

California Job Applicant Privacy Notice

Last Updated: April 1, 2026

The purpose of this California Job Applicant Privacy Notice (“Privacy Notice”) is to inform individuals who inquire about and/or apply for employment (“you” or “Job Candidates”) with **International Training & Exchange, Inc.** and its subsidiaries and affiliates (the “Company”, “Intrax” or “we” or “us”) of the categories of personal information we collect and the purposes for which we use and disclose such personal information for employment consideration.

As a job applicant, you have the right to know and understand the categories of personal information we collect about you, and the purposes for which we use such personal information, pursuant to the California Consumer Privacy Act of 2018, effective as of January 1, 2020, as subsequently amended by the California Privacy Rights Act of 2020, effective January 1, 2023, and Assembly Bill 1008, effective January 1, 2025, (collectively, “CPRA”), and applies solely to residents of the State of California. This Privacy Notice only applies to job applicants who are residents of the State of California.

1. Categories of Personal Information Collected

This section sets forth the categories of “personal information” (as such term is defined under the CPRA) we may collect about you when you inquire about and/or apply for employment at Intrax. In the preceding twelve (12) months, we have collected the following categories of personal information from one or more of the job candidates.

- **Personal identifiers**, such as your name, preferred name, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, date of birth, and other similar identifiers.
- **Personal Records**, such as your signature, Social Security number, address, telephone number, education, employment or employment history.
- **Protected characteristics**, such as minority, veteran and disability status, through voluntary self-disclosure. Such information will only be collected as permitted by applicable law and will not be used to make hiring decisions.
- **Internet or other similar network activity information**, such as your IP address, log-in information or information regarding your interaction with a website, application or advertisement.
- **Geolocation Data**, such as IP addresses from which we can determine your general location.

- **Sensory data**, such as audio and visual information, for example if you use video interviewing as part of the application process. If you visit our facilities, your entry and exit may be monitored by CCTV.
- **Professional or employment-related information**, such as your work history, references, information about skills and abilities, accomplishments and awards, training and development information, performance evaluation information, and employment termination information.
- **Education information**, such as your education history, education records (such as grades, transcripts and class lists), professional certifications (if applicable), and other information included in your resume or cover letter.
- **Inferences drawn from other personal information**, such as a profile reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.
- **Other**: Job interview notes, responses to screening questions, assessment results, and any other information you provide in connection with the recruitment process. We also collect legal and contractual information, such as information necessary to respond to law enforcement and governmental agency requests, comply with legal and contractual obligations, exercise legal and contractual rights, and initiate or respond to, or establish, exercise and defend, legal and contractual rights claims.

Certain categories of personal information we collect, including Social Security number, racial or ethnic origin, disability status, and video or audio information, constitute Sensitive Personal Information under the CPRA. We process this information only for the purposes described above (such as evaluating your application, complying with legal obligations, or supporting diversity and inclusion efforts) and, where required by law, based on your explicit consent.

2. Sources of Personal Information

We collect personal information you voluntarily provide to us when you apply for a job or otherwise contact us in the recruitment context. If you are visiting our website or online job application, we may also automatically collect device information such as IP addresses and device identifiers.

We may also combine personal information collected from other sources with the personal information that you provide to us. For example, we may collect information from:

- Recruiters
- Prior employers (e.g., for references)
- Professional references you provide to us
- Educational institutions
- Pre-employment screening services

- Credentialing and licensing organizations
- Publicly available sources such as your social media profile (e.g., LinkedIn)
- Other sources as directed by you

We may combine information that we receive from the various sources described in this Privacy Notice, including third party sources and public sources, and use or disclose it for the purposes set forth in this Privacy Notice.

