



**Monterey County Department of Social Services  
Renewal Order Form**

**CONTACT INFORMATION**

<b>Sold To Company:</b>	Monterey County Department of Social Services	<b>Sales Representative:</b>	Jacquelyn Gourley
<b>Bill To Address:</b>	1000 South Main Street, Suite #306 Salinas, California 93901	<b>Sold To Address:</b>	1000 South Main Street, Suite #306 Salinas, California 93901
<b>Bill To Contact:</b>	Marcie Castro	<b>Primary Contact:</b>	Marcie Castro
<b>Bill To Email:</b>	501- mcdssaccountspayable@countyofmonterey.gov	<b>Primary Contact Email:</b>	castrom@countyofmonterey.gov
<b>Bill To Phone:</b>		<b>Primary Contact Phone:</b>	(831) 755-3480

**SUBSCRIPTION DETAILS**

<b>Subscription Period:</b> 36 Months	<b>Total Subscription Fees:</b> USD 52,491.60
<b>Subscription Start Date:</b> January 01, 2025	<b>Currency:</b> USD
<b>Subscription End Date:</b> December 31, 2027	
<b>Effective Date:</b> Last Date of Signature	

**RECURRING PRODUCT SUBSCRIPTIONS**

Other Products			
Name	Description	Employees	Quantity
SkillSurvey Reference	Automated reference checking with job-specific surveys and predictive analytics. Subscriber's use of this product is governed by the SkillSurvey Addendum available at <a href="http://www.icims.com/gc">www.icims.com/gc</a> as of the date hereof, which is incorporated into the Subscription Agreement.	900	1

**Total Contract Value:** USD 52,491.60

**ADDITIONAL SERVICES INCLUDED AT NO ADDITIONAL INVESTMENT**

<b>iCIMS SUPPORT SERVICES</b>	Digital chat and case support for designated System Administrators through the iCIMS Community, as further detailed in our Support & Maintenance Policy available at <a href="http://www.icims.com/gc">www.icims.com/gc</a> .	INCLUDED
<b>iCIMS TRAINING PACKAGE</b>	Access to eLearnings, New Release Trainings, and Knowledge-Base Resources through the iCIMS Community	INCLUDED
<b>SUBSCRIPTION UPDATES</b>	Ongoing Updates to the Subscription as further detailed in iCIMS' Support & Maintenance Policy available at <a href="http://www.icims.com/gc">www.icims.com/gc</a> . No additional fees apply to new iCIMS Platform versions.	INCLUDED

To view a list of iCIMS' standard iForms, please click here: [iCIMS iForms Library](#)

**SUMMARY OF SUBSCRIPTION FEES**

Start Date	End Date	Amount	Billing Frequency	Payment Terms
January 1, 2025	December 31, 2025	USD 17,497.20	Annual	Net 30
January 1, 2026	December 31, 2026	USD 17,497.20	Annual	Net 30
January 1, 2027	December 31, 2027	USD 17,497.20	Annual	Net 30

All recurring Subscription fees shall begin on the Subscription Start Date, are invoiced in advance per the Billing Frequency as set forth above and are payable in accordance with the Net Payment Terms above.

**ADDITIONAL CONTRACT TERMS**





Prices are good through December 23, 2024.

All fees for the implementation of the subscriptions listed in the Recurring Subscription Section (and any Training Fees noted above) are included in the One-Time Fees listed herein, exclusive of any change requests or if specifically noted otherwise. Any additional implementation services or professional services will only be performed in the case of a separate Order Form between the parties.

**SIGNATURES**

The parties by their authorized representatives execute this Order Form and make it a part of the Subscription Agreement between the parties, the terms of which are attached hereto as of the date hereof. By remitting this signed Order Form back to iCIMS, Subscriber acknowledges that it has read and understood the Subscription Agreement and agrees to be bound by the terms and conditions set forth therein. Further, each party warrants that its respective signatory whose signature appears below is duly authorized by all necessary and appropriate corporate action to execute the Order Form and the Subscription Agreement on behalf of such party effective as of the effective date above.

**iCIMS, Inc.**

**Subscriber: Monterey County Department of Social Services**

**Signature:**   
Signed by:  
87D511B83FE440F...

**Signature:**

**Name:** Michael Pastore

**Name:**

**Title:** VP, Sales Operations


**Title:**

**Date:** 11/4/2024 | 1:55:37 PM EST

**Date:**

**GCO Initial:** 

**Date:** 11/4/2024 | 1:46:10 PM EST

**DocuSigned by:**  
  
A46091E5DE63489...

**Deputy County Counsel**

11/7/2024 | 10:34 AM PST





## SUBSCRIPTION AGREEMENT

**PLEASE READ THIS SUBSCRIPTION AGREEMENT CAREFULLY. BY SIGNING AN ORDER FORM REFERENCING THIS SUBSCRIPTION AGREEMENT, CLICKING ON THE "I AGREE" BUTTON, OR USING PRODUCTS OR SERVICES DESCRIBED IN THE SUBSCRIPTION AGREEMENT, YOU ARE ACCEPTING AND AGREEING TO BE LEGALLY BOUND BY THE TERMS AND CONDITIONS IN THIS SUBSCRIPTION AGREEMENT.**

iCIMS, Inc. ("iCIMS") and the subscriber identified in the applicable Order Form ("**Subscriber**") enter into and agree to be bound by this Subscription Agreement (the "**Agreement**").

### 1. DEFINITIONS

The capitalized terms below shall have the following meanings for purposes of this Agreement:

- 1.1 "**Affiliate**" of a Party means an entity that directly or indirectly controls, is controlled by, or is under common control with that Party, in each case through majority voting power.
- 1.2 "**Candidate**" means any person who directly or indirectly enters into the Subscription, a job application or other information related to a job or job opportunity with Subscriber or its Affiliate.
- 1.3 "**Data Processing Addendum**" means the Data Processing Addendum that may be accessed through <https://www.icims.com/gc>, a copy of which as it exists on the commencement of the Term is attached hereto as Exhibit A.
- 1.4 "**Documentation**" means the product functionality descriptions and release notes that may be accessed at <https://care.icims.com/s/>.
- 1.5 "**iCIMS Content**" means the forms, content samples, reports, and other support and informational materials provided by iCIMS for use in connection with the Subscription, as may be modified from time to time by iCIMS, excluding any Documentation.
- 1.6 "**Order Form**" means an order form signed by Subscriber and iCIMS and expressly designated as an "Order Form," including the first Order Form and any renewal or other Order Form.
- 1.7 "**Party**" means iCIMS or Subscriber, and collectively, the "Parties".
- 1.8 "**Subscription**" means the iCIMS-hosted software components set forth in an Order Form.
- 1.9 "**Subscriber Data**" as used in this Agreement means the electronic data and files entered, imported, uploaded or transferred into the Subscription by Subscriber, its Affiliate, a User, or a Candidate, excluding any iCIMS Content.
- 1.10 "**Subscriber Data Security Addendum**" means the Subscriber Data Security Addendum that may be accessed through <https://www.icims.com/gc>, a copy of which as it exists on the commencement of the Term is attached hereto as Exhibit B.
- 1.11 "**Support & Maintenance Policy**" means the Support & Maintenance Policy that may be accessed at <https://www.icims.com/gc>, a copy of which as it exists on the commencement of the Term is attached hereto as Exhibit C.
- 1.12 "**User**" means Subscriber's or its Affiliate's employee, contractor or agent authorized by Subscriber or its Affiliate to use the Subscription.

### 2. SUBSCRIPTION AND OTHER PRODUCTS AND SERVICES

2.1 **Subscription and iCIMS Content.** Subject to the terms and conditions set forth in this Agreement, Subscriber may use the Subscription solely for Subscriber's and its Affiliate's own pre-employment and employment purposes, and use the Documentation and iCIMS Content solely to support use of the Subscription under this Agreement. Subscriber may allow its Affiliates and Users to use the Subscription, Documentation and iCIMS Content subject to the same terms and conditions of this Agreement as

are applicable to use by Subscriber. Subscriber shall remain fully responsible and liable for the acts and omissions of its Affiliates and Users.

2.2 **iCIMS Services.** iCIMS shall host, support and maintain the Subscription in accordance with the Support & Maintenance Policy. Updates as defined in the Support & Maintenance Policy are deemed part of the Subscription. iCIMS also shall deliver the implementation, training, consulting and other services set forth in an applicable Order Form.

2.3 **Third-Party Products and Services.** Subscriber may use, or iCIMS may enable or allow access to products, services and web sites provided by other persons or entities, including the products and services available through the iCIMS' Marketplace and other third-party web sites, products and services (each, a "**Third-Party Product**"). Subscriber is solely responsible for entering into and complying with any contractual agreement or other terms and conditions that are required by the provider of any Third-Party Product. iCIMS does not make any representation regarding any Third-Party Product. iCIMS shall have no obligation or liability relating to any Third-Party Product. Except as expressly set forth in an addendum to this Agreement, iCIMS' sole responsibility for any integration or other link or connection to a Third-Party Product identified in an Order Form is to make the Subscription available to receive and send data between the Subscription and the Third-Party Product in accordance with the Documentation, subject to the usage and other limitations set forth in an Order Form, the Documentation, or an addendum to this Agreement.

### 3. SUBSCRIBER RESPONSIBILITIES

3.1 **Equipment and Resources.** Subscriber is solely responsible for any travel, accommodations, computer equipment, telecommunications, and expenses required for Subscriber or its Users to access or use the Subscription.

