Talent Platform Security Policy

1. **PRIVACY STATEMENT**

iCIMS, Inc. and iCIMS International, LLC ("iCIMS") has created this privacy statement to demonstrate a commitment to privacy. The following information discloses information gathering and dissemination practices for the iCIMS-hosted software components, as further defined in iCIMS's Subscription Agreement (collectively, the "Subscription").

A. General Data Protection Regulation (GDPR), EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

iCIMS, Inc. and its subsidiary company iCIMS International, LLC recognize the importance of protecting and ensuring the integrity of sensitive data, including personal data as defined by the European Union (EU) General Data Protection Regulation (GDPR).

iCIMS, Inc. and its subsidiary company iCIMS International, LLC also participate in and have certified their compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. iCIMS is committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, in reliance on each Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Frameworks, visit the U.S. Department of Commerce's Privacy Shield List.

iCIMS is responsible for the processing of personal data it receives, under GDPR and each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. iCIMS complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to GDPR iCIMS is subject to the regulatory enforcement powers of the EU in conjunction with the U.S. Federal Trade Commission. For each Privacy Shield Framework, iCIMS is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain circumstances, iCIMS may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with GDPR and the Privacy Shield Principles, iCIMS commits to resolve complaints about our collection and use of your personal data.

iCIMS commits to cooperate with the panel established by the EU Data Protection Authorities (DPAs) and/or the Swiss Federal Data Protection and Information Commissioner, as applicable and comply with the advice given by the panel and/or Commissioner, as applicable with regard to human resources data transferred from the EU and/or Switzerland, as applicable in the context of the employment relationship.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

B. Information Collection and Use

iCIMS is not responsible for the privacy practices of other organizations ("subscribers") that use the Subscription under a subscription agreement with iCIMS. This privacy statement applies solely to the role iCIMS plays in collecting and storing data via the Subscription for its subscribers. If you are using the Subscription by and through a subscriber, the subscriber's privacy practices control. iCIMS encourages users of the Subscription to read the privacy statements of each and every applicable company to which they apply. It is the responsibility of the subscriber to provide its privacy practices to you so please reach out to that organization to obtain relevant privacy practices.

The use of information collected through the Subscription shall be limited to the purpose of providing the service for which the particular subscriber has engaged iCIMS.

The Subscription collects personal identifiable information (PII) (such as, name, work history, and home address) through a number of points throughout iCIMS products. Candidates or employees may enter PII directly through the Subscription and/or indirectly through a subscriber's HR staff or other systems (i.e., data entered manually or fed electronically from another system into the Subscription).[1] PII within the Subscription is stored within the applicable Data Center for a subscriber. Specific details regarding the Data Center are available at https://www.icims.com/gc-it.

Candidate users may have the ability to remain anonymous during the initial states of the application process depending on the subscriber's configuration of the web portal in the Subscription.

C. Choice

The Subscription collects information for its subscribers. Unless otherwise removed by the subscriber, users are given open notice of and the choice to provide PII.

If you are a candidate or employee user of one of our subscribers and would no longer like to be contacted by one of our subscribers that use the iCIMS subscription, please contact the applicable subscriber directly.

By submitting your information to iCIMS, you acknowledge and agree that the technical processing and transmission of your information, may involve, (a) transmissions over various networks, including the transfer of this information to the United States and/or other countries for storage, processing and use by iCIMS, its affiliates, and their agents; and (b) changes to conform and adapt to technical requirements of connecting networks or devices. Accordingly, you agree to permit such parties to make such transmissions and changes.

D. Correction /Updating PII

iCIMS acknowledges that you have a right to access your PII. iCIMS has no direct relationship with the individuals whose PII it processes. A candidate or employee user who seeks access, or who seeks to correct, amend, or delete inaccurate data may do so by directly logging into the applicable career site or by contacting the subscriber's HR staff (the data controller) to update the data within their subscription.

E. Data Retention

iCIMS will retain PII we process on behalf of our subscribers within the Subscription for as long as needed to provide services to our subscribers. iCIMS will retain this PII as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. iCIMS will retain back-up copies of PII within the Subscription for approximately one (1) year.

[1] Options depend on configuration of Subscription, which is set up initially during implementation, but can be changed at any time upon request of the subscriber.

F. Service Provider, Sub-Processors/Onward Transfer

iCIMS may transfer PII to companies that help us provide our service. Transfers to subsequent third parties are covered by the provisions in this policy regarding notice, choice, and the subscription agreements with our subscribers.

G. Rights of the Data Subject

If you are a European Union resident, under the General Data Protection Regulations (GDPR) you have certain rights when it comes to the personal data you submit when you apply for a job with one of our subscribers. These rights include: 1) the right to be informed; 2) the right to access your information; 3) the right to correct any information that is inaccurate; 4) the right to have your information erased; 6) the right to restrict or suppress information; 6) the right to obtain and reuse their personal data for their own purposes across different services; 7) the right to object to the processing of their personal data; 8) the right to object to how your data is used in automated decision making; and 9) lodge a complaint with the applicable supervisory authority.

If you wish to enact your rights please contact the applicable subscriber directly in accordance with their privacy practices.

If you wish to lodge a complaint with the supervisory authority, please contact that authority directly.

H. Notification of Changes

Users should contact the subscriber for more information regarding changes to a subscriber's privacy policy. Changes to the iCIMS Talent Platform Security Policy are posted on the iCIMS website at www.icims.com/gc.

2. AUTOMATED DATA COLLECTION TECHNOLOGY

A. Information Collection and Use

iCIMS may collect information about users automatically as they navigate through the Subscription.

