

Notice at Collection and Privacy Policy for California Job Applicants

Last Updated: **December 20, 2022**

EMCOR Group, Inc. and its subsidiaries and affiliated companies ("Company") takes your privacy seriously. We want you to know how we collect, use, and disclose, your personal information.

EEO Statement

Company is an equal employment opportunity employer. The Company's policy is not to unlawfully discriminate against any applicant or employee on the basis of race, color, sex, religion, national origin, age, disability, or any other consideration made unlawful by applicable federal, state, or local laws. The Company also prohibits harassment of applicants and employees based on any protected category, characteristic or status. It is also the Company's policy to comply with all applicable state, federal and local laws respecting consideration of unemployment status in making hiring decisions.

Company complies with the ADA, the ADAAA and applicable state law and considers reasonable accommodation measures that may be necessary for qualified applicants/employees to perform the essential functions of the job. Hire may be contingent upon a post-offer medical examination, and to skill and agility tests, as appropriate for the position.

Assistance For The Disabled

Alternative formats of this Privacy Policy are available to individuals with a disability. Please contact emcor_info@emcor.net for assistance.

This Privacy Policy explains:

1. The categories of personal information we collect about you
2. The categories of sources from which we collect your personal information
3. The purposes for which we use your personal information
4. How we may disclose your personal information
5. How long we keep your personal information
6. Your rights and how to exercise them
7. Changes to this Privacy Policy

Scope:

This Privacy Policy applies to the personal information of California residents in their role as job applicants to Company ("Applicants").

"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 Applicant.

1) THE CATEGORIES OF PERSONAL INFORMATION WE COLLECT ABOUT YOU

- a) **Identifiers**, for example: real name, nickname, telephone number, postal address, e-mail address, and signature.
- b) **Professional or employment-related information**, for example: evaluations, certifications, licenses, employment history, and professional memberships and affiliations.
- c) **Educational information**, for example: academic transcripts, educational discipline records, and academic counseling records.
- d) **Background screening Information**: Company collects background screening information, including results of the following types of background screening: criminal history; sex offender registration; motor vehicle records;

credit history; employment history; drug and/or alcohol testing (as permitted by applicable law); and educational history.

- e) **Commercial information**, for example: travel expense records for an interview.
- f) **Internet and other electronic activity information**, for example: interactions with Company's email system and other networks and systems, browsing history, job application, or job advertisement, and publicly available social media activity.
- g) **Audio or visual information**, for example: audio/visual recordings of interviews, and footage from video surveillance cameras.
- h) **§ 1798.80**: personal information described under Cal. Civ. Code § 1798.80 to the extent not already included in other categories in this section, such as a photograph and physical description for security and internal identification purposes.
- i) **Other details**, for example, hobbies and leisure activities or membership in voluntary/charitable/public organizations, for example, as stated on the Applicant's resume.
- j) **Inferences**: Company collects profile data, which may include the following: individual's preferences, characteristics, predispositions, behavior, and aptitudes.
- a) **Sensitive personal information**, for example: sensitive identifiers such as Social Security, driver's license, state identification card, or passport number, account log-in, information concerning health, biometric information, and information concerning racial or ethnic origin.
- b) **Biometric information**, for example, a fingerprint to conduct criminal history background checks, imagery of the face, hand, palm, and voice recordings from an identifier template, such as a fingerprint, a minutiae template, or a voiceprint can be extracted.
- c) **Geolocation data**, for example: through a radio frequency identification (RFID) chip in a security badge to determine an Applicant's physical location.

Characteristics of Protected Classifications Under California or Federal Law:

Company collects information about race, age, national origin, disability, sex, and veteran status as necessary to comply with legal obligations, including the reporting requirements of the federal Equal Employment Opportunity Act, the federal Office of Contracting Compliance Programs (applicable to government contractors), and California's Fair Employment and Housing Act, and for purposes of diversity analytics.

The Company collects this category of Personal Information on a purely voluntary basis, except where collection is required by law, and uses the information only in compliance with applicable laws and regulations.

Note on inferring characteristics: Company does not collect or process sensitive personal information or characteristics of protected classifications for the purpose of inferring characteristics about the Applicant.