3.2 **Configuration and Use.** Subscriber may not allow any person or entity to use or access the Subscription, Documentation, or iCIMS Content except its Affiliates, Users, and Candidates. Use of the Subscription, Documentation, and iCIMS Content under this Agreement is limited to authorized Users only, and other limitations set forth in the applicable Order Form or Documentation. Subscriber and its Affiliates and Users shall comply with iCIMS' Acceptable Use Policy that may be accessed at <https://www.icims.com/gc>, and shall not authorize its Candidates to violate the Acceptable Use Policy, a copy of which as it exists on the commencement of the Term is attached hereto as Exhibit D. Subscriber is solely responsible for any configuration of the Subscription and any electronic forms, materials, communications, content and processes selected by Subscriber or its Affiliate or User for use in or in connection with the Subscription. Subscriber acknowledges and agrees that any output, recommendation, suggestion, explanation, or analysis provided by the Subscription is for informational purposes only. Subscriber is solely responsible for any use of the Subscription by Subscriber or its Affiliate or User, including any recruiting, hiring or employment-related process, action or decision, and shall ensure that any process, action or decision does not violate any law or regulation. Subject to iCIMS' compliance with Section 4 of this Agreement, Subscriber is solely responsible for and shall ensure that use or disclosure of any Subscriber Data in accordance with this Agreement complies with applicable laws and regulations, including any required notices or consents.

3.3 **Certification.** Upon reasonable belief that Subscriber has violated this Agreement, with prior written notice from iCIMS, Subscriber shall provide to iCIMS or its representatives access to any information reasonably





necessary for iCIMS to verify Subscriber's compliance with the applicable provisions of this Agreement

#### 4. SUBSCRIBER DATA

4.1 **Data Protection.** iCIMS shall maintain administrative, physical and technical safeguards intended to protect the security, privacy and integrity of Subscriber Data as set forth in the Data Processing Addendum and Subscriber Data Security Addendum. iCIMS may update the Subscriber Data Security Addendum from time to time in accordance with Section 13.8, provided however iCIMS shall not make changes to the Subscriber Data Security Addendum that materially diminish the protections for Subscriber Data set forth therein. iCIMS in its discretion also may maintain supplemental or additional safeguards.

4.2 **Data Use and Disclosure.** iCIMS and its Affiliates may use Subscriber Data only for the purpose of providing the Subscription and related services under this Agreement or as otherwise set forth in this Agreement. iCIMS may disclose Subscriber Data to its contractor under a written agreement requiring the contractor to use and disclose the Subscriber Data only for the purposes permitted under this Agreement, and subject to the Subscriber Data Security Addendum. iCIMS also may disclose Subscriber Data to Subscriber's and its Affiliate's contractors, providers of Third-Party Products, and other third parties, only for purposes of providing the Subscription or as otherwise directed or permitted by Subscriber or its Affiliate or User. Notwithstanding anything to the contrary in this Agreement:

(a) iCIMS may use and disclose Subscriber Data as reasonably necessary to comply with applicable laws and regulations, cooperate with law enforcement agencies, or attempt to prevent or respond to illegal conduct, fraud, abuse, or a threat to the security or integrity of systems or data including the Subscription or Subscriber Data.

(b) iCIMS may derive or create benchmarking, transactional, or performance information, and other forms of statistics or analytics on an aggregated basis that may not reasonably be used on its own to distinguish or trace the identity of a Subscriber or its Affiliate, User, or Candidate (collectively, "**Analytics**"). iCIMS shall maintain policies and procedures, which may include de-identification, aggregation or other steps, reasonably necessary to prevent Analytics from including information that may be used on its own to distinguish or trace the identity of a Subscriber or its Affiliate, User, or Candidate.

(c) Nothing in this Agreement prohibits iCIMS from using Subscriber Data or the same or similar information that: (i) is or becomes publicly available except through violation of this Agreement by iCIMS; (ii) is or was received by iCIMS from a third party that to iCIMS' knowledge is not under a confidentiality obligation with respect to the Subscriber Data; or (iii) is or was previously known to or independently developed by iCIMS without use of the Subscriber Data.

4.3 **Data Access and Storage.** During the Subscription Period set forth in an applicable Order Form, Subscriber may access and download the Subscriber Data in accordance with the Documentation, and iCIMS will provide backups of Subscriber Data if requested and as further agreed by the Parties in writing, including payment of fees for data backups. Backups will be transferred to a secure ftp site or Subscriber hosted ftp site in .csv format, as determined by iCIMS, or in such other manner as is agreed by the Parties. In addition, upon written request by Subscriber no more than ten (10) days following the expiration or termination of this Agreement and payment of all outstanding amounts due under the Agreement, iCIMS shall promptly deliver a copy of the Subscriber Data in a file to an iCIMS secure ftp site or Subscriber-hosted ftp site in .csv format, as determined by iCIMS. iCIMS shall dispose of the Subscriber Data in accordance with the Data Processing Addendum and Subscriber Data Security Addendum.

#### 5. PAYMENT

5.1 **Fees and Expenses.** Upon signing an Order Form, Subscriber shall pay the total one-time fees set forth in such Order Form. Unless otherwise set forth in the applicable Order Form, iCIMS will invoice recurring fees in advance, on an annual basis, payable within thirty (30) days of delivery of an invoice. Except as otherwise provided herein, all fees paid under this Agreement are non-refundable.

5.2 **Taxes and Surcharges.** Subscriber shall be solely responsible for paying any sales, value-added, business use or other similar taxes, third-party fees, charges, or surcharges, relating to, imposed on, or associated with Subscriber's use of the Subscription or any other product or service provided by iCIMS (collectively, "**Taxes**"), exclusive of iCIMS' income taxes. The fees listed in an Order Form are exclusive of Taxes, and iCIMS shall have the right to invoice Taxes together with or separately from the fees payable by Subscriber. Notwithstanding the foregoing, if Subscriber provides iCIMS with a certificate regarding the tax status of Subscriber certifying that Subscriber has received a ruling or determination letter(s) from the relevant tax authorities stating that it qualifies as an organization exempt from state and local sales and similar taxes, then Subscriber shall not be required to pay to or reimburse iCIMS for such taxes for so long as Subscriber maintains such qualification.

5.3 **Purchase Orders.** Any terms or conditions in any purchase order, online payment or vendor portal, or other document issued by Subscriber are void and of no force or effect as between Subscriber and iCIMS. Issuance of a purchase order or other document is not a condition of Subscriber's payment obligations.

5.4 **Overdue Payments.** iCIMS may suspend access and use of the Subscription by Subscriber and its Affiliates and Users, if Subscriber fails to make timely payment within fifteen (15) days of iCIMS providing written notice of late payment.

5.5 **Invoice Disputes.** Any invoice must be disputed prior to when it is due. If within that period Subscriber delivers written notice disputing an invoiced amount and describing the basis for dispute with reasonable particularity, the Parties shall make a good faith effort to confer and resolve the dispute within thirty (30) days of delivery of Subscriber's notice. If Subscriber has paid all undisputed amounts, and engages in good faith negotiations, iCIMS' rights under this Agreement to assess overdue payment charges, suspend access to the Subscription, and terminate the Agreement for material breach based on non-payment of the disputed payment, shall be suspended during that thirty (30) day period.

#### 6. TERM AND TERMINATION

6.1 **Subscription Period.** The Subscription Period under each Order Form begins on the Subscription Start Date (as defined in the applicable Order Form) and ends upon the expiration of the Subscription Period as set forth in the applicable Order Form. Except as otherwise specified in an Order Form, upon expiration of the Subscription Period under an Order Form, Subscriber's right to access and use the Subscription pursuant to that Order Form expires. iCIMS may require the Subscription Period under any subsequent Order Form to end on the same date as the Subscription Period under the first Order Form (or subsequent renewal), so that all Subscription Periods share the same expiration date, and in such event iCIMS will prorate the fees for the Subscription Period of each Order Form accordingly.

6.2 **Term.** The term of this Agreement (the "**Term**") commences on the last date of signature of the first Order Form and shall remain in effect until the Subscription Periods on all Order Forms have expired or the date of termination of this Agreement under its terms, whichever is earlier.

6.3 **Termination for Cause.**





(a) Either Party (the “**Non-Breaching Party**”) may terminate this Agreement upon written notice to the other Party (the “**Breaching Party**”) if the Breaching Party does not cure its material breach of the Agreement within thirty (30) days of written notice from the Non-Breaching Party stating its intent to terminate and describing the breach with reasonable particularity. Nonpayment by Subscriber of any amount within thirty (30) days of the due date constitutes material breach, subject to the overdue payment resolution procedures set forth in Section 5.5 above. Reference to the unpaid amount and invoice constitutes sufficiently reasonable particularity for the notice of breach.

(b) iCIMS may terminate this Agreement upon written notice in the event of filing of a petition in bankruptcy of Subscriber, or commencement of a receivership or similar proceeding based on the insolvency of Subscriber.

(c) Termination by iCIMS for material breach will not relieve Subscriber of its obligation to pay all fees that would have otherwise been due had the Agreement not been terminated for breach, and all such fees shall become immediately due.

**6.4 Effect of Termination.** Upon termination or expiration of this Agreement, all rights and licenses granted by a Party under the Agreement immediately terminate, and Subscriber and its Affiliates and Users shall immediately cease use of the Subscription, Documentation, and iCIMS Content. Termination by either Party will not relieve Subscriber of any obligation to pay fees due for periods prior to termination. iCIMS may provide post-termination or expiration assistance services as further agreed by the Parties in writing, including the fees payable for such assistance. Notwithstanding this Section 6.4, iCIMS may continue to use the Subscriber IP (as defined below) to satisfy its post-termination or expiration obligations or as otherwise set forth in this Agreement or the Data Processing Addendum and Subscriber Data Security Addendum. Sections 6.4, 8.1, 8.2, 10, 11 and the provisions of Section 13 that by their terms naturally survive shall survive expiration or termination of the Agreement. The Receiving Party’s obligations under Section 7 of this Agreement with respect to Confidential Information received during the Term shall survive: (i) with respect to Confidential Information that constitutes a trade secret of the Disclosing Party, as long as that Confidential Information remains a trade secret; and (ii) with respect to all other Confidential Information, for a period of five (5) years after the expiration or termination of the Agreement.

