months.

5. DATA SECURITY

While no data security system can fully protect personal information from unauthorized data breaches, the Company has implemented reasonable safeguards and controls, consistent with its legal obligations under California and other local, state, and federal laws. The Company is committed to: (i) seeking to safeguard all personal information that you provide to us; (ii) seeking to ensure that it remains confidential and secure; and (iii) taking all reasonable steps to ensure that personal privacy is respected. All our data is stored in written or electronic form on our servers and computers and in various physical locations. We maintain physical, electronic, and procedural safeguards to protect your personal information from misuse, unauthorized access or disclosure and loss or corruption by computer viruses and other sources of harm. We restrict access to personal information to those staff members of the Company and our services providers who need to know that information for the purposes identified in our privacy policy and privacy notices.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

6. DATA RETENTION

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements. Generally, we retain personal information for the duration of our relationship with you plus any legally required record or data retention period and/or any period of time necessary to exercise our legal rights. Thereafter, we will securely destroy your personal information in accordance with the Company's record retention policies.

In some circumstances we may anonymize your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

7. PERSONAL INFORMATION OF MINORS

The Company does not sell or share personal information for individuals under the age of 16.

8. CHANGES TO THIS PRIVACY POLICY

As we strive to improve our practices, we may revise the Company's privacy policy from time to time. The description of our data practices in this Notice covers the 12 months prior to the date this Notice and will be updated at least annually. This privacy policy is not a contract, and we reserve the right to change this policy at any time and to notify you of those changes by posting an updated version of this policy. It is your responsibility to check this policy from time to time for any changes.

This privacy policy was last updated on April 1, 2024

9. QUESTIONS AND FURTHER INFORMATION

If you have any questions or would like further information regarding this privacy policy or our privacy practices, you may contact us using the following details:

- ***Via Email Address***: privacy@ssoe.com
- ***Via Postal Address*****:**
  SSOE, Inc.
  Attn: Privacy, Human Resources Department
  1001 Madison Ave, Toledo, Ohio 43604
- ***Via Phone*****: 833-822-7726**