

California Employee and Applicant Privacy Notice

Mountain Cascade, Inc. and its affiliates and subsidiaries (collectively, “Mountain Cascade,” “Company,” “we,” “us,” or “our”) collect, use, disclose and retain personal information of employees and job applicants (“you” or “your”). We provide you with this California Employee and Applicant Privacy Notice (“Notice”) to inform you about the categories of personal information we may collect about you at or before the time personal information is collected. This Notice is provided to job applicants at the time of application, to candidates at or before the time an offer of employment is extended.

This Notice is intended to comply with the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CCPA/CPRA”) and applies only to employment related personal information. Any terms defined in the CCPA/CPRA have the same meaning when used in this Notice.

What Personal Information We May Collect

We and our service providers may collect, use, disclose, and retain the following categories of your personal information in connection with your employment relationship or job application:

- **Identifiers**, such as your full name, alias, postal address, email address, Social Security Number, driver’s license number, other government issued identification number, and signature.
- **California Customer Records information** (Cal. Civ. Code § 1798.80(e)), including telephone number, bank account and other financial account information, tax withholding information, and emergency contact information.
- **Protected classification characteristics** under California or federal law, such as age, race, color, national origin, ancestry, sex, gender, gender identity, marital status, medical condition, mental or physical disability, veteran or military status, and religion.
- **Commercial information**, such as expense reports, travel records, company credit card transactions, per diem and allowance records, and reimbursement records.
- **Internet or other electronic network activity**, such as log files, access logs, browsing and search history on Company-owned devices or systems, email metadata, and information generated through your use of Company networks, software, or applications.
- **Geolocation data**, such as precise or approximate location data derived from Company-owned devices, vehicles, equipment, or access control systems, including GPS data from Company vehicles or field equipment, location data generated by Company-issued mobile devices or MiFi devices, and jobsite check-in and check-out records.
- **Professional or employment-related information**, such as job title and classification, employment history, compensation and payroll records, timekeeping records, performance evaluations, disciplinary records, safety training and certification records, professional licenses, skills and qualifications, and work authorization status.
- **Education and credential information**, such as highest level of education completed, trade certifications, professional licenses and endorsements, apprenticeship records, operator certifications, and other vocational or professional training records provided in connection with your employment.
- **Sensitive Personal Information**, as defined under CPRA, including Social Security number, driver's license number, state identification number, and passport number; precise geolocation data derived from Company-provided devices or equipment, such as MiFi devices or GPS-enabled field equipment; racial or ethnic origin, religious beliefs, and union membership status collected for EEO reporting, benefits administration, or other legally required purposes; contents of employee communications on Company systems where accessed for security or compliance purposes; biometric identifiers, such as fingerprints, where used for timekeeping or facility access; and health or medical information collected in connection with workers' compensation, leave administration, or benefits enrollment.

In administering benefits programs, we may also collect personal information about your dependents, beneficiaries, and emergency contacts, such as names, addresses, dates of birth, Social Security numbers, phone numbers, and email

addresses. This information is collected solely to administer your benefits, process claims, or contact designated individuals in an emergency.

How We Collect Your Personal Information

We collect your personal information from the following sources:

- Directly from you, through job applications, onboarding documents, timesheets, expense reports, benefits enrollment forms, and information you provide during the course of your employment.
- Background check and consumer reporting agencies, in connection with pre-employment and ongoing screening.
- Payroll, benefits, and human resources service providers and administrators.
- Government agencies and licensing authorities, such as the California Contractors State License Board, DMV, and other regulatory bodies.
- Clients, project owners, and project partners, such as information provided for jobsite access, badging, or compliance with project-specific requirements.
- Automated Company systems, including access control systems, timekeeping systems, fleet tracking systems, IT infrastructure, and security tools.
- Healthcare providers, workers' compensation administrators, and insurance carriers, in connection with benefits, claims, or leave administration.

How the Company Uses Your Personal Information

We collect, use, disclose, and retain your personal information for the following business purposes:

- Recruiting, evaluating, and onboarding job applicants and employees, including conducting background checks as required by law, regulation, or contract.
- Managing your employment relationship, including timekeeping, payroll, and expense administration; benefits enrollment (including but not limited to 401K and/or Company profit sharing) and administration for you and your dependents; employee training, development, and continuing education; performance management, promotions, discipline, and termination; workers' compensation claims management; and other human resources functions.
- Complying with applicable federal, state, and local laws and regulations, and with professional, industry, and regulatory standards applicable to Company's construction, engineering, and infrastructure services.
- Providing, managing, and monitoring access to Company facilities, jobsites, equipment, vehicles, and systems, and monitoring, administering, and retaining Company internal communications, including emails, instant messages, and other correspondence transmitted through Company systems, platforms, or devices.
- Monitoring, administering, and retaining communications and activity conducted through Company-owned or Company-provided systems, devices, platforms, and networks, including but not limited to email, messaging applications, internet usage, and other electronic communications, consistent with applicable law and Company policy.
- Administering and maintaining workplace health and safety programs, including Cal/OSHA compliance, incident reporting, and jobsite safety requirements.
- Conducting internal audits, workplace investigations, and enforcing compliance with Company policies and procedures.
- Maintaining commercial insurance policies and processing claims, including workers' compensation, general liability, professional liability, and other coverages.
- Performing workforce planning, data analytics, and benchmarking to support Company operations.
- Engaging in corporate transactions, such as mergers, acquisitions, financing, or restructuring, where review of employee records is required.
- Supporting the services Company provides to its clients and project owners, including compliance with project-specific requirements.