## 7. CONFIDENTIAL INFORMATION

**7.1 Confidential Information Defined.** “**Confidential Information**” as used in this Agreement means any information that during the Term is disclosed by or on behalf of a Party or its Affiliate (the “**Disclosing Party**”) to the other Party or its Affiliate (the “**Receiving Party**”) and at the time of disclosure: (i) is designated in writing as confidential or proprietary; (ii) is designated orally as confidential or proprietary, and embodied by the Disclosing Party in written or other tangible form, including meeting minutes, memos, diagrams, flow charts, and software; or (iii) should reasonably be understood by the Receiving Party to be confidential to the Disclosing Party under the circumstances. Notwithstanding the absence of any designation of confidentiality, the Parties agree that: (a) any Order Form, non-public Documentation, iCIMS Content, specifications regarding the Subscription or its functionality, and Analytics are the Confidential Information of iCIMS; and (b) without limiting any of the rights in Section 4.2, any Subscriber Data is the Confidential Information of Subscriber, subject to the exceptions in Section 7.3 below.

**7.2 Obligations.** Except as approved by the Disclosing Party in writing, the Receiving Party shall not: (i) use the Confidential Information of the Disclosing Party except to perform or exercise its rights and obligations under this Agreement; or (ii) disclose the Confidential Information of the Disclosing Party to any third party except to the Receiving Party’s Affiliates, contractors,

agents, or corporate directors or officers (each, a “**Representative**”) who are under a duty in substance and effect to use and disclose the Confidential Information only as permitted under this Agreement. The Receiving Party shall be responsible for any use by its Representative of the Confidential Information it discloses to its Representative. Upon termination of the Agreement, each Party shall cease use of, and within thirty (30) days of termination shall destroy or return, all Confidential Information of the other Party, except that: (a) iCIMS may retain Confidential Information of Subscriber as needed to comply with any post-expiration or termination obligation under this Agreement; and (b) each Party may retain Confidential Information as required to comply with its obligations under applicable laws, regulations, or record retention policies.

**7.3 Exceptions.** Confidential Information does not include any: (i) information which is or becomes publicly available except through any act or omission of the Receiving Party in violation of a duty to the Disclosing Party; (ii) information received by the Receiving Party from a third party that to the Receiving Party’s knowledge is not under a confidentiality obligation with respect to the Confidential Information; or (iii) information previously known to or independently developed by the Receiving Party without use of the Disclosing Party’s Confidential Information. The Receiving Party may disclose Confidential Information in accordance with a subpoena, judicial or other governmental order, or requirement of any law, regulation or the rules of any applicable stock exchange, provided that where legally permissible the Receiving Party must give the Disclosing Party reasonable written notice prior to such disclosure so that the Disclosing Party may, at Disclosing Party’s sole expense, take appropriate action to seek a protective order or injunction to seek confidential treatment for the disclosed Confidential Information.

## 8. INTELLECTUAL PROPERTY

**8.1 iCIMS IP Ownership.** As used in this Agreement, “**Intellectual Property Right**” means any patent application, patent, copyright, moral right, database right, trademark right, trade secret or other intellectual property or proprietary right recognized or enforceable under any U.S., foreign or international law, rule, or regulation. iCIMS retains ownership of and reserves all Intellectual Property Rights in or related to the Subscription, iCIMS Content or Analytics (collectively, “**iCIMS IP**”). iCIMS does not convey to Subscriber or its Affiliate or User any Intellectual Property Right in any iCIMS IP except for the non-exclusive right to use the Subscription and iCIMS Content as set forth in this Agreement. Subscriber agrees further that iCIMS is free to use and incorporate into iCIMS IP any comment, feedback, review or other input provided by Subscriber or its Affiliate, User, or Candidate, and that such use or incorporation does not create or give rise to any Intellectual Property Right of Subscriber or its Affiliate or User in iCIMS IP.

**8.2 Subscriber IP Ownership.** Subscriber retains ownership of and reserves all Intellectual Property Rights in the Subscriber Data or any other materials, communications or content that Subscriber or its Affiliate or User supplies for use in connection with the Subscription (collectively, “**Subscriber IP**”). Subscriber does not convey to iCIMS any Intellectual Property Right in any Subscriber IP, except as set forth in this Agreement.

**8.3 Subscriber IP License.** Subscriber grants iCIMS a non-exclusive, non-sublicensable right during the Term to use, copy, create derivative works of and display the Subscriber IP to perform its obligations under or as otherwise set forth in this Agreement.

**8.4 Subscriber Marks.** Subscriber grants iCIMS a non-exclusive, non-sublicensable right, during the Term, to use any Subscriber trademark, service mark or tradename contained in the Subscriber IP or designated by Subscriber for use in the Subscription (the “**Subscriber Marks**”), to perform under this Agreement, and to identify Subscriber in iCIMS’ customer lists and other marketing and promotional materials and communications referencing Subscriber as a customer of iCIMS. iCIMS shall comply with Subscriber’s written guidelines for trademark usage provided reasonably in advance.







## 9. WARRANTIES AND LIMITATIONS

9.1 **Software Warranty.** iCIMS warrants that during the Term the Subscription will perform materially in accordance with the Documentation. iCIMS' warranty does not apply to any: (i) Third-Party Product; (ii) use of the Subscription not in accordance with the Documentation, iCIMS' published policies or this Agreement; or (iii) failure of Subscriber or its Affiliate or User to follow reasonable support or maintenance instructions provided by iCIMS (each of (i), (ii), and (iii) above, an **"Excluded Condition"**). iCIMS' sole liability and obligation for breach of warranty will be to use commercially reasonable efforts to promptly repair or replace the Subscription to correct the breach, and the sole remedy of Subscriber is that it may terminate the specific portion of the Subscription (i.e., the particular products, offerings, portals, modules, or line items) that do not conform to the Documentation (**"Affected Subscription"**), subject to iCIMS' ability to cure pursuant to Section 6.3(a) herein, upon prior written notice and receive a refund of any pre-paid but unused amounts specific to the Affected Subscription if the breach extends for sixty (60) consecutive days or for any one-hundred and twenty (120) days in any three-hundred and sixty (360) day period.

9.2 **Limitations.** EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION 9, ICIMS DOES NOT MAKE AND EXPRESSLY DISCLAIMS ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, ARISING AT COMMON LAW, OR OTHERWISE RELATED TO THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING THE SUBSCRIPTION, ICIMS CONTENT AND ANY SERVICES PROVIDED UNDER THE AGREEMENT. WITHOUT WAIVING THE GENERALITY OF THE FOREGOING, ICIMS DOES NOT MAKE AND EXPRESSLY DISCLAIMS ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, DATA OR SYSTEM INTEGRITY, AVAILABILITY, TIMELINESS, COMPLETENESS, NON-INFRINGEMENT, OR THAT THE SUBSCRIPTION WILL PERFORM WITHOUT INTERRUPTION OR ERROR FREE, AND ANY WARRANTY REGARDING SUBSCRIBER'S USE OF THE SUBSCRIPTION, DATA OR INFORMATION ACCESSIBLE THEREFROM, ANY DECISION MADE USING THE SUBSCRIPTION, UNAUTHORIZED ACCESS TO THE SUBSCRIPTION, OR SUBSCRIBER'S USE OF ANY EQUIPMENT OR SOFTWARE IN CONNECTION WITH THE SUBSCRIPTION. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, ICIMS MAY MAKE CHANGES TO THE SUBSCRIPTION FROM TIME TO TIME, OR THE CORRESPONDING DOCUMENTATION, AND THOSE CHANGES SHALL NOT BE DEEMED TO GIVE RISE TO BREACH OF WARRANTY OR LIABILITY OF ICIMS.

## 10. INDEMNIFICATION

10.1 **iCIMS Indemnification.** iCIMS shall defend Subscriber and its Affiliates, officers, directors, shareholders and agents (each, a **"Subscriber Indemnitee"**) from and against any third-party claim, demand, lawsuit or legal action: (i) alleging that the iCIMS IP infringes or violates an Intellectual Property Right of a third party; (ii) arising from iCIMS' failure to perform under Section 4.1 (Data Protection) or 4.2 (Data Use and Disclosure) above; or (iii) arising from iCIMS' violation of its obligations under this Agreement with respect to Confidential Information (each of (i), (ii) and (iii)), an **"iCIMS Indemnified Claim"**), and indemnify each Subscriber Indemnitee against any damages, attorneys' fees, or other costs awarded against it in connection with an iCIMS Indemnified Claim. iCIMS' obligations under this Section 10.1 do not apply to any Excluded Condition.

10.2 **Subscriber Indemnification.** Subscriber shall defend iCIMS and its Affiliates, officers, directors, shareholders and agents (each, an **"iCIMS Indemnitee"**) from and against any third-party claim, demand, lawsuit or legal action: (i) alleging that Subscriber IP or Subscriber Marks infringe or violate an Intellectual Property Right of a third party; (ii) arising from any matter for which Subscriber is responsible under Section 3 (Subscriber Responsibilities) above; or (iii) arising from violation by Subscriber of its obligations under this Agreement with respect to Confidential Information (each of (i), (ii) and (iii)), a **"Subscriber Indemnified Claim"**), and indemnify

each iCIMS Indemnitee against any damages, attorneys' fees, or other costs awarded against it in connection with a Subscriber Indemnified Claim.