3. Use of Personal Information

We use the categories of personal information listed above for the following purposes:

- **Process and manage your application:** We use your personal information to process your job application, establish a job applicant profile for the recruitment process, assess your qualifications for a specific role with us, schedule and conduct interviews, communicate with you, and carry out background and reference checks (see the following bullet point for additional information). We may collect audio and visual information of job applicants through photographs used for identification purposes. With your consent, we may record video of you in connection with the application process, for example through a third-party screening service. Additionally, if you are offered a position with us, we may use your personal information in the employee on-boarding process.
- **Conduct reference and background checks (as permitted by applicable law):** We use personal information we collect to conduct reference checks and to evaluate your qualifications and experience. We may also conduct background checks (as authorized by you and permitted by applicable law).
- **Provide immigration support:** If applicable and as permitted by applicable law, we may collect your personal information to assist with immigration support, such as applying for visas or work permits.
- **Analyze and improve our recruitment process and tools:** For example, we analyze trends in our applicant pool and use personal information to understand and improve our recruitment process and tools (including improving diversity and inclusion). If you use our online job application process, we collect personal information in this category, such as your interactions with our “Careers” page and our online application process. We collect IP address location information to better understand how candidates use our careers page and online application process.
- **Record-keeping:** We keep records of your personal information as required by law and in accordance with our record retention policies.
- **Meeting legal requirements and enforcing legal terms:** We collect and process your personal information for purposes of fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and

investigating security incidents and potentially illegal or prohibited activities; protecting the rights, property or safety of you, us or another party; enforcing any agreements with you; responding to claims; and resolving disputes. Additionally, we may use information about protected characteristics to analyze and monitor the diversity of our job applicants in accordance with applicable laws.

- **Sensitive Personal Information:** During the recruitment process, we generally do not collect or process any Sensitive Personal Information as defined in the CPRA. However, there are circumstances in which we are required or permitted by local law to process Sensitive Personal Information provided, however, any processing of your sensitive personal information in connection with your job application is based on your explicit consent. For example, Intrax may be required to collect information about your racial/ethnic origin, gender and disabilities for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws or for government reporting obligations. Similarly, information about your physical or mental condition may be collected in order to consider accommodations we need to make for the recruitment process and/or subsequent job role. You may also provide, on a voluntary basis, other Sensitive Personal Information during the recruiting process. Please note that you can always withdraw your consent, although this may affect our ability to consider you for employment at Intrax.

If we collect any Sensitive Personal Information (as defined under the CPRA), we will process it only for the limited, necessary purposes disclosed above (e.g., equal opportunity compliance, background checks, or as required by law). To the extent required under the CPRA, you may request restrictions on the use or disclosure of your Sensitive Personal Information. If you choose to withdraw consent for processing of Sensitive Personal Information, please contact us — note that this may affect our ability to continue evaluating your application.

4. Disclosure of Personal Information

We may share your personal information as necessary for the purposes described in this Privacy Notice, including internally with our personnel involved in the hiring process. We make third party business purpose disclosures under written contracts that describe the purposes, require the recipient to keep the personal information confidential, and prohibit using the disclosed information for any purpose except performing the contract. We share, and during the past 12 months, we have shared for our business purposes the categories of personal information listed above to the following categories of third parties:

- **Affiliates:** We may share your personal information with our affiliates.
- **Service Providers:** We use service providers to operate, host and facilitate our hiring and recruitment process. These include hosting, technology and communication providers; security and fraud prevention consultants; analytics providers; background and reference check screening services; and hiring process management tools.

- **Government authorities and law enforcement:** In certain situations, we may be required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- **Business transfers:** Your personal information may be transferred to a third-party if we undergo a merger, acquisition, bankruptcy or other transaction in which that third party assumes control of our business (in whole or in part).
- **Professional advisors:** We may share your personal information with our professional advisors.
- **Other:** We may also share your personal information with third parties in conjunction with any of the activities set forth under “Meeting legal requirements and enforcing legal terms” in the “Use of Personal Information” section above.

5. Sale of Personal Information

We do not sell (as such term is defined under the CPRA) your personal information to third parties. This means that we do not sell your personal information to third parties in exchange for monetary or other valuable consideration.