2) THE CATEGORIES OF SOURCES FROM WHICH WE COLLECT YOUR PERSONAL INFORMATION

- **You**, for example, in your job application, forms you fill out for us, assessments you complete, surveys you complete, and any information you provide us during the course of your application and interview process.
- **Vendors and service providers**, for example, recruiters, safety councils, drug testing consortiums.
- **Third parties**, for example, job references, affiliated companies, professional employer organizations, staffing agencies, or labor unions and joint apprenticeship training programs.
- **Public internet sources**, for example, social media, job boards, public profiles, and other public online sources
- **Public records**, for example, court records, and credentialing and licensing organizations.
- **Automated technologies** such as cookies on Company's electronic resources, for example, to track activity on Company's careers page.
- **Surveillance/recording technologies installed by Company**, for example, video surveillance in common areas of Company facilities, webcams, and audio/video recording technologies with consent to the extent required by law.

- **Government or administrative agencies**, for example, law enforcement or public health authorities.
- **Acquired company**, if Company acquired your employer, Company might collect personal information from that employer.

Note: This Privacy Policy does not cover background screening conducted by third-party background check vendors subject to the federal Fair Credit Reporting Act. Company provides a separate disclosure for such screening.

3) THE PURPOSES FOR WHICH WE USE YOUR PERSONAL INFORMATION

A. Generally Applicable Purposes:

Unless stated otherwise in section 3.B, below, we may use Applicants' personal information for the following purposes:

Recruiting

- To evaluate Applicants' qualifications or suitability for employment with Company
- To communicate with Applicants
- To conduct a pre-employment or criminal history background check
- For identification purposes
- For diversity and inclusion purposes
- To arrange and manage Company-sponsored events
- To create a talent pool for future job openings
- For recordkeeping purposes
- To demonstrate Applicants' agreement to, or acceptance of, documents presented to them, *e.g.*, pre-employment arbitration agreement, acknowledgment of employment application, offer letter
- To evaluate and improve the recruiting process
- To promote Company as a place to work

Monitoring, Security, and Compliance:

- To monitor use of Company information systems and other electronic resources
- To help maintain the safety, security, and integrity of Company information systems and other electronic resources
- To conduct internal audits
- To conduct internal investigations
- To protect the safety and security of Company's facilities, Company employees and others
- To administer Company's whistleblower hotline
- To report suspected criminal conduct to law enforcement and cooperate in investigations
- To control access to secure facilities
- To monitor compliance with Company policies
- To impose discipline
- To exercise Company's rights under applicable law and to support any claim, defense, or declaration in a case or before a jurisdictional and/or administrative authority, arbitration, or mediation panel

Conducting Our Business:

- For training purposes or quality assurance with respect to Company employees conducting the interviews or otherwise assisting with the recruiting and hiring process
- To engage in crisis management
- To manage travel reimbursements

Miscellaneous Other Purposes:

- To manage and operate information technology and communications systems, risk management and insurance functions, budgeting, financial management and reporting, strategic planning;
- To manage litigation involving Company, and other legal disputes and inquiries and to meet legal and regulatory requirements;
- In connection with a corporate transaction, sale, or assignment of assets, merger, divestiture, or other changes of control or financial status of Company or any of its subsidiaries or affiliates;
- To manage licenses, permits, and authorizations applicable to Company's business;
- To satisfy Company's reporting obligations to taxing authorities and other government agencies; and
- To protect the rights, property, or safety of Company, HR Individuals, customers or others.

B. Purposes Specific To Sensitive Personal Information and Related Categories Of Personal Information:

We may use the categories of Applicants' personal information listed in this Section 3.B for the purposes stated below:

Purposes for Using Applicants' Sensitive Identifiers:

Company uses background screening information to evaluate Applicants' qualifications for employment with Company.

Purposes For Using Applicants' Biometric Information:

Company uses biometric technology to control access to secure facilities systems and to protect the safety and security of Company facilities during the interview and hiring process. Company also uses biometric information to conduct criminal background checks.