## 10.3 Indemnification Conditions.

(a) As a condition of any Party's duty to defend or indemnify under this Section 10, the person or entity seeking defense or indemnification must: (i) give the defending and indemnifying Party prompt written notice of the applicable claim, demand, or legal action; (ii) allow the defending and indemnifying Party sole control of the defense and settlement; and (iii) reasonably cooperate in the defense and settlement at the defending and indemnifying Party's reasonable cost, except that the indemnified person or entity will not be required to make any settlement payment unless the defending and indemnifying Party agrees to include that payment as an indemnified expense.

(b) In the event of any claim, demand, legal action, or notice alleging infringement of iCIMS IP, iCIMS may either: (i) replace or modify the iCIMS IP in whole or in part in a manner that does not materially degrade the Subscription; (ii) obtain a license or other grant necessary to continue to provide the iCIMS IP in accordance with the Agreement, or (iii) terminate the Agreement upon written notice to Subscriber. In such event, iCIMS' sole liability will be its obligations under Section 10.1 above and a refund to Subscriber of any pre-paid but unused fees.

## 11. LIMITATIONS OF LIABILITY

11.1 IN NO EVENT WILL ICIMS OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT OR ITS SUBJECT MATTER, WHETHER UNDER ANY THEORY OF CONTRACT, NEGLIGENCE, INTENTIONAL OR UNINTENTIONAL TORT, OR ANY OTHER LEGAL THEORY, FOR: LOST REVENUE, LOST PROFITS, LOST DAMAGES, LOSS OF DATA, LOSS OF USE, ANY CLAIM OR ACTION OF ANY THIRD PARTY (EXCEPT UNDER SECTION 10 (INDEMNIFICATION) OF THIS AGREEMENT), OR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES, WHETHER OR NOT ICIMS OR ITS AFFILIATE MAY HAVE ANTICIPATED OR BEEN ADVISED OF SUCH DAMAGES.

11.2 THE TOTAL CUMULATIVE LIABILITY OF ICIMS AND ITS AFFILIATES AND REPRESENTATIVES ARISING OUT OF OR RELATED TO THIS AGREEMENT OR ITS SUBJECT MATTER, WHETHER UNDER CONTRACT, TORT OR ANY OTHER LEGAL THEORY, SHALL NOT EXCEED, IN THE AGGREGATE, THE AMOUNT OF FEES PAID BY SUBSCRIBER IN THE TWENTY-FOUR (24) MONTHS PRIOR TO WHEN THE FIRST OF ANY SUCH LIABILITIES AROSE. IN NO EVENT WILL ICIMS BE LIABLE FOR ANY DAMAGES FOR BREACH OF CONTRACT UNDER THIS AGREEMENT UNLESS SUBSCRIBER FIRST PROVIDED TO ICIMS THIRTY (30) DAYS' PRIOR WRITTEN NOTICE AND AN OPPORTUNITY FOR ICIMS TO CURE THE BREACH WITHIN THOSE THIRTY (30) DAYS.

11.3 TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE LIMITATIONS IN THIS SECTION 11 SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE.

## 12. INSURANCE

12.1 During the Term, iCIMS shall maintain the following insurance: worker's compensation insurance, as applicable; combined single limit automobile liability insurance of at least One Million Dollars (\$1,000,000); commercial general liability insurance of at least One Million Dollars (\$1,000,000) per occurrence and Two Million Dollars (\$2,000,000) in annual aggregate; excess/umbrella liability insurance of at least Seven Million Dollars (\$7,000,000) in annual aggregate; and technology errors & omissions insurance, including cybersecurity liability, of at least Fifteen Million Dollars (\$15,000,000) per claim and in annual aggregate. iCIMS shall deliver a certificate of insurance evidencing the coverages set forth above no more than thirty (30) days after written request by Subscriber. Neither the requirement to maintain, nor failure to maintain, the specified insurance





policies shall relieve iCIMS of its responsibility for its defense or indemnity obligations under Section 10 above or liability for breach of this Agreement. Within thirty (30) days of the Subscription Start Date, iCIMS shall include Subscriber as an additional insured on its general liability, automobile, and umbrella policies, and upon written request no more frequently than once annually, iCIMS will provide a certificate evidencing the foregoing.

### 13. GENERAL TERMS

13.1 **Headings.** The descriptive headings in this Agreement are for convenience only and are not intended to be part of, or to affect the interpretation of, this Agreement.

13.2 **Relationship of the Parties.** Both Parties agree that they are independent entities and that nothing in this Agreement creates a partnership, joint venture, fiduciary, agency, or affiliate relationship between the Parties. Each Party is solely responsible for the supervision, management, direction and payment of compensation and benefits to its own employees.

13.3 **Federal Government Provisions.** If Subscriber is directly or indirectly acquiring the Subscription on behalf of the U.S. Government, the software object code and source code that is delivered as part of the Subscription is classified as "Commercial Computer Product" and "Commercial Computer Documentation" developed at private expense and containing confidential information and trade secrets of iCIMS, Inc. and its licensors, and is subject to "Restricted Rights" as that term is defined in the U.S. Federal Acquisition Regulations. Manufacturer is: iCIMS, Inc., 101 Crawford's Corner Road, Suite 3-100, Holmdel, NJ 07733, U.S.A.

13.4 **Force Majeure.** No Party will be deemed in default of this Agreement to the extent that performance of its obligations or attempts to cure any breach are materially delayed or prevented by reason of any event that is beyond the reasonable control of that Party and could not reasonably have been foreseen and protected against by that Party, including any act of nature (including fire, earthquake or natural disaster) or act of government (such as war, terrorism or embargo), provided that the non-performing Party must give the other Party prompt written notice of the event. In the event the delay or nonperformance by iCIMS as described in this Section 13.4 continues for a period of forty-five (45) consecutive days, Subscriber may elect to terminate this Agreement by written notice no more than thirty (30) days' after the end of the forty-five (45) day period, and receive a refund of any pre-paid fees for unused portions of the remaining Subscription Period. This Section 13.4 does not apply to payment obligations.

13.5 **Notices.** Notices required under this Agreement to be in writing must be made by, and notice is deemed to have been duly given when, sent by confirmed email or deposited with an overnight courier with a reliable system for tracking delivery. iCIMS shall deliver any written notice and invoice to the email address listed as the "Bill To Contact" (as listed in the most recent Order Form or as subsequently updated by Subscriber). Subscriber shall deliver any written notice to: [generalcounsel@icims.com](mailto:generalcounsel@icims.com) or iCIMS, Inc., Attn: General Counsel, 101 Crawford's Corner Road, Suite 3-100, Holmdel, New Jersey 07733, USA. Either Party may from time to time change the address for written notices by giving the other Party prior written notice of the change.

13.6 **Assignment.** Neither Party may assign any of its rights or obligations under this Agreement without prior written consent from the other Party, provided that a Party may assign this Agreement to an Affiliate or successor in interest by merger, acquisition of all stock or of substantially all assets, or reorganization. The assigning Party shall provide written notice of the assignment either before, or no more than thirty (30) days after, the assignment. Any purported assignment in violation of this paragraph is void and constitutes a material breach of this Agreement. This Agreement inures to the benefit of and is binding on each of the Parties, their successors, permitted assigns, and legal representatives.

13.7 **Size and Scale.** Subscriber shall give iCIMS written notice of any merger, acquisition (whether of stock or assets), formation of any joint venture or partnership, reorganization, or other transaction that materially increases the size or scale of Subscriber's or its Affiliate's use of the Subscription (collectively, a "**Corporate Transaction**"). In the event of any Corporate Transaction, or other material increase in Subscriber's or its Affiliate's size or scale of use, iCIMS may, by written notice, request that the fees under this Agreement be increased commensurate with the increase in size and scale, and if a written agreement increasing the fees is not entered into by the Parties within forty-five (45) days of delivery of that notice, then iCIMS may terminate this Agreement effective upon sixty (60) days' prior written notice.

13.8 **Documentation, Policy, and Addendum Changes.** iCIMS may make changes to the Documentation, Subscriber Data Security Addendum, or the policies referenced in this Agreement, or the hyperlink or other means of access to the Documentation, Subscriber Data Security Addendum, or policies, except that iCIMS may not make changes to the Subscriber Data Security Addendum that materially diminish the protections for Subscriber Data set forth therein. iCIMS provides a mechanism which may be accessed on <https://www.icims.com/gc> for Subscriber to subscribe to receive email notice of any changes to the Subscriber Data Security Addendum or policies listed on <https://www.icims.com/gc>. If Subscriber believes that any change to the Subscriber Data Security Addendum or a policy creates a materially new obligation of Subscriber, materially degrades the Subscriber Data Security Addendum or applicable policy, or materially diminishes the Subscription taken as a whole (each, a "**Material Adverse Change**"), then Subscriber may, within thirty (30) days of the change, object to such Material Adverse Change by delivering written notice to iCIMS. Any objection notice must set forth the basis of the objection with reasonable particularity. In the event of such an objection, the Material Adverse Change will not be deemed effective as to Subscriber for thirty (30) days, and iCIMS and Subscriber shall work together reasonably, and in good faith, to resolve the objection. If within that thirty (30) day period the objection is not resolved and Subscriber delivers a further written notice of objection within ten (10) days of the end of such period, then the Material Adverse Change shall remain ineffective as to Subscriber and iCIMS shall have ten (10) days from iCIMS' receipt of such further written notice in which to notify Subscriber that the Material Adverse Change will not apply to Subscriber for the remainder of the Term. If iCIMS does not provide such notice within ten (10) days, then Subscriber may terminate this Agreement for convenience if it provides iCIMS with written notice of termination within ten (10) days, with the effective date of such termination to be no later than thirty (30) days from the date of the termination notice.