6. How long we retain your personal information

We will only retain your personal information for as long as reasonably necessary to fulfill the purposes we collected it for, including satisfying any legal, regulatory, tax, 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 unauthorized 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, regulatory, tax, accounting or other requirements. When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it or, if this is not possible (e.g., because your personal information has been stored in backup archives), we will securely store your personal information and isolate it further from any further processing until deletion is possible.

For each category of personal information (including any sensitive personal information) collected, we retain the information only for as long as is reasonably necessary to fulfill the disclosed purposes (such as processing your application, background screening, compliance with legal obligations, or on-boarding), unless a longer retention period is required by law. Where we do not delete the information, we will continue to store it securely and isolate it from further processing until deletion is possible.

7. Your California Rights under the CPRA

Subject to certain legal exceptions, the CPRA provides California residents with specific rights regarding their personal information. This section describes your CPRA rights and explains how to exercise those rights.

7.1 Right to Know and Data Portability

Subject to certain exceptions, you have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months (the “right to know”). Once we receive your request and confirm your identity, we will disclose to you: 1. The categories of personal information we collected about you; 2. The categories of sources for the personal information we collected about you; 3. Our business or commercial purpose for collecting that personal information; 4. The categories of third parties with whom we share that personal information, including identifying the personal information categories that each category of recipient obtained; and 5. The specific pieces of personal information we collected about you (also called a data portability request). To make a right to know and data portability request, please submit a request by emailing us at privacy@intrax.io.

7.2 Right to Delete

Subject to certain exceptions, you have the right to request that we delete any of your personal information that we collected from you and retained.

7.3 Right to Correct

Subject to certain exceptions, you have the right to correct inaccurate personal information that we maintain about you.

7.4 Right to Limit

Use or Disclosure of Sensitive Personal Information: If we collect your Sensitive Personal Information (such as Social Security number, racial or ethnic origin, disability status, or video/audio information), you have the right to request that we only use or disclose it for the limited, necessary purposes permitted under the CPRA.

7.5 Right to opt out of selling or “sharing” certain Personal Information

You have the right to opt out of the sale or sharing of your personal information. The California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CPRA”), requires us to describe the categories of personal information we sell or share with third parties and how you can opt out of future sales or sharing. Under the CPRA, personal information includes, among other things, internet or other electronic network activity information, such as identifiers associated with devices or online activity (e.g., IP addresses, cookie identifiers, pixels, and mobile identifiers). The CPRA defines “sharing” broadly and, in some cases, includes making personal information available to third parties for cross-context behavioral advertising.

You may opt out of receiving promotional emails from us by using the unsubscribe link in each email, updating your email preferences in your Service account settings, or by contacting us as

described below. Please note that opting out of promotional communications does not affect transactional or service-related messages, which we may continue to send. You may manage certain notification preferences through your account settings.

You also have the right to opt out of the sharing of your personal information for cross-context behavioral advertising. We use a consent management platform to process California consumer opt-out requests and to communicate those preferences to our systems and applicable partners in accordance with applicable law. You may use this platform to submit an opt-out request or to confirm the status of your preferences by contacting us at hr@intraxinc.com or 455 Market Street, Suite 1700, San Francisco, CA 94105.

8. How to Exercise your CPRA Rights

To exercise your rights to know, or delete or correct under the CPRA, please submit a request by emailing us at hr@intraxinc.com. Only you, or someone legally authorized to act on your behalf, may make a request to know or delete related to your personal information. You may only submit a request to know twice within a 12-month period. Your request must provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative. 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.

9. Response Timing and Format

We endeavor to substantively respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to another forty-five (45) days), we will inform you of the reason and extension period in writing. 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. We do not charge a fee to process or respond to your verifiable consumer 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.

10. Non-discrimination

We will not discriminate against you for exercising any of your CPRA rights.

11. Updates

We may amend this Privacy Notice from time to time. When we do, we will post the revised Privacy Notice on our website www.intraxinc.com/careers.

12. Contact for Questions

If you have any questions or concerns regarding this Privacy Notice or the collection of your personal information, please contact hr@intraxinc.com.