DATA SECURITY & PRIVACY STATEMENT

1. GLOSSARY OF TERMS

Term/Acronym	Definition
Anonymity	a characteristic of information that does not permit a Data Subject to be identified directly or indirectly.
Anonymization	a process by which Personal Data is irreversibly altered in such a way that a Data Subject can no longer be identified directly or indirectly, either by the Data Controller alone or in collaboration with any other party.
Anonymized Data	data that has been produced as the output of a Personal Data anonymization process.
Automated Decision-Making (ADM)	when a decision is made solely on the basis of Automated Processing.
Automated Processing	any computerized Processing of Personal Data to evaluate certain aspects relating to an individual, including analysis or predictions concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Profiling is an example of Automated Processing.
CCPA	the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.
Confidential Information	non-public information that derives independent value from not being generally known to the public, but does not include any information that (i) was or subsequently becomes publicly available without breach of any confidentiality obligations, (ii) was known prior to the disclosure of such information, (iii) was or is subsequently obtained from another source without breach of any confidentiality obligation, or (iv) is independently developed without reference to any Confidential Information and/or Personal Data.
Consent	a Data Subject's freely given, specific, and informed agreement to the Processing of their Personal Data.
Data Breach	*Please refer to the iCIMS Incident Response Policy.*
Data Controller	the person or organization that determines the purposes and means for Processing Personal Data other than natural persons who use data for personal purposes.
Data Processor	the person or organization that Processes Personal Data on behalf of and in accordance with the instructions of a Data Controller.
Data Subject	an identified or identifiable natural person to whom the Personal Data relates and whose rights are protected by applicable data protection and privacy laws, including, but not limited to, a "Consumer" as defined in the CCPA.
Dispose	the discarding or abandonment of Confidential Information and/or Personal Data; or the sale, donation, or transfer of any medium, including computer equipment, upon which this Confidential Information and/or Personal Data is stored.
GDPR	(i) the Regulation (EU) 2016/679 on the protection of natural persons with regard to Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and (ii) the UK GDPR.
ISMS	Information Security Management System, which stems from ISO/IEC: 27001:2013
Joint Controller	Data Controller that determines the purposes and means of the processing of Personal Data jointly with one or more other Data Controllers.
Need to Know Parties (NKP)	iCIMS consultants, vendors, partners, or other third parties that are provided Information by iCIMS on a need-to-know basis subject to confidentiality obligations.
Personal Data *(also known as PII)*	any information relating, directly or indirectly, to an identified or identifiable Data Subject, where such information is protected under applicable data protection or privacy law.
Personnel	iCIMS employees (part-time and full-time), interns, directors, and members.
PIMS	Privacy Information Management System, which stems from ISO/IEC: 27701:2019
Privacy Event	a situation where PII or Personal Data is potentially Processed in violation of one or more relevant iCIMS Privacy Principles.
Privacy Incident	a situation where PII or Personal Data is Processed in violation of one or more relevant iCIMS Privacy Principles.
Processing of Personal Data *(also known as Processing and Processing of PII)*	any operation or set of operations performed upon Personal Data.
Processor	a specific NKP that Processes Personnel Data with respect to iCIMS' corporate operations.
Security Event or Incident	*Please refer to the iCIMS' Incident Response Policy.*
Sensitive or Special Category Personal Data (SPD) *(also known as Sensitive PII)*	category of Personal Data, either whose nature is sensitive, such as those that relate to the Data Subject's most intimate sphere, or that might have a significant impact on the Data Subject.

Term/Acronym	Definition
Subject Access Request (SAR)	a request made by or on behalf of an individual for action on or access to their Personal Data, which they are entitled to ask for under applicable data protection and/or privacy law.
Subprocessor	a NKP third-party Data Processor engaged by iCIMS, who has or potentially will have access to or process Subscriber Data (as defined in the iCIMS Subscription Agreement), which may contain Personal Data.
Subscriber	*Please refer to the iCIMS Subscription Agreement, which may be found at www.icims.com/gc.*
Subscriber Data	*Please refer to the iCIMS Subscription Agreement, which may be found at www.icims.com/gc.*
Subscription	*Please refer to the iCIMS Subscription Agreement, which may be found at www.icims.com/gc.*
UK GDPR	the EU GDPR as amended and incorporated into United Kingdom ("UK") law under the UK European Union (Withdrawal) Act 2018, if in force.

