



## CALIFORNIA PRIVACY NOTICE FOR APPLICANTS

This California Privacy Notice supplements the general Privacy Policy of **Burns Engineering, Inc.** ("we," "us," or "our"). It applies solely to California residents who submit job or user applications ("applicants" or "you"). We adopt this notice to comply with the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA").

As a federal contractor subject to Office of Federal Contract Compliance Programs (OFCCP) and Equal Employment Opportunity Commission (EEOC) regulations, we collect and retain specific applicant information to fulfill statutory affirmative action and non-discrimination obligations.

### 1. Information We Collect

In the preceding 12 months, we have collected the following categories of personal information from applicants for employment or platform evaluation:

- **Identifiers:** Full name, email address, mailing address, and mobile phone number.
- **Sensitive Personal Information:** Social Security Number (SSN), driver's license number, or other government-issued identification used for identity verification or background screening.
- **Protected Classification Characteristics:** Voluntary self-identification data, including race, gender, veteran status, and physical or mental disability status.
- **Professional & Employment-Related Information:** Resume, employment history, qualifications, and background check results (including criminal history or reference checks where legally permitted).
- **Application History:** System logs detailing your application status, history, and communication preferences.
- **Internet/Electronic Network Activity:** Information regarding your interaction with our online application portal or website.

### 2. Sources of Information

We obtain these categories of personal information from the following sources:

- **Directly from you:** Information you type into online forms, application questionnaires, and voluntary demographic self-identification forms during the application process.
- **Third parties:** Consumer reporting agencies or background check vendors that perform authorized screenings on our behalf.

### 3. Use of Personal Information & System-Generated Texting

We use your personal information and sensitive personal information primarily to process, evaluate, verify, and track your application.

- **OFCCP Affirmative Action Program (AAP) Compliance:** We collect voluntary protected classification data (race, gender, veteran, and disability status) solely to satisfy federal recordkeeping, data analysis, and reporting mandates. This information is kept strictly confidential, stored separately from standard application forms, and is never used to make hiring or employment decisions.
- **System-Generated Text Messages:** If you choose to receive updates via text, our automated system will send application status changes, reminders, and screening notifications to your mobile device.
- **Opting Out of Texts:** You can opt out of these system-generated texts at any time. To stop receiving messages, simply reply "STOP" to any text message received from our system. You will receive one final text confirming your unsubscription.
- **Email Updates:** Standard transactional updates will also be routed to your email address provided.

### 4. Use and Limitation of Sensitive Personal Information

We collect and use your Social Security Number and other government identifiers strictly for regulatory compliance, identity verification, and performing authorized pre-employment background screening. We **do not** use or disclose your Sensitive Personal Information for any purposes other than those business purposes explicitly authorized under CCPA regulations.

### 5. Sharing and Selling Personal Information

In the preceding 12 months, we have not sold applicants' personal information or shared it with third parties for cross-context behavioral advertising.

- We only disclose identifiers and background screening criteria to trusted background check vendors and system communication vendors to execute the recruitment process.
- Demographic data collected for AAP compliance is reported in aggregate to federal agencies when required and is never disclosed to hiring managers or third-party marketing entities.

### 6. Data Retention & Regulatory Compliance

We retain your application records, text messaging logs, background check disclosures, and demographic self-identification metrics in strict accordance with federal law:

- **Federal Contractor Retention Thresholds:** Pursuant to OFCCP recordkeeping standards (41 CFR 60-1.12), we retain all personnel and applicant records for **two (2) years** from the date the record was made or the personnel action was taken, whichever is later.
- **Extended Audit Retention:** If an administrative charge, compliance evaluation, or lawsuit is pending, all records will be retained indefinitely until final disposition of the matter.

## 7. Your Rights Under the CCPA:

California residents have specific rights regarding their personal information:

- **Right to Know/Access:** Request disclosure of the specific pieces or categories of personal information we hold about you.
- **Right to Delete:** Request that we delete the personal information collected from you. Please note that the CCPA permits us to deny a deletion request if retaining the information is legally required to comply with federal compliance mandates, including EEOC and OFCCP records retention laws.
- **Right to Correct:** Request corrections to inaccurate personal data (e.g., an error on your application or contact info).
- **Right to Non-Discrimination:** We will not deny employment or discriminate against you for exercising your privacy rights.

## 8. How to Exercise Your Rights:

To exercise your CCPA rights to know, delete, or correct your data, please submit a request via:

- **Emailing us at:** [hrdepartment@burns-group.com](mailto:hrdepartment@burns-group.com)
- **Calling us at:** 215-240-6073