CCPA Privacy Policy for

Employees, Former Employees, and Applicants

This Privacy Policy is made available pursuant to the California Consumer Privacy Act (CCPA).

Please review this notice carefully, as it applies to the personal information we collect about you solely in your capacity as an applicant, job candidate, employee, or former employee of TraPac, LLC (the "Company").

Under the CCPA, personal information includes information that identifies and describes who you are; as well as information that relates to, is capable of being associated with, or could reasonably be linked to you, one of your devices and/or a member of your household. In this Policy, we refer to the information subject to the CCPA as "Employee Personal Information."

You have the right to receive information on the Company's privacy practices, including why we collect Employee Personal Information, from whom it is collected and for what purpose.

The Company collects and uses Employee Personal Information for human resources, employment, benefits administration, health and safety, and business-related purposes and to be in compliance with applicable statutes and regulations. Below are the categories of Employee Personal Information we collect and the purposes for which we intend to use this information.

<u>The Company Collects the Below Information:</u>

- **Identifying information**, such as your full name, gender, date of birth, and signature.
- **Demographic data**, such as race, ethnic origin, marital status, disability, and veteran or military status.
- **Contact information**, such as your home address, telephone numbers, email addresses, and emergency contact information.
- **Dependent's or other individual's information**, such as their full name, address, date of birth, and Social Security numbers (SSN).
- **National identifiers**, such as SSN, passport and visa information, and immigration status and documentation.
- **Educational and professional background**, such as your work history, academic and professional qualifications, educational records, references, and interview notes.
- **Employment details**, such as your job title, position, hire dates, compensation, performance and disciplinary records, and vacation and sick leave records.
- **Financial information**, such as banking details, tax information, payroll information, and withholdings.
- **Health and Safety information**, such as health conditions (if relevant to your employment), job restrictions, workplace illness and injury information, and health insurance policy information.

- **Information Systems (IS) information**, such as your login credentials and information, search history, browsing history, and IP addresses on the Company's information systems and networks.
- **Geolocation data**, such as time and physical location related to use of an internet website, application, device, or physical access to a Company office location.
- **Sensory or surveillance information**, such as COVID-19 related temperature checks and call monitoring and video surveillance.
- **Profile** or summary about an applicant or employee's preferences, characteristics, attitudes, intelligence, abilities, and aptitudes.

The Company Collects Employee Personal Information to Use or Disclose as Appropriate to:

- Comply with all applicable laws and regulations.
- Recruit and evaluate job applicants and candidates for employment.
- Conduct background checks.
- Manage your employment relationship with us, including for:
  - onboarding processes;
  - timekeeping, payroll, and expense report administration;
  - employee benefits administration;
  - employee training and development requirements;
  - the creation, maintenance, and security of your online employee accounts;
  - reaching your emergency contacts when needed, such as when you are not reachable or are injured or ill;
  - workers' compensation claims management;
  - employee job performance, including goals and performance reviews, promotions, discipline, and termination; and
  - other human resources purposes.
- Manage and monitor employee access to company facilities, equipment, and systems.
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential breaches of Company policies and procedures.
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company.
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- Administer and maintain the Company's operations, including for safety purposes.

- For client marketing purposes.
- Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and or agents.

The Company does not use sensitive personal information, such as Social Security number; driver's license number; racial or ethnic origin; personal mail, email, and text messages; precise geolocation; and personal information collected and analyzed concerning an individual's health to infer personal characteristics, but instead uses such information to perform the functions listed above on behalf of the Company.

The Company Collects Employee Personal Information by:

- The applicant or job candidate themselves. Either in person, by telephone, or email, or through systems that facilitate collection of information from you (e.g., the online administrative systems for employment applications, benefits, 401(k), and more).
- From publicly accessible sources (e.g., court records, social media sites, social networking sites).
- Directly from a third party (e.g., job boards, recruiters, screening providers, credit reporting agencies, or customer due diligence providers).
- Indirect or passive sources (e.g., cookies on our Sites; our IT systems; building security systems).

The Company May Share Employee Personal Information with:

- Service providers the Company uses to help deliver benefits and services related to your prospective or actual employment, such as identity verification providers, payment service providers, time and attendance programs, benefits programs, and more.
- Third parties approved by you (e.g., your legal counsel, assessment and background check providers, and others).
- Law enforcement, government entities and pursuant to legal process where required by law.