13.9 **Third-Party Beneficiaries.** No other person has any rights, interest, or claims hereunder or is entitled to any benefits under or on account of this Agreement as a third-party beneficiary or otherwise.

13.10 **Subpoenas.** *Reserved.*

13.11 **Law and Forum.** The law that will apply in any dispute or lawsuit arising out of or in connection with this Agreement, and the courts that have jurisdiction over any such dispute or lawsuit, will be construed in accordance with, the laws of the State of California, and any lawsuit related to this Agreement or its subject matter will be heard only in the federal or state courts located in the State of California in the County of Monterey.

The foregoing shall apply without regard to conflict of law provisions, the United Nations Convention on Contracts for the International Sale of Goods, or the Uniform Computer Information Transactions Act. The Parties hereby submit to the personal jurisdiction of and venue in the courts listed above in each case.

13.12 **Rules of Interpretation.** It is the intention of the Parties that if a court of competent jurisdiction determines that any provision of this Agreement is unenforceable, the remaining provisions of the Agreement will remain in full force and effect. In the event of any conflict between this





Agreement and an Order Form, statement of work, addendum or exhibit, the Agreement will be given precedence, except as expressly set forth in the applicable Order Form, statement of work, addendum or exhibit. Unless explicitly specified to the contrary, the word "including" wherever used herein or in any addendum means "including, but not limited to". This Subscription Agreement is drafted in the English language, but may be made available in other languages for convenience purposes only, at iCIMS' discretion. The Parties agree that the English language version of the Subscription Agreement shall control for the purposes interpretation and with respect to any dispute.

13.13 **Entire Agreement; Amendment; and Waiver.** Certain components of the Subscription or other products or services set forth in an Order Form may be subject to additional terms and conditions as stated in such Order Form or an addendum to the Agreement. No Order Form or statement of work is binding on the Parties unless agreed by both Parties in writing. Each binding Order Form, statement of work, and addendum is incorporated into and made part of this Agreement. This Agreement supersedes all prior discussions, statements, representations, and

agreements, oral or written, between the Parties relating to the subject matter of the Agreement, and constitutes the entire agreement between the Parties relating to its subject matter. Subscriber acknowledges and agrees that its purchase and use of the Subscription and iCIMS Content is neither contingent on the delivery of any new future functionality or features, nor dependent on any oral or written comments made by iCIMS or its Affiliates regarding any new future functionality or features. Except as expressly provided herein, this Agreement may be amended, modified, or supplemented only by a written document signed by an authorized representative of each Party. The failure of either Party, at any time, to enforce any right or remedy available to it under this Agreement or otherwise with respect to any breach or failure by the other Party does not constitute a waiver of such right or remedy with respect to any other breach or failure by the other Party.

13.14 **Counterparts.** This Agreement may be executed by facsimile or other electronic means, and in one or more counterparts, each of which is deemed to be an original, but all of which together constitute one and the same Agreement.

**IN WITNESS WHEREOF**, the Parties hereto have caused this Agreement to be signed by duly authorized officers or representatives as of the date of last signature below.

iCIMS, Inc.

Signature:

Signed by:  
*Michael Pastore*  
87D511B83FE440F...

Name:

Michael Pastore

Title:

VP, Sales Operations

Date:

11/4/2024 | 1:55:37 PM EST

GCO Initial:

*GCO*

Date: 11/4/2024 | 1:46:10 PM EST

Subscriber: Monterey County Department of Social Services

Signature:

Name:

Title:

Date:

DocuSigned by:

*Anne Brunton*  
A46091E5DE63489...  
Deputy County Counsel

11/7/2024 | 10:34 AM PST







## Data Processing Addendum

This Data Processing Addendum (“**Addendum**”) is incorporated into and forms part of the Subscription Agreement (“**Subscription Agreement**”) between the applicable iCIMS contracting entity under the Subscription Agreement (“**iCIMS**”) and the entity that executed the Subscription Agreement and/or Order Form (“**Subscriber**”) acting on its own behalf and as agent for each Subscriber Affiliate.

### About this Addendum:

1. This Addendum consists of four parts: the main body of the Addendum, Appendix 1, Appendix 2, and Appendix 3. Part C of Appendix 1 and Appendix 3 shall only be applicable to the extent required by Data Protection & Privacy Laws, and in such case the Annexes of the Standard Contractual Clauses shall be populated with the information set out in the Appendices of this Addendum.
2. If the Standard Contractual Clauses in Appendix 3 are applicable, the Subscriber’s signature of the Subscription Agreement and/or applicable Order Form(s) shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Annexes. Please note that the contracting entity under the Subscription Agreement and/or Order Form may be an iCIMS Affiliate.
3. Subscriber must review Appendices 1 and 2 for accuracy and completeness.

iCIMS acknowledges that Subscriber and each Subscriber Affiliate is/are Controller(s) in relation to the Personal Data under their respective control as the legal person competent to determine purposes and methods of the Processing of the Personal Data and the relevant means, including the adequacy of the security measures. Subscriber hereby appoints iCIMS as a Processor to Process Subscriber Personal Data as described in the Subscription Agreement and Appendix 1 which further details the subject-matter, type, and purpose of Processing, the types of data, and categories of Data Subjects. iCIMS accepts the appointment and undertakes to duly fulfil the obligations set forth in this Addendum. Subscriber shall serve as a single point of contact for iCIMS with regards to any notification or information to be given to either Subscriber or any Subscriber Affiliate under this Addendum and is responsible for the internal coordination, review and submission of instructions or requests of Subscriber Affiliates to iCIMS. With regard to Personal Data Processed for iCIMS Business Operations, the Parties acknowledge that Subscriber and each Subscriber Affiliate is/are Controller(s) and iCIMS and iCIMS Affiliates is/are independent Controller(s), not a joint controller with Subscriber and/or each Subscriber Affiliate.

Unless otherwise defined below, all capitalized terms have the meaning given to them in the Subscription Agreement and/or exhibits thereto. Any examples in this Addendum are illustrative and not the sole examples of a particular concept.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Subscription Agreement. Except where the context requires otherwise, references in this Addendum to the Subscription Agreement are to the Subscription Agreement as amended by, and including, this Addendum.

### 1. Definitions

- 1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:
- 1.1.1 “**Business**” has the meaning assigned to it in the CCPA (as defined below);
  - 1.1.2 “**Business Purpose**” has the meaning assigned to it in the CCPA (as defined below);
  - 1.1.3 “**California Consumer Privacy Act of 2018**” or “**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended, and its implementing regulations;



- 1.1.4 “**Collects**” or “**Collected**” have the meaning assigned to it in the CCPA;
- 1.1.5 “**Contracted Processor**” means iCIMS or one of its Sub-Processors;
- 1.1.6 “**Controller**” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
- 1.1.7 “**Data Protection & Privacy Laws**” means all data protection and privacy laws, including local, state (e.g., the CCPA), national and/or foreign laws, treaties, and/or regulations, the GDPR (as defined below), and implementations of the GDPR into national law, in each case, to the extent applicable to the respective Party in its role in the Processing of Personal Data under the Subscription Agreement;
- 1.1.8 “**Data Subject**” means an identified or identifiable natural person whose rights are protected by Data Protection & Privacy Laws, including a “Consumer” as defined in the applicable Data Protection & Privacy Laws;
- 1.1.9 “**GDPR**” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Where applicable, references to the “GDPR” include the UK GDPR, Swiss DPA, and/or Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the Processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC;
- 1.1.10 “**iCIMS Affiliate**” means an entity that directly or indirectly controls, is controlled by, or is under common control with iCIMS, in each case through majority voting power;
- 1.1.11 “**iCIMS Business Operations**” means iCIMS’ legitimate business operations incident to administration and delivery of the Subscription to Subscriber, and for its other legitimate purposes relating to iCIMS’ business operations, including billing and account management, internal reporting, provision of customer support, preventing or responding to illegal conduct, fraud, abuse or a threat to the security or integrity of iCIMS’ systems or data including the Subscription, improving iCIMS products and services, establishing, exercising or defending iCIMS’ legal claims, and compliance with applicable legal obligations. For purposes of the CCPA, all processing of Personal Data in connection with iCIMS Business Operations is a permitted Business Purpose;
- 1.1.12 “**Personal Data**” means any information relating to a Data Subject, including “Personal Information” as defined in the CCPA;
- 1.1.13 “**Personal Data Breach**” has the meaning assigned to it or an equivalent defined term in the applicable Data Protection & Privacy Laws, in each case as it relates to the Processing of Subscriber Personal Data by iCIMS under the Subscription Agreement and this Addendum where such Personal Data Breach occurs as a result of iCIMS’ breach of its data security obligations under this Addendum;
- 1.1.14 “**Process**” and “**Processing**” mean any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing, or destroying;
- 1.1.15 “**Processor**” means the entity which Processes Subscriber Personal Data on behalf of the Controller;