2. Overview and Background

iCIMS, Inc. and its subsidiaries (collectively, "iCIMS") recognizes the importance of protecting and ensuring the integrity of Subscriber's Confidential Information and Personal Data, including SPD. Subscribers' Confidential Information and Personal Data are gathered, used, stored, shared, secured, retained, and disposed of in accordance with applicable laws and regulations, privacy best practices, and the terms of the agreement between iCIMS and the Subscriber.

This Data Security & Privacy Statement ("Statement") explains how we process, gather, use, store, share, secure, retain, and dispose of Confidential Information and Personal Data on behalf of our subscribers' and their users. To this end, iCIMS has adopted this statement to secure and limit unauthorized disclosure of subscribers' Confidential Information and/or Personal Data.

EU-U.S. and Swiss-U.S. Privacy Shield

iCIMS complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks ("Privacy Shield Frameworks") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Economic Area, the UK, and Switzerland to the United States. iCIMS has self-certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

Compliance with Applicable Data Protection and Privacy Law

iCIMS complies with applicable data protection and privacy laws and regulations, including the EU GDPR, the UK GDPR, and the CCPA, by and through its information security and privacy information management systems that comply with internationally recognized standards (ISO/IEC 27001 and 27701), as well as other technical and organizational measures, including the Privacy Shield Frameworks and standard contractual clauses, as applicable, regarding the legal safeguards required to protect Personal Data.

3. Types of Information Processed

iCIMS processes Subscriber Data, which may include Confidential Information and/or Personal Data, on behalf of its subscribers, which generally includes the following categories of information:

- Data submitted in résumés, CVs, letters, writing samples, or other written materials necessary for evaluation of employment.
- Data generated by interviewers and recruiters based on interactions with candidates.
- Data generated through Internet searches or publicly available information.
- Recommendations provided on a candidate's behalf by others.
- Data about a candidate's previous employment, education, and where applicable, credit history, criminal records, or other information revealed during a background check.

- Data about any disabilities that are relevant to a workplace accommodation.
- Data about race, ethnicity, religion, disability, gender and self-identified LGBT status, for the purposes of government reporting where required, as well as to understand the diversity characteristics of applicants.

To this end, iCIMS recognizes that Processing Personal Data varies by country, and we adhere to the below data protection principles based upon our Subscribers' user's country of residence, the agreement between the Subscriber and iCIMS, and the Subscriber's requirements.

3.1. Personal Data

iCIMS Processes Personal Data on behalf of its subscribers. Depending on the subscribers' instructions and settings, Personal Data may include the following data categories: internal data; external data; financial data; social data; historical data; and tracking data.

Examples of Types of Personal Data

Internal Data	External Data	Financial Data	Social Data	Historical Data	Tracking Data
○ Religious or Philosophical Beliefs ○ Passwords ○ PINs ○ Mother's Maiden Name ○ Opinions ○ Intentions ○ Interests ○ Likes/Dislikes	○ Name ○ Username ○ Unique Identifier ○ Gov't Issued Identification ○ Picture ○ Biometric Data ○ Ethnicity/Race ○ Spoken Language ○ Sex Life or Orientation ○ Browsing Behavior ○ Call Logs ○ Links Clicked ○ Demeanor/ Attitude ○ Demographic Information ○ Medical or Health Information ○ Physical Characteristics	○ Credit Card Number ○ Bank Account Number ○ Automobile Ownership ○ Home Ownership ○ Apartment Rentals ○ Personal Possessions ○ Credit Report ○ Sales and Purchases ○ Loan Records ○ Spending Habits ○ Taxes ○ Credit Worthiness ○ Credit Score ○ Credit Capacity	○ Job Titles ○ Work History ○ School Attended ○ Employee Records ○ Employment History ○ Evaluations ○ References ○ Interviews ○ Certifications ○ Disciplinary Actions	○ Information about an individual's personal history (e.g., whether they were part of 9/11, WWI, WWII)	○ IP Address ○ MAC Address ○ Browser Fingerprint ○ Email Address ○ Physical Address ○ Telephone Number ○ Country ○ GPS coordinates ○ Electronic Room Number

4. How We Process Confidential Information and Personal Data

Personnel and NKPs shall only use Confidential Information and Personal Data for a legitimate business purpose in the performance of their duties, including (without limitation):

- To provide and improve the Subscription to subscribers and their users or as otherwise permitted by a Subscriber in its agreement with iCIMS; and
- To support iCIMS' quality, security, and customer experience improvement initiatives.