The Company Protects Employee Personal Information:

The Company stores personal information using industry standard, reasonable and technically feasible physical, technical, and administrative safeguards against foreseeable risks, such as unauthorized access.

Please be aware that the Websites and data storage are run on software, hardware and networks, any component of which may, from time to time, require maintenance or experience problems or breaches of security beyond the Company's control. The Company is not responsible for the acts and omissions of any third parties.

The Company cannot guarantee the security of the information on and sent from the Websites. No transmission of data over the internet is guaranteed to be completely secure. It may be possible for third parties not under the control of The Company to intercept or access transmissions or private communications unlawfully. While we strive to protect your personal information, neither The Company nor any of our Service Providers can ensure or warrant the

security of any information you transmit to us over the internet. Any such transmission is done at your own risk.

Retention and Sharing of Employee Personal Information:

The Company will not sell the personal information we collect and will not share information with third parties for the purpose of cross-context behavioral marketing.

The Company may collect the Employee Personal Information categories listed above, as well as, in the table below. The table also lists, for each category, our expected retention period, and whether we sell the information or share it with third parties for cross-context behavioral advertising.

Personal Information Category	**Retention Period**	**Information Sold or Shared?**
Identifying Information	10	No
Demographic Data	10	No
Contact Information	10	No
Dependent's or Other Individual's Information	10	No
National Identifiers	10	No
Educational and Professional Background	10	No
Employment Details	10	No
Financial Information	10	No
Health and Safety Information	10	No
Information Systems Information	10	No
Geolocation Data	10	No
Sensory or Surveillance Information	10	No
Profile or Summary	10	No

Your Rights and Choices

The CCPA/CPRA provides employees or applicants (California residents) with specific rights regarding their personal information. This section describes your CCPA/CPRA rights and explains how to exercise those rights.

- You have the right to request that we disclose certain information to you about our collection and use of your personal data over the past twelve months, such as (i) the categories of personal data we collected about you; (ii) the categories of sources from which we collected such data; (iii) the specific pieces of personal data we collected about you; (iv) the purpose for collecting personal data about you; and (v) the categories of personal data about you that we shared or disclosed and the categories of third parties with whom we shared or to whom we disclosed such data in the preceding twelve months, subject to legal restrictions.
- You have the right to request that we delete your personal data, subject to legal restrictions.
- You have the right to request us to correct any inaccurate personal information about you. If any personal information requires correction, we will use commercially reasonable efforts to fulfill your correction request.

Only you, or someone legally authorized to act on your behalf, may make a request to know, delete or correct related to your personal information.

You may only submit a request to know twice within a 12-month period.

Your request to know, delete or correct must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We will pass your deletion requests on to service providers, contractors, and, unless impossible or involves disproportionate effort, to all third parties to whom shared the information.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. We will only use personal information provided in the request to verify the requestor's identity or authority to make it. To exercise your privacy rights, send us your verifiable employee or applicant request using the “Contact” section below.

Response Timing and Format

We will respond to your request consistent with applicable law, which does not apply to certain data.

Any disclosures we provide will only cover the 12-month period preceding our receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable employee or applicant request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Data Storage and Security

We may store your personal data in the U.S. Except as otherwise permitted or required by law, we only retain your personal data for as long as necessary to fulfill the purposes for which they were collected. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use of processing by other means, and any applicable legal requirements.

We maintain reasonable administrative, technical, and physical safeguards to protect your data from accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use. Our service providers are also required to adhere to reasonable security practices to further ensure your data. That being said, digital transmission and storage of data is not completely secure and we cannot guarantee the safety of your data.

Changes to Our Privacy Policy

We reserve the right to amend this Privacy Policy at our discretion and at any time. When we make changes to this Privacy Policy, we will post the updated policy on the respective website and update the Privacy Policy's effective date

Exercising Access, Data Portability, and Deletion Rights

If you have any questions about this Policy or need to access this Policy in an alternative format due to having a disability, or to exercise your access, data portability, and deletion rights described above, please submit a verifiable consumer request by calling us at (310)830-2000 or emailing us at hr@trapac.com. If you have any questions about this Policy or need to access this Policy in an alternative format due to having a disability, please contact Human Resources at hr@trapac.com.