- 1.1.16 **“Restricted Transfer”** means:
- 1.1.16.1 a transfer of Subscriber Personal Data or Personal Data Processed for iCIMS Business Operations from any Subscriber Group Member to a Contracted Processor; or
  - 1.1.16.2 an onward transfer of Subscriber Personal Data or Personal Data Processed for iCIMS Business Operations from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor;
- in each case, where such transfer would be prohibited by Data Protection & Privacy Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection & Privacy Laws) in the absence of appropriate safeguards such as the Standard Contractual Clauses to be established under Section 6.4.3 or Section 13. For the avoidance of doubt, where a transfer of Subscriber Personal Data or Personal Data Processed for iCIMS Business Operations is of a type authorized by Data Protection & Privacy Laws in the exporting country, such transfer shall not be a Restricted Transfer;
- 1.1.17 **“Sale”** or **“Sell”** has the meaning assigned to it in the CCPA;
- 1.1.18 **“Service Provider”** has the meaning assigned to it in the CCPA;
- 1.1.19 **“Share”** has the meaning assigned to it in the CCPA;
- 1.1.20 **“Standard Contractual Clauses”** means the clauses set forth, or incorporated by reference, in Appendix 3;
- 1.1.21 **“Sub-Processor”** means any entity engaged by iCIMS, including any iCIMS Affiliate, to Process Subscriber Personal Data on behalf of any Subscriber Group Member pursuant to or in connection with the Subscription Agreement, including “Service Provider” as defined in the CCPA;
- 1.1.22 **“Subscriber Affiliate”** means an entity that directly or indirectly controls, is controlled by, or is under common control with Subscriber, in each case through majority voting power;
- 1.1.23 **“Subscriber Group Member”** means Subscriber or any Subscriber Affiliate;
- 1.1.24 **“Subscriber Personal Data”** means any Subscriber Data that is Personal Data and is Processed by a Contracted Processor on behalf of a Subscriber Group Member pursuant to or in connection with the Subscription Agreement;
- 1.1.25 **“Supervisory Authority”** means, as applicable, an appointed government entity with the authority to enforce Data Protection & Privacy Laws, such as a supervisory authority as defined in the GDPR or “Commissioner” as defined under Swiss member state law and/or the UK GDPR;
- 1.1.26 **“Swiss DPA”** means the Swiss Federal Data Protection Act as may be amended or superseded from time to time; and
- 1.1.27 **“UK GDPR”** means, collectively, the United Kingdom (“UK”) General Data Protection Regulation as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018, and amended Data Protection Act 2018, in each case as may be amended or superseded from time to time.



1.2 The word “**include**” shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

## **2. Roles & Scope**

2.1 This Addendum applies to the Processing of Subscriber Personal Data by iCIMS in connection with the provision of the Subscription and related services. For the purposes of this Addendum, Subscriber and Subscriber Affiliates are the Controller(s) and iCIMS is the Processor. To the extent Subscriber Personal Data is subject to the CCPA, Subscriber and Subscriber Affiliates (as applicable) are the Business(es) and iCIMS is the Service Provider.

2.2 iCIMS does not determine whether Subscriber Data includes information subject to any specific laws or regulations. As between the Parties, Subscriber is responsible for determining the lawfulness of the Processing of Subscriber Personal Data. For the avoidance of doubt, iCIMS is not responsible for determining that Subscriber’s configuration of the Subscription meets the requirements of any applicable laws or regulations, or for complying with data protection and privacy laws applicable to Subscriber or Subscriber’s industry that are not applicable to the Subscription, such as those not generally applicable to online service providers.

2.3 Subscriber acknowledges and agrees that as part of providing the Subscription and related services, iCIMS has the right to Process data (including Personal Data) relating to or obtained in connection with the operation, support, or use of the Subscription for iCIMS Business Operations. To the extent iCIMS uses or otherwise Processes Personal Data subject to Data Protection & Privacy Laws for iCIMS Business Operations, iCIMS will comply with the obligations of an independent Controller under Data Protection & Privacy Laws for such use and only for the purposes compatible with those described in the Subscription Agreement, this Addendum, or other agreement between the Parties. iCIMS will not use or disclose such Personal Data for any other purpose unless it has first rendered the Personal Data anonymous, de-identified, and non-personal so it does not identify the Subscriber or any other person.

## **3. Processing of Subscriber Personal Data**

3.1 iCIMS and each iCIMS Affiliate shall:

3.1.1 comply with Data Protection & Privacy Laws in the Processing of Subscriber Personal Data;

3.1.2 Process Subscriber Personal Data only on the relevant Subscriber Group Member’s documented instructions for the following purpose:

3.1.2.1 Processing in accordance with the Subscription Agreement and applicable Order Form(s);

3.1.2.2 Processing initiated by Candidates and Users in their use of the Subscription;

3.1.2.3 Processing to render Subscriber Personal Data anonymous, de-identified, and non-personal; and

3.1.2.4 Processing to comply with other documented reasonable instructions provided by Subscriber (e.g., via email);

where such instructions are consistent with the terms of the Subscription Agreement, unless Processing is required by Data Protection & Privacy Laws to which the relevant Contracted Processor is subject, in which case iCIMS or the relevant iCIMS Affiliate shall to the extent permitted by Data Protection & Privacy Laws inform the relevant Subscriber Group Member of that legal requirement



before the relevant Processing of that Subscriber Personal Data. For the avoidance of doubt, an instruction, approval, request or similar action given via the Subscription, including Subscriber's configuration of any settings or options in the Subscription (as Subscriber may be able to modify from time to time), is considered a Subscriber's Processing instruction. The Parties agree that for the purpose of the Standard Contractual Clauses, the Processing of Subscriber Personal Data by iCIMS is deemed to be in compliance with Subscriber's instructions if authorized by the Subscription Agreement, Order Form, this Addendum, or other agreement between the Parties;

3.1.3 immediately inform the Subscriber if, in its opinion, an instruction from Subscriber infringes Data Protection & Privacy Laws. For purposes of clarity, Subscriber understands and acknowledges that iCIMS and the relevant iCIMS Affiliate do not monitor Subscriber's configuration of settings or options in the Subscription and Subscriber is solely responsible to ensure that its Processing of Personal Data pursuant to or in connection with the Subscription does not violate Data Protection & Privacy Laws; and

3.1.4 where Processing of Subscriber Personal Data is subject to the CCPA,

3.1.4.1 be prohibited from: (i) Selling or Sharing Subscriber Personal Data it Collects pursuant to the Subscription Agreement; (ii) retaining, using, or disclosing the Subscriber Personal Data that it Collected pursuant to the Subscription Agreement for a commercial purpose other than the Business Purposes specified in the Subscription Agreement, or as otherwise permitted by the CCPA; (iii) retaining, using, or disclosing the Subscriber Personal Data that it Collected pursuant to the Subscription Agreement outside of the direct business relationship between iCIMS and Subscriber except as permitted by the CCPA; and (iv) combining Subscriber Personal Data that it Collected pursuant to the Subscription Agreement with Personal Data that iCIMS receives from or on behalf of another source, or that iCIMS Collected from its own interactions with Data Subjects, except where permitted by the CCPA. iCIMS certifies that it understands the foregoing restrictions and shall comply with them; and

3.1.4.2 notify Subscriber if iCIMS makes a determination that it can no longer meet its obligations with respect to its Processing of Subscriber Personal Data, in which case upon such notice, Subscriber may take reasonable and appropriate steps to stop and remediate unauthorized use of Subscriber Personal Data.

3.2 Each Subscriber Group Member:

3.2.1 instructs, subject to section 3.1, iCIMS and each iCIMS Affiliate (and authorizes iCIMS and each iCIMS Affiliate to instruct each Sub-Processor) to:

3.2.1.1 Process Subscriber Personal Data; and

3.2.1.2 in particular, transfer Subscriber Personal Data to any country or territory permitted by Subscriber, which, for the avoidance of doubt, includes: (i) the location(s) of the iCIMS data center(s), which will be the United States unless otherwise indicated in the Subscription Agreement, product addenda, and/or applicable Order Form(s); (ii) the locations of Processing by the Sub-Processors identified in this Addendum and/or the Standard Contractual Clauses; and (iii) the United States, India, European Economic Area





("EEA"), and UK, to the extent necessary for iCIMS personnel to implement and provide support and maintenance of the Subscription;

as reasonably necessary for the provision of the Subscription and consistent with the Subscription Agreement;

3.2.2 shall obtain all rights, permissions and/or authorizations, including provide all disclosures and/or obtain all consents, required by applicable Data Protection & Privacy Laws, to permit Processing of Personal Data, including transfers of Personal Data, as provided in the Subscription Agreement and/or this Addendum;

3.2.3 is responsible for compliance with any data residency or localization obligations under applicable Data Protection & Privacy Laws that mandate retention of Personal Data or a copy thereof in the local jurisdiction if Subscriber elects to use the Subscription in any country or territory where iCIMS does not have a data center; and

3.2.4 warrants and represents that its instructions for the Processing of Subscriber Personal Data complies with Data Protection & Privacy Laws, and it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 3.2.1 on behalf of each relevant Subscriber Affiliate.

3.3 Appendix 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Subscriber Personal Data as required by Article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection & Privacy Laws) and Personal Data Processed for iCIMS Business Operations.

#### **4. iCIMS and iCIMS Affiliate Personnel; Data Protection Officer**

iCIMS and each iCIMS Affiliate shall take reasonable steps to ensure the reliability of any employee or contractor of iCIMS who may have access to the Subscriber Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Subscriber Personal Data, as strictly necessary for the purposes of the Subscription Agreement, and to comply with Data Protection & Privacy Laws in the context of that individual's duties, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. iCIMS has appointed a data protection officer who can be reached at [privacy@icims.com](mailto:privacy@icims.com).