4.1. PROCESSING OF PERSONAL DATA

iCIMS recognizes the importance of Processing Personal Data, and values the lawful, accurate, and secure Processing of Personal Data. Therefore, to assist its Subscribers in complying with applicable laws and regulations, iCIMS' Subscription is enabled to Process Personal Data on behalf of its subscribers and in accordance with the following data protection principles:

1. Personal Data is obtained and Processed fairly and lawfully and shall not be Processed unless the Processing is necessary for the purposes defined under applicable data protection and privacy laws and regulations.
2. Personal Data is obtained for one or more lawful purposes and not Processed in a manner incompatible with those purposes.
3. Personal Data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are Processed.
4. Personal Data is accurate and kept up to date.
5. Personal Data should not be kept for longer than is necessary for that purpose.
6. Personal Data shall be Processed in accordance with the rights of the Data Subject.

These data protection principles must be followed at all times when Processing or using Personal Data. Through appropriate management and strict application of criteria and controls, iCIMS enables subscribers, by and through the iCIMS Subscription, to:

1. Observe the fair collection and use of Personal Data by collecting consent or providing notice about the legitimate grounds for Processing Personal Data.
2. Deliver notification of how Personal Data is Processed at the time it is collected from a Data Subject.
3. Provide notification to a Data Subject, explaining the details required to Process their Personal Data.
4. Not Process Personal Data using ADM.
5. Ensure that Data Subject rights can be fully exercised under applicable data protection and privacy laws and regulations.
6. Process Personal Data to fulfill only business and operational requirements.
7. Be informed if a Subscriber, in iCIMS' opinion, provides a Processing instruction that infringes applicable data protection and privacy laws and/or regulations.
8. Inform a Data Subject if their Personal Data is to be used in a new way.
9. Ensure that sharing of Personal Data with third parties is subject to formal information sharing protocols and agreements.
10. Transfer Personal Data to Processors and Subprocessors only under circumstances where the Personal Data is adequately protected, the use of such Processors and Subprocessors has been disclosed to Subscriber, and the engagement of such Processors and Subprocessors is in accordance with the agreement between iCIMS and Subscriber, including any changes to such Processors and Subprocessors and the Subscriber's right to object to such changes.
11. Document all requests and disclosures of Personal Data.
12. Disclose Personal Data for a stated purpose.
13. Maintain the necessary records in support of demonstrating compliance with iCIMS' obligations for the Processing of Personal Data carried out on behalf of a Subscriber.
14. Provide subscribers with the appropriate information such that subscribers can demonstrate compliance with their obligations.

15. Provide notification to a Subscriber when iCIMS receives a legally binding request for access to or disclosure of the Subscriber's Personal Data (unless prohibited by applicable laws and regulations) and will: (a) attempt to oppose and/or narrow such request; (b) consult with the Subscriber before making any Personal Data disclosures pursuant to such request; and (c) reject such request if it is not legally binding.

Lastly, where iCIMS processes Personal Data on behalf of its subscribers, iCIMS serves as a Service Provider as defined in CCPA Section 1798.140(v). Under those same circumstances, iCIMS' subscribers are considered to be a Business as defined in CCPA Section 1798.140(c). Under no circumstances envisioned in the Subscription Agreement is either party considered to be a Third Party as defined in CCPA Section 1798.140(w).

As such, subscribers disclose Personal Data to iCIMS solely for: (i) a valid business purpose; and (ii) iCIMS to provide the Subscription. Except as agreed upon in writing by iCIMS and each Subscriber, iCIMS is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Subscription; and (iii) retaining, using, or disclosing the Personal Data outside of the Subscription Agreement between iCIMS and Subscriber.