As is true of most websites, iCIMS gathers certain information automatically. This information may include Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, the files viewed on our site (e.g., HTML pages, graphics), operating system, date/time stamp, and/or clickstream data to analyze trends in the aggregate and administer the website.

iCIMS and its partners use cookies or similar technologies to analyze trends, administer the website, track users' movements around the website, and to gather demographic information about our user base as a whole. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our website or service.

This information is used by iCIMS for a number of purposes, including authentication, preferences, and performance analytics.

The technologies iCIMS uses for this automatic data collection may include, without limitation:

- **Cookies (or browser cookies).** A cookie is a small file placed on the hard drive of the user's computer. Users may refuse cookies by activating the appropriate setting on their browser. However, if this setting is selected users may be unable to access certain parts of the Subscription. iCIMS will issue cookies when

users direct their browser to our Subscription unless the user has adjusted their browser setting so that it will refuse cookies.

- **Flash Cookies.** Certain features of the Subscription may use local stored objects (or Flash cookies) to collect and store information about user preferences and navigation to, from, and on the Subscription. Flash cookies are not managed by the same browser settings as are used for browser cookies. Users may manage Flash cookies by clicking here.
- **Web Beacons.** Pages of our Subscription and our e-mails may contain small electronic files known as web beacons (also referred to as clear gifs. pixel tags and single-pixel gifs) that permit iCIMS, for example, to count users who have visited those pages or opened an e-mail and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity). By disabling browser cookies, unique information associated with web beacons will also be disabled.
- **Third Party Cookies or Behavioral Retargeting.** iCIMS partners with third parties to display advertising on our website or to manage our advertising on other sites. Our third-party partners may use technologies such as cookies to gather information about your activities on this website and others sites in order to provide you advertising based upon your browsing activities and interests. If you wish to not have this information used for the purpose of serving you interest-based ads, you may opt-out by clicking here (or if located in the European Union click here). Please note that you will continue to receive generic ads.

B. Choice

Unless otherwise removed by the subscriber, users are given open notice of and the choice to allow for automated data collection. Users can set their browser to refuse all or some browser cookies, or to alert them when cookies are being sent. Users can learn how to manage their Flash cookie settings, by visiting the Flash player settings page on Adobe's website. If users disable or refuse cookies, some parts of the Subscription may be inaccessible or not function properly. Users who wish to prevent the collection of data by Google Analytics may use the opt-out browser add-on developed by Google for this purpose, as further described in applicable materials made publicly available by Google.

3. SECURITY MEASURES

A. Data Security

Each instance of the Subscription is password protected, and is configured to enforce SSL (128-bit encryption) to secure access. Passwords are selected using a password strength feature permitting a minimum of six (6) characters; however, the number of required characters may be configured to be greater than six (6) characters. Passwords are stored on secure database servers and can only be accessed or updated by parties having sufficient access permissions. Passwords are not sent in clear text over the Internet if the Subscription is configured to enforce SSL.

Multiple failed login attempts result in users being blocked from the Subscription[2]. To maintain the integrity of the access controls, the ability to login concurrently to the Subscription using the same username and password is disabled. Additionally, subscribers may request the hashing of sensitive data within the iCIMS platform.

[2] Number of attempts depends on configuration of Subscription.

iCIMS can enable IP locks to restrict access to the platform. iCIMS does not provide VPN to VPN, direct database, or any out-of-band access. All data access is restricted to the web-based platform itself, except for data feeds and other integration methodologies supported by iCIMS.

4. **DISCLOSURE OF INFORMATION FOR LAW ENFORCEMENT**

iCIMS may disclose PII as required by law, such as to comply with a subpoena, or similar legal or security process when we believe in good faith that disclosure is necessary to protect our rights, protect the safety of our users or others, investigate fraud, or respond to a government request.

5. **MOBILE APP DISCLOSURES**

If you download and use our Mobile Hiring Manager App (the "App"), iCIMS will automatically collect information on the type of device you use, operating system version, and the device identifier (or "UDID").

iCIMS may send you push notifications from time-to-time in order to update you about any events or promotions that iCIMS may be running. If you no longer wish to receive these types of communications, you may turn them off at the device level. To ensure you receive proper notifications, iCIMS will need to collect certain information about your device such as operating system and user identification information.

iCIMS does not ask for, access or track any location based information from your mobile device at any time while downloading or using our App.

iCIMS uses mobile analytics software to allow us to better understand the functionality of our App software on your phone. This software may record information such as how often you use the App, the events that occur within the App, aggregated usage, performance data, and where the App was downloaded from. iCIMS does not link the information iCIMS stores within the analytics software to any personally identifiable information you submit within the App.

6. **OWNERSHIP & ADMINISTRATION**

This Talent Platform Security Policy is owned and administered by the iCIMS IT department.

iCIMS may update this Talent Platform Security Policy to reflect changes to our information practices. If we make any material changes we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this website prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

To ask questions or comment about this policy and our privacy practices, contact us at: accounts@icims.com.

iCIMS, Inc.
101 Crawfords Corner Road
Suite 3-100
Holmdel, NJ 07733

7. **APPLICABILITY**

A. This Policy applies to the information gathering and dissemination practices for the Subscription and supersedes all other policies, procedures, practices, and guidelines relating to the matters set forth herein.
    a. iCIMS use reasonable efforts to ensure that all Power-Ups maintain information gathering and dissemination practices that meet industry standards for security and privacy, and such Power-Ups use reasonable efforts to protect the security and privacy of all Information received by, though, and on behalf of iCIMS. As specific practices are unique to each Power-Up and its provider, such practices may not match those set forth herein for the Subscription.