#### **5. Security**

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, iCIMS and each iCIMS Affiliate shall in relation to the Subscriber Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR or as otherwise contained in Data Protection & Privacy Laws and the measures set forth in the Subscriber Data Security Addendum attached as Appendix 2.

5.2 In assessing the appropriate level of security, iCIMS and each iCIMS Affiliate shall take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Subscriber Personal Data transmitted, stored, or otherwise Processed.



## 6. Sub-Processing

6.1 Each Subscriber Group Member authorizes iCIMS and each iCIMS Affiliate to appoint (and permit each Sub-Processor appointed in accordance with this Section 6 to appoint) Sub-Processors in accordance with this Section 6.

6.2 iCIMS and each iCIMS Affiliate may continue to use those Sub-Processors already engaged by iCIMS or any iCIMS Affiliate as at the date of this Addendum, subject to iCIMS and each iCIMS Affiliate in each case meeting the obligations set out in Section 6.4. The list of Sub-Processors used to provide the Subscription and their country or location of Processing may be accessed at <https://www.icims.com/subprocessors/> (the “**Sub-Processor List**”). Intended changes to Sub-Processors will be posted to the Sub-Processor List and, subject to the terms in Section 6.3, shall go into effect thirty (30) days thereafter. Subscriber shall access and complete the registration form at <https://www.icims.com/gc> to subscribe to receive email notice when iCIMS intends to add or replace a third-party Sub-Processor, and iCIMS shall provide notification of such changes to the email address(es) registered by Subscriber.

6.3 Subscriber may object to iCIMS’ proposed Sub-Processor changes by notifying iCIMS in writing at [privacy@icims.com](mailto:privacy@icims.com) within thirty (30) days of iCIMS’ notice in accordance with the mechanism set forth in Section 6.2 (the “**Objection Period**”) if Subscriber reasonably determines such Sub-Processor is unable to Process Subscriber Personal Data in accordance with the terms of this Addendum. Such notice shall explain the Subscriber’s good-faith, reasonable grounds for the objection. If iCIMS receives a Sub-Processor objection notice from Subscriber within the Objection Period:

6.3.1 iCIMS shall work with Subscriber in good faith to make available a reasonable change in the provision of the Subscription or recommend a reasonable change to Subscriber’s configuration or use of the Subscription which avoids the use of the proposed Sub-Processor; and

where such a change cannot be made within thirty (30) days from iCIMS’ receipt of Subscriber’s objection notice (the “**Cure Period**”), notwithstanding anything in the Subscription Agreement, Subscriber may by written notice to iCIMS within five (5) business days after the expiration of the Cure Period, with immediate effect, terminate the applicable Order Form(s) with respect only to those Subscriptions (i.e., product offering, portal, module, line item) which cannot be provided by iCIMS without the use of the objected-to new Sub-Processor (the “**Terminated Service Portion**”). iCIMS will refund to Subscriber any prepaid fees covering the remainder of the Subscription Period for the Terminated Service Portion following the effective date of termination with respect to such Terminated Service Portion, without imposing a penalty for such termination on Subscriber. Notwithstanding anything to the contrary in the Subscription Agreement or this Addendum, the Terminated Service Portion and refund as set forth above shall be Subscriber’s sole and exclusive remedy if Subscriber objects to changes to Sub-Processors. If Subscriber does not provide an objection within the Objection Period, then such Sub-Processor shall be deemed approved by Subscriber. If Subscriber submitted a valid objection during the Objection Period and does not terminate the applicable Order Form(s) within five (5) business days after the expiration of the Cure Period, Subscriber’s objection shall be considered withdrawn and the proposed Sub-Processor shall be deemed approved.

6.4 With respect to each Sub-Processor, iCIMS or the relevant iCIMS Affiliate shall:

6.4.1 before the Sub-Processor first Processes Subscriber Personal Data (or, where relevant, in accordance with Section 6.2), carry out due diligence to ensure that the Sub-Processor is capable of providing the level of protection for Subscriber Personal Data required by the Subscription Agreement;



- 6.4.2 ensure that the arrangement between on the one hand (a) iCIMS, or (b) the relevant iCIMS Affiliate, or (c) the relevant intermediate Sub-Processor; and on the other hand, the Sub-Processor, is governed by a written contract including terms which offer at least the same level of protection for Subscriber Personal Data as those set out in this Addendum and meet the requirements of Data Protection & Privacy Laws, which include Article 28(3) of the GDPR; and
- 6.4.3 if that arrangement involves a Restricted Transfer, ensure that appropriate safeguards (e.g., the applicable Standard Contractual Clauses, binding corporate rules, etc.) are at all relevant times incorporated into the agreement between on the one hand (a) iCIMS, or (b) the relevant iCIMS Affiliate, or (c) the relevant intermediate Sub-Processor; and on the other hand, the Sub-Processor.
- 6.5 iCIMS shall be liable for the acts and omissions of its Sub-Processors to the same extent iCIMS would be liable if performing the services of each Sub-Processor directly under the terms of this Addendum.
- 6.6 The Parties agree that any copy of a Sub-Processor agreement that iCIMS must provide to Subscriber pursuant to the Standard Contractual Clauses may have all commercial, proprietary, and confidential information, and clauses unrelated to this Addendum and the Standard Contractual Clauses, removed or redacted by iCIMS beforehand; and, that such copy will be provided by iCIMS, in a manner mutually agreed upon by the Parties, only upon request by Subscriber.
- 6.7 For the avoidance of doubt, Subscriber is solely responsible for its integration and/or use of any Third-Party Product to Process Subscriber Personal Data pursuant to or in connection with the Subscription and ensuring that such Processing complies with Data Protection & Privacy Laws. Any Third-Party Product integrated and/or used shall not be deemed a Sub-Processor for any purpose under this Addendum.
- 7. Data Subject Rights**
- 7.1 Taking into account the nature of the Processing and the information available to iCIMS as a Processor, iCIMS and each iCIMS Affiliate shall assist each Subscriber Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Subscriber Group Members' obligations to respond to requests to exercise Data Subject rights under Data Protection & Privacy Laws. To the extent legally permitted, Subscriber shall be responsible for any costs arising from iCIMS' provision of such assistance that is beyond the scope of such technical and organizational measures and standard assistance provided by iCIMS in the ordinary course of business.
- 7.2 iCIMS will, at its election and as necessary to enable Subscriber to meet its obligations under Data Protection & Privacy Laws, either (i) provide Subscriber the ability within the Subscription to correct or delete Subscriber Personal Data or restrict its Processing; or (ii) make such corrections, deletions, or restrictions within the Subscription on Subscriber's behalf if such self-service functionality is not available within the Subscription for the Subscriber to perform itself. To the extent any Subscriber Personal Data of a Data Subject is not accessible to Subscriber through the Subscription, iCIMS will, as necessary to enable Subscriber to meet its obligations under Data Protection & Privacy Laws, provide reasonable assistance to make such Subscriber Personal Data available to Subscriber.
- 7.3 During the term of the Subscription Agreement, Subscriber may extract Subscriber Personal Data from the Subscription in accordance with the Documentation and the relevant provisions of the Subscription Agreement, including so that Subscriber can provide the Personal Data to a Data Subject who makes an applicable Data Subject Request (as defined below) for such Personal Data.



7.4 For the avoidance of doubt, Subscriber is responsible for responding to and complying with a Data Subject's request to exercise their rights under Data Protection & Privacy Laws regarding their Personal Data in the Subscription ("**Data Subject Request**"). The Subscription includes controls that Subscriber may use to assist Subscriber with responding to a Data Subject Request. If Subscriber is unable to use the controls within the Subscription to assist Subscriber with responding to the Data Subject Request, iCIMS will reasonably cooperate with Subscriber to enable Subscriber to respond to the Data Subject Request. If iCIMS directly receives a Data Subject Request outside of the Subscription that specifically names Subscriber, iCIMS will promptly redirect the Data Subject to submit its request to Subscriber, promptly notify Subscriber of such request, and not otherwise respond to such request unless expressly authorized by Subscriber.

## **8. Personal Data Breach**

8.1 In accordance with iCIMS' documented incident response policies and procedures, in the event that iCIMS becomes aware of a Personal Data Breach affecting Subscriber Personal Data, iCIMS shall notify Subscriber without undue delay, and in any event within the notification period required by Data Protection & Privacy Laws, providing Subscriber with at least the following information (to the extent such information is known or available to iCIMS): (i) a description of the nature of the Personal Data Breach, the categories and approximate number of Data Subjects and Personal Data records concerned, (ii) name and contact details of a contact person at iCIMS for further information, (iii) a description of the likely consequences of the Personal Data Breach, and (iv) a description of the measures taken or proposed to be taken for the remedy or mitigation of the Personal Data Breach. When it is not possible to provide such information at the same time, the information may be provided in phases without undue further delay. iCIMS will promptly take all measures and actions that are reasonably necessary to remedy or mitigate the effects of the Personal Data Breach and shall keep Subscriber informed of all developments in connection with the Personal Data Breach to allow Subscriber and each Subscriber Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection & Privacy Laws.

8.2 iCIMS shall cooperate with Subscriber and each Subscriber Group Member and take such reasonable steps as are directed by Subscriber to assist in the investigation, mitigation, and remediation of each such Personal Data Breach. In the event that a personal data breach (or similar term defined under applicable Data Protection & Privacy Laws) is not the result of iCIMS' breach of its data security obligations under this Addendum, iCIMS reserves the right to charge Subscriber for costs arising from provision of cooperation and assistance, provided such costs will be mutually agreed between the Parties.

8.3 Subscriber shall notify iCIMS promptly after becoming aware of any misuse of Subscriber's accounts or authentication credentials or any personal data breach related to the Subscription.