4.1.1. Data Subject Rights

Under the applicable data protection and privacy laws and regulations, a Data Subject may request details about his/her Personal Data which iCIMS Processes on behalf of a Subscriber. These rights may include, for example, the right to be informed that processing is being undertaken, to access one's Personal Data, to prevent Processing in certain circumstances, or to correct, rectify, block, or erase one's Personal Data.

iCIMS' Subscription enables subscribers to fulfill their own Subject Access Requests. Within the Subscription, iCIMS has also implemented appropriate technical and organizational measures, insofar as this is possible, so that subscribers may fulfill their obligations to respond to SARs. In addition, when necessary, iCIMS provides subscribers with reasonable assistance to fulfil SARs in accordance with the terms of the agreement between iCIMS and the Subscriber. Should iCIMS received a SAR outside of the Subscription that names a Subscriber, iCIMS will redirect the Data Subject to the Subscriber and promptly forward the SAR to the Subscriber.

4.2. Privacy By Design & Default

iCIMS embeds privacy considerations into business processes and systems through appropriate physical, technological, and procedural controls reasonably designed to ensure Personal Data is Processed and secured in accordance with applicable data protection and privacy laws and regulations. Through its security policies and procedures, iCIMS implements various information security measures, including that it only processes the minimal amount of Confidential Information and/or Personal Data necessary for a specific purpose, ensuring that unauthorized access or disclosure of Confidential Information and/or Personal Data does not happen by accident or design.

5. Safeguarding of Confidential Information and Personal Data

In addition to processing Personal Data in accordance with the principles provided for in the Section titled, "PROCESSING OF PERSONAL DATA," iCIMS implements the following physical,

procedural, and information security safeguards to protect all subscribers' Confidential Information and/or Personal Data:

1. iCIMS configures its outgoing email transmissions to include the General Counsel's Office approved unintended recipient confidentiality language.
2. iCIMS implements physical measures to prevent unauthorized entry to our premises and secured areas, as well as unauthorized access to our Confidential Information and/or Personal Data.
3. iCIMS uses an access control system to restrict and monitor the iCIMS' premise and secured areas.
4. iCIMS uses reasonable efforts to ensure all visitors are authorized before entering the iCIMS premises and areas where Confidential Information and/or Personal Data is processed or maintained, including, but not limited to, taking the following actions as appropriate:
    a. Providing visitors a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-Personnel;
    b. Asking visitors to surrender the physical token before leaving the facility or at the date of expiration;
    c. Documenting procedures to help all Personnel easily distinguish between Personnel and visitors, especially in areas where Personal Data is accessible.
5. iCIMS uses reasonable efforts to maintain a physical audit trail of visitor activity, including, but not limited to, documenting the visitor's name, the firm represented, and Personnel authorizing physical access on the log. Logs should be kept for a minimum of three months unless otherwise required by law.
6. iCIMS restricts and monitors access to areas containing sensitive material and stored items, including personal records, financial records, office supplies, and computer equipment.
7. iCIMS and its Personnel implements and maintains security, information gathering, and dissemination practices on its IT systems, including network, equipment, and communication systems supporting iCIMS' internal and remote operations and iCIMS-hosted products and services, including, but not limited to, encryption, virus protection, access controls, firewall egress and ingress, and LAN/WAN security. *See* IT Security Policy for further details.

6. RESPONSIBILITIES OF PERSONNEL

iCIMS strictly prohibits unauthorized disclosure of Confidential Information and Personal Data. Personnel, Processors, and Subprocessors should not disclose Confidential Information and Personal Data obtained in the course of their work with iCIMS, or access Confidential Information and Personal Data without appropriate permissions. The agreement between iCIMS and the Subscriber dictates how Subscriber Data are obtained and/or disclosed.

Personnel shall use reasonable efforts to safeguard Confidential Information and Personal Data and keep it private and confidential, including, but not limited to, taking the following actions as appropriate:

1. Only sharing Information with authorized Personnel and NKP who "need to know" such Information for a legitimate business purpose in the performance of their authorized duties;