- Conducting limited business development activities using aggregated or de-identified workforce data, and not for the sale, sharing, or profiling of your personal information.
- Establishing, exercising, or defending the legal rights and claims of Company and its employees, affiliates, clients, subcontractors, and agents.

We use Sensitive personal information only for purposes directly related to your employment, such as payroll processing, benefits administration, workplace security, and legal compliance. We do not use or disclose Sensitive Personal Information in ways that would require us to offer you a right to limit its use under CPRA. Accordingly, while this right is described below for completeness, it has limited practical applicability at Company; the Company's use of Sensitive Personal Information is restricted to purposes expressly permitted by CPRA that do not trigger that right.

How We Disclose Your Personal Information

We may disclose your personal information to the following categories of third parties for the business purposes described in this Notice:

- Payroll processors, benefits administrators (including but not limited to 401K and/or Company profit sharing), and employee assistance program (EAP) providers.
- Background check and consumer reporting agencies.
- Insurance carriers, brokers, and claims administrators, including workers' compensation and general liability carriers.
- Federal, state, and local government agencies and regulators, including taxing authorities, labor agencies, licensing boards, and law enforcement when required by law.
- Clients, project owners, and project partners, limited to information necessary for jobsite access, badging, safety compliance, or project-specific requirements.
- Subcontractors and joint venture partners, to the extent necessary for project coordination and compliance.
- IT service providers, cybersecurity vendors, and cloud storage and data hosting providers.
- Professional advisors, including legal counsel, accountants, auditors, and consultants, under obligations of confidentiality.
- Potential acquirers, investors, or financing parties in connection with a corporate transaction, under appropriate confidentiality obligations.
- Other employees or Company personnel on a need-to-know basis for legitimate business purposes.

We do not sell your personal information. We do not share your personal information for cross-context behavioral advertising. These restrictions apply to the personal information of both employees and job applicants.

How Long We Keep Your Personal Information

We retain your personal information only for as long as reasonably necessary to fulfill the purposes described in this Notice, including to satisfy legal, regulatory, accounting, and operational requirements. The criteria used to determine retention periods include the nature of the information, the purposes for which it was collected, applicable legal requirements, and business necessity.

Your California Privacy Rights

As a California employee or job applicant, you have the following rights with respect to your personal information under the CCPA/CPRA. These rights are subject to certain legal exceptions and limitations, including where the information is necessary for Company to comply with legal obligations, complete a transaction, or exercise legal rights.

- **Right to Know.** You have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the sources from which it was collected, the purposes for which it was collected, and the categories of third parties with whom it has been shared.
- **Right to Delete.** You have the right to request deletion of personal information we have collected about you. We may deny your request where retention is necessary to comply with a legal obligation, complete your employment relationship, exercise legal rights, or for other purposes permitted under CCPA/CPRA.
- **Right to Correct.** You have the right to request correction of inaccurate personal information we maintain about you. We will use commercially reasonable efforts to correct the information as directed, taking into account the nature of the information and the purposes for which it is maintained.
- **Right to Limit Use of Sensitive Personal Information.** You have the right to request that we limit our use and disclosure of your Sensitive Personal Information to purposes expressly permitted under CCPA/CPRA. As described above, Company uses Sensitive Personal Information only for purposes that do not trigger this right, so it has limited practical applicability in the employment context.
- **Right to Non-Discrimination.** You have the right not to be discriminated or retaliated against for exercising any of your privacy rights under this Notice. Company will not deny you employment opportunities, alter your compensation, or take any adverse employment action against you for exercising these rights.

How to Exercise Your Rights

To submit a privacy rights request, you may contact Company's Human Resources department using any of the following methods:

Human Resources
Mountain Cascade, Inc.
Email: hr@moutaincascade.com
Address: 555 Exchange Ct
Livermore, CA 94550

When submitting a request, please include your full name, employee ID number or last four digits of your Social Security Number, department, and a description of your request so we can locate your information and respond efficiently.

Response Time. We will respond to your request within 45 days of receipt. If we require additional time, we will notify you within the initial 45-day period and may extend our response by an additional 45 days where reasonably necessary, for a maximum total response period of 90 days.

Verification. To protect your personal information, we are required to verify your identity before processing your request. We may ask you to confirm identifying information such as your employee ID number, last four digits of your Social Security Number, job title, or other details consistent with the information we maintain about you. The verification steps we take may vary depending on the sensitivity of the information requested.

Authorized Agents. You may designate an authorized agent to submit a request on your behalf. To do so, you must provide the agent with signed written authorization permitting them to act on your behalf, and we may require you to verify your own identity directly with us before we process the request. We may deny a request from an agent who does not provide sufficient proof of authorization.

No Fee. We do not charge a fee to process or respond to your privacy rights request unless it is excessive, repetitive, or manifestly unfounded. If we determine that a fee is warranted, we will notify you of the fee and provide a cost estimate before completing your request.

Last Updated: July 15, 2026. Mountain Cascade, Inc. may update this Notice from time to time to reflect changes in our practices or applicable law.