Purposes For Using Applicants' Geolocation Data:

Upon entry to Company's facilities, Company may issue Applicants an RFID-enabled security badge. Company will use this information to confirm that an Applicant has arrived and left Company facilities when scheduled, to monitor the safety of the Applicant, and to protect the safety and security of Company facilities.

Purposes For Using Applicant Health Information:

- To the extent necessary to comply with Company's legal obligations, such as to accommodate disabilities
- To protect the health and safety of Company's employees and facilities, for example, to take the Applicant's temperature
- For occupational health surveillance
- For occupational health and safety compliance and record-keeping
- To conduct pre-employment and fitness-for duty medical examinations
- To respond to an Applicant's medical emergency

Note: This Privacy Policy does not cover health information governed by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), or California's Confidentiality of Medical Information Act (CMIA).

Purposes For Using Applicants' Protected Categories Of Information:

Company collects information about race, age, national origin, disability, sex, and veteran status as necessary to comply with legal obligations, including the reporting requirements of the federal Equal Employment Opportunity Act, the federal Office of Contracting Compliance Programs (applicable to government contractors), and California's Fair Employment and Housing Act, and for purposes of diversity analytics.

Company also uses this personal information for purposes including: (a) with respect to disability and/or medical condition, as necessary, to comply with federal and California law related to accommodation; and (b) with respect to age, incidentally to the use of birth date for identity verification.

Company collects protected categories of Personal Information on a purely voluntary basis, except where required by law, and uses the information only in compliance with applicable laws and regulations.

C. Purposes For Using Deidentified Information

At times, Company converts personal information into deidentified information using reasonable measures to ensure that the deidentified information cannot be associated with the individual (“Deidentified Information”). Company maintains Deidentified Information in a deidentified form and does not attempt to reidentify it, except that Company may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes ensure that the information cannot be associated with the individual. Company prohibits vendors, by contract, from attempting to reidentify Company’s Deidentified Information.

4) HOW WE MAY DISCLOSE YOUR PERSONAL INFORMATION

Company generally maintains information related to Applicants as confidential. However, from time to time, Company may have a legitimate business need to disclose Applicants’ personal information for one of the purposes listed in Section 2, above, to one or more of the categories of external recipients listed below. In that event, Company discloses your personal information and/or sensitive personal information only to the minimum extent necessary to achieve the purpose of the disclosure and only if the disclosure is permitted by the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the “CCPA”) and other applicable laws.

- **Service providers and contractors:** Company discloses your personal information to service providers and contractors for the purposes above to assist us in our recruiting efforts and in meeting our business needs and legal obligations.
 - Company only discloses your personal information to service providers and contractors subject to written contracts as required by applicable law.
 - Service providers and contractors include recruiters, law firms, travel agencies, and any other entity providing services to Company.
- **Affiliated companies:** Other companies within the EMCOR Group, Inc. family of companies.
- **Clients and customers:** This may include, for example, disclosing an applicant’s personal information to a client for the purposes of the client granting an applicant access to a secured-entry work-site; we may also disclose an applicant’s resume in connection with work applicant will be performing for the client.
- **Labor Unions:** This may include, for example, disclosing an applicant’s personal information when requesting to hire an employee by name from a Union hall.
- **Government or administrative agencies:** These may include, for example:
 - Equal Employment Opportunity Commission as required for reporting.
 - California Department of Fair Employment and Housing as required to respond to employment claims and charges.
 - Law enforcement in the event of criminal investigations.
- **Required Disclosures:** We may be required to disclose personal information in a court proceeding, in response to a court order, subpoena, civil discovery request, other legal process, or as otherwise required by law.
- **Legal Compliance and Protections:** We may disclose personal information when we believe disclosure is necessary to comply with the law or to protect the rights, property, or safety of Company, our users, or others.
- **Corporate Transactions:** We may disclose your personal information in connection with a corporate merger, consolidation, bankruptcy, the sale of all, or substantially all, of our membership interests and/or assets or other corporate change, including to any prospective purchasers.

No sales and no “sharing”, i.e., disclosure for cross-context behavioral advertising:

Company does not sell the personal information of any Applicants nor share their personal information for cross-context behavioral advertising.