2. Only storing all electronic Confidential Information and Personal Data in secured equipment or devices (e.g., using a unique password or biometric security measure for Windows login, Outlook login, and/or directory or file access);
3. Only storing paper Confidential Information and Personal Data in a locked drawer or office (i.e., not leaving documents lying openly on desks);
4. Not sharing unique passwords and updating existing passwords on a periodic basis;
5. Properly labeling and/or segregating Confidential Information and Personal Data belonging to one party from information belonging to another party;
6. Not storing any Personal Data on any laptop or portable device unless it has been confirmed that such Personal Data is encrypted on such equipment or device;
7. Not transmitting any Personal Data from a non-iCIMS mail server (e.g., personal Gmail, Yahoo!, or Hotmail account);
8. Not leaving any unsecured Confidential Information and/or Personal Data, or unsecured equipment or devices containing Confidential Information and/or Personal Data unattended or in an unsecured area; and
9. Using reasonable efforts to Dispose of Confidential Information and/or Personal Data when such Information is no longer needed, and shall obtain the return of Confidential Information and/or Personal Data from an NKP when it no longer needs such Information or it is no longer an authorized NKP.

If Personnel encounter information, documents, or other materials, whether disclosed in writing or orally, for which there is some doubt as to whether it should be treated as Confidential Information or Personal Data, or how it can be disclosed or used he or she shall:

a. Treat such information, documents, or materials as Confidential Information and/or Personal Data as provided herein; and/or
b. Contact the iCIMS Privacy team, who shall make a joint determination on how best to proceed.

7. Return, Transfer, or Disposal of Information

1. All Confidential Information and/or Personal Data must be returned, transferred, or Disposed of in accordance with applicable laws and regulations, the agreement between the Subscriber and iCIMS, and iCIMS' policies and procedures that control the Disposal of Confidential Information and/or Personal Data. iCIMS will take reasonable measures to ensure that such Disposal is performed in a secure manner and includes temporary files created as a result of the Processing of Personal Data.
2. When Disposing of Subscriber Data, Personnel and NKPs shall take reasonable measures to protect against unauthorized access to or use of the information in connection with its Disposal. Examples of such reasonable measures include, but are not limited to, any of the following:
    a. Burning, pulverizing, or shredding of papers or records containing Information so that the Information cannot be practicably read or reconstructed;
    b. Destroying or erasing electronic media containing Information so that the Information cannot practicably be read or reconstructed, consistent with reasonable standards.
3. iCIMS will provide further details about its internal Document Retention Policy to its Subscribers upon written request.

8. Accountability and Liability

1. On a quarterly basis, iCIMS conducts privacy reviews on new or emerging applicable laws to proactively identify potential privacy risks and to ensure proper tracking and resolution of any applicable data protection and privacy law or regulatory issues.
2. Additionally, on an annual basis, iCIMS conducts an ISMS audit to determine whether the control objectives, controls, processes, and procedures of the ISMS conform to the requirements of ISO 27001: 2013, relevant legislation and/or regulations, and identified information security requirements. The internal audit will ensure that ISMS control objectives, controls, processes and procedures are implemented, maintained effectively, and perform as expected.
3. The iCIMS General Counsel's Office ("GCO") shall monitor compliance with this Statement through periodic audits of iCIMS, its Personnel, and NKPs.
4. Any Personnel or NKPs who violate any provision of this Statement may be subject to disciplinary action, up to and including immediate termination of their employment or contractual relationship (as applicable), as is determined appropriate in management's discretion.
5. In accordance with the Privacy Shield Principles, iCIMS has named independent recourse mechanisms for investigation of an individual's complaints and disputes. For specifics, please click here.

9. Data Backup and Disaster Recovery

iCIMS, through its Support & Maintenance Policy conducts a Backup at least daily and prior to any Update to the Subscription. iCIMS maintains daily Backups onsite and moves one of the daily Backups to an off-site storage facility. iCIMS also maintains an Incident Response Policy and Procedure that ensures a consistent and effective approach to the management of Security and/or Privacy Events or Incidents, including a Data Breach.

10. Services Privacy Notice

For more information on iCIMS' privacy practices with respect to the collection, use, and disclosure of Personal Data obtained in connection with the use of our Subscription, please see its Services Privacy Notice. It also describes iCIMS' privacy practices with respect to Personal Data processed by iCIMS for Subscriber account, contract, and billing management purposes.

11. Contact Information

To contact iCIMS' Data Protection Officer, please email privacy@icims.com or write to iCIMS, Inc., Attn: Privacy, Legal Department, 101 Crawfords Corner Road, Suite 3-100, Holmdel, NJ 07733 USA.