5) HOW LONG WE KEEP YOUR PERSONAL INFORMATION

If Company hires you, the information collected about you during the job application process may become part of your personnel file and may be used to administer the employment relationship and for related reporting and recordkeeping purposes. Company will retain this application information for the entire duration of your employment relationship with Company and for as long thereafter as permitted or required by applicable law. Company makes its document retention schedule available to employees for review.

Company will retain information of Applicants who are not hired for four (4) years after the record is collected. These records will be retained for our internal recordkeeping and reporting purposes in compliance with California Government Code § 12946. During that time, we may use your information to consider you for positions in addition to the position(s) for which you initially applied.

6) YOUR PRIVACY RIGHTS AND HOW TO EXERCISE THEM

a. Your California Privacy Rights

Subject to applicable law, Applicants have the following rights:

- **Right to Know:** You have the right to submit a verifiable request for information about the categories of personal information we collect from you as well as to obtain copies of specific pieces of your personal information collected.
- **Right to Delete:** You have the right to submit a verifiable request for the deletion of personal information that you have provided to Company.
- **Right to Correct:** You have the right to submit a verifiable request for the correction of inaccurate personal information maintained by Company, taking into account the nature of the personal information and the purposes of processing the personal information.

Please note that the rights described here are not absolute and we reserve all of our rights available under applicable laws.

b. How to Exercise Your Rights

Company will respond to requests know, delete, and correct in accordance with applicable law if it can verify the identity of the individual submitting the request. You can exercise these rights in the following ways:

- Call 888-711-3648
- Email employeeatarequest@emcor.net with the phrase "California Consumer Rights" in the subject line.

c. How We Will Verify Your Request:

The processes that we follow to verify your identity when you make a request to know, correct, or delete are described below. The relevant process depends on how and why the request is submitted.

If you submit a request by any means other than through a password-protected account that you created before the date of your request, the verification process that we follow will depend on the nature of your request as described below:

1. **Requests To Know Categories Or Purposes:** If you request to know how we collect and handle your personal information, we will match at least two data points that you provide with your request, or in response to your verification request, against information about you that we already have in our records and that we have

determined to be reliable for purposes of verifying your identity. Examples of relevant data points include your mobile phone number, your zip code, and the month and year you submitted a job application to us.

2. **Requests To Know Specific Pieces Of Personal Information:** We will match at least three data points that you provide with your request to know, or in response to our request for verification information, against information that we already have about you in our records and that we have determined to be reliable for purposes of verifying your identity. In addition, we may require you to sign a declaration under penalty of perjury that you are the individual whose personal information is the subject of the request.
3. **Requests To Correct or Delete Personal Information:** Our process for verifying your identity will depend on the sensitivity (as determined by Company) of the personal information that you ask us to correct delete. For less sensitive personal information, we will require a match of two data points as described in Point No. 1, above. For more sensitive personal information, we will require a match of three data points and a signed declaration as described in Point No. 2, above.

We have implemented the following additional procedures when verifying the identity of requestors:

1. If we cannot verify your identity based on the processes described above, we may ask you for additional verification information. If we do so, we will not use that information for any purpose other than verification.
2. If we cannot verify your identity to a sufficient level of certainty to respond to your request, we will let you know promptly and explain why we cannot verify your identity.

d. Authorized Agents

If an authorized agent submits a request to know, correct or delete on your behalf, the authorized agent must submit a document signed by you that authorizes the authorized agent to submit the request on your behalf. In addition, we may ask you or your authorized agent to follow the applicable process described above for verifying your identity. You can obtain “Authorized Agent Designation” form by contacting us at emcor_info@emcor.net.

d. Company’s Non-Discrimination and Non-Retaliation Policy

Company will not unlawfully discriminate or retaliate against you for exercising your privacy rights under the California Privacy Rights Act.

7) CHANGES TO THIS PRIVACY POLICY

If we change this Privacy Policy, we will post those changes on this page and update the Privacy Policy modification date above. If we materially change this Privacy Policy in a way that affects how we use or disclose your personal information, we will provide a prominent notice of such changes and the effective date of the changes before making them.

For More Information

For questions or concerns about Company’s privacy policies and practices, please contact us at emcor_info@emcor.net.