8.4 Neither Party's notification of or response to a Personal Data Breach under this Section 8 is an acknowledgment by such Party of any fault or liability with respect to the Personal Data Breach.

## **9. Data Protection Impact Assessment and Prior Consultation**

iCIMS and each iCIMS Affiliate shall, to the extent Subscriber does not otherwise have access to the relevant information, and to the extent it is available to iCIMS, provide reasonable assistance to each Subscriber Group Member with any data protection impact assessments or like assessments (e.g., privacy impact assessment), and prior consultations with a Supervisory Authority or other competent data privacy authority, which Subscriber reasonably considers to be required of any Subscriber Group Member by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection & Privacy Law, in each case solely in relation to Processing of Subscriber Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors. To the extent legally permitted, Subscriber shall be responsible for any costs arising from



iCIMS' provision of such assistance that is beyond the scope of standard assistance provided by iCIMS in the ordinary course of business.

## 10. Deletion or Return of Subscriber Personal Data

- 10.1 Subject to Sections 10.2 and 10.3, iCIMS and each iCIMS Affiliate shall promptly and in any event within thirty (30) days of Subscriber's written request or the date of cessation of any Subscription involving the Processing of Subscriber Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of Subscriber Personal Data, in accordance with iCIMS' documented data storage and retention policies and procedures.
- 10.2 Subject to Section 10.3, Subscriber may, in its absolute discretion, by written notice to iCIMS and within ten (10) days of the Cessation Date, request that iCIMS and each iCIMS Affiliate return a complete copy of all Subscriber Personal Data to Subscriber in a format and method as set forth in the Subscription Agreement.
- 10.3 Each Contracted Processor may retain Subscriber Personal Data (i) to the extent required by Data Protection & Privacy Laws or other applicable laws and only to the extent and for such period as required by such laws, and/or (ii) on its backup media and backup servers until such time as the backup copies are scheduled to be deleted (not to exceed one (1) year from the Cessation Date or deletion request, as applicable); provided, however, that iCIMS and each Contracted Processor shall ensure the confidentiality of all such Subscriber Personal Data and shall ensure that such Subscriber Personal Data is not Processed in violation of Data Protection & Privacy Laws.
- 10.4 After the Cessation Date, upon the written request of Subscriber, iCIMS shall provide written certification, within thirty (30) days of receiving the request, that it has deleted and/or returned all copies of Subscriber Personal Data governed by Data Protection & Privacy Laws in accordance with iCIMS' documented data storage and retention policies and procedures. The Parties agree that for the purpose of the Standard Contractual Clauses, iCIMS is required to provide certification of deletion of Subscriber Personal Data only upon the written request by Subscriber.

## 11. Controller Responsibilities

With regard to Subscriber Personal Data, the Parties agree that iCIMS shall not be required to undertake any task that according to Data Protection & Privacy Laws is assigned to be performed by the Subscriber, in their capacity as Controller.

## 12. Audit Rights

- 12.1 If a Supervisory Authority requires an audit of the facilities from which iCIMS Processes Subscriber Personal Data in order to ascertain or monitor Subscriber's compliance with Data Protection & Privacy Laws, iCIMS will reasonably cooperate with such audit. Subscriber is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time iCIMS expends for any such audit, in addition to the rates for services performed by iCIMS, where (a) such assistance is beyond the scope of such technical and organizational measures and standard assistance provided by iCIMS in the ordinary course of business; and (b) to the extent that such costs do not result from iCIMS' breach of this Addendum or are not expressly prohibited by Data Protection & Privacy Laws.
- 12.2 Subscriber agrees that iCIMS' then-current SOC2 audit report (or comparable industry-standard successor reports) and/or iCIMS' ISO 27001 and 27701 certifications (collectively, "**Audit Reports**") will be used in the first instance to satisfy any audit or inspection rights or requests by or on behalf of Subscriber, and iCIMS shall make such Audit Reports available to Subscriber upon written request thereof. If such Audit Reports do not provide sufficient





information to demonstrate that iCIMS' implementation and maintenance of the technical and organizational measures complies with iCIMS' obligations as a processor under applicable Data Protection & Privacy Laws, iCIMS will make available to Subscriber such information in iCIMS' possession or control as Subscriber may reasonably request with a view to demonstrating iCIMS' compliance with the obligations of Processors under Data Protection & Privacy Laws in relation to its Processing of Subscriber Personal Data in the form of: (i) answers to a written security and/or privacy questionnaire provided by the Subscriber, or references to where information required under such questionnaire is available, and (ii) a description of iCIMS' technical and organizational practices in respect of the Processing of Subscriber Personal Data. Subscriber shall promptly provide in writing to iCIMS any audit findings, including, information regarding any non-compliance discovered during the course of an audit, which, together with the Audit Reports and any additional information provided by iCIMS, shall be considered iCIMS' Confidential Information. The Parties further agree that the Subscriber that is the contracting party to the Subscription Agreement shall, when carrying out any audit of the procedures relevant to the protection of Subscriber Personal Data, take all reasonable measures to limit any impact on iCIMS by combining several audit requests carried out on behalf of different Subscriber Affiliates in one single audit.

- 12.3 The Parties agree that the audits described in the Standard Contractual Clauses or required under applicable Data Protection & Privacy Laws, shall be carried out in accordance with the specifications set forth in Sections 12.1 and 12.2.

### 13. Restricted Transfers

- 13.1 For Restricted Transfers, the Parties agree that such Restricted Transfers between the Parties shall be governed by the Standard Contractual Clauses, which are incorporated into and made subject to this Addendum by this reference. Notwithstanding the foregoing, iCIMS participates in the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework (together, "**Frameworks**"). The Parties agree that transfers of Subscriber Personal Data and Personal Data Processed for iCIMS Business Operations to the United States that are subject to the Frameworks are transfers on the basis of an adequacy decision unless and until either: (i) iCIMS discontinues its participation with the applicable Frameworks, or (ii) there is a legally binding, final decision that the Frameworks do not ensure an adequate level of protection under Data Protection & Privacy Laws, in which case, the Parties agree that any transfers that constitute a Restricted Transfer between the Parties, shall be governed by the Standard Contractual Clauses as set forth in Appendix 3 of this Addendum.
- 13.2 *Alternative Transfer Mechanism.* To the extent that iCIMS adopts an alternative data export mechanism approved by the applicable government authority or applicable Supervisory Authority (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Data Protection & Privacy Laws ("**Alternative Transfer Mechanism**")), the Alternative Transfer Mechanism shall automatically apply instead of any applicable transfer mechanism described in this Addendum (but only to the extent such Alternative Transfer Mechanism complies with applicable Data Protection & Privacy Laws and extends to territories to which Personal Data is transferred).



## 14. General Terms

- 14.1 *Governing law and jurisdiction.* The Parties to this Addendum hereby agree to the governing law and submit to the choice of jurisdiction stipulated in the Subscription Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity. If the Standard Contractual Clauses are in effect between the Parties, then this Addendum shall be governed by the laws of the jurisdiction stipulated for this purpose in the Standard Contractual Clauses.
- 14.2 *Order of precedence.* Nothing in this Addendum reduces iCIMS' or any iCIMS Affiliate's obligations under the Subscription Agreement in relation to the protection of Subscriber Personal Data or permits iCIMS or any iCIMS Affiliate to Process (or permit the Processing of) Subscriber Personal Data in a manner which is prohibited by the Subscription Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail, except with respect to provisions of this Addendum that expressly clarify a specific provision of the Standard Contractual Clauses. In addition, subject to Section 14.1 and the preceding provisions of this Section 14.2, with regard to the subject matter of this Addendum, in the event of any conflict or inconsistency between the provisions of this Addendum and any other agreements between the Parties, including the Subscription Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail. The Parties hereto agree that this Addendum shall amend and replace any other amendment or addendum pertaining to the Processing of Subscriber Personal Data entered into by the Parties.
- 14.3 *Third-Party Beneficiary Rights.* Except where required by Data Protection & Privacy Laws and/or as explicitly provided for by the Standard Contractual Clauses, the terms of this Addendum and the Standard Contractual Clauses do not create any third-party beneficiary rights for any individual Data Subjects.
- 14.4 *Changes in Data Protection & Privacy Laws.* In the event that Data Protection & Privacy Laws are amended, replaced, or repealed, the Parties shall, where necessary, negotiate in good faith a solution to enable the Processing of Subscriber Personal Data to be conducted in compliance with Data Protection & Privacy Laws.
- 14.5 *Cooperation.* If iCIMS receives a legally binding request from a public authority, including judicial authorities, or becomes aware of any direct access by a law enforcement agency to Subscriber Personal Data, iCIMS will notify Subscriber so long as iCIMS is not legally prohibited from doing so. If iCIMS is legally prohibited from notifying Subscriber, iCIMS agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible, to Subscriber. iCIMS agrees to document its best efforts in order to be able to demonstrate them on request of Subscriber. For the avoidance of doubt, this Addendum shall not require iCIMS to pursue action or inaction that could result in civil or criminal penalty for iCIMS such as contempt of court.
- 14.6 *Updates.* iCIMS may update the terms of this Addendum where the changes (a) are required to comply with applicable Data Protection & Privacy Laws, applicable regulation, a court order or guidance issued by a regulator or agency; or (b) do not materially diminish the protections for Personal Data. The current version of this Addendum may be accessed through <https://www.icims.com/gc>. iCIMS provides a mechanism which may be accessed on <https://www.icims.com/gc> for Subscriber to subscribe to receive email notice of any changes to this Addendum. If Subscriber believes that updates to this Addendum materially diminish the protections for Personal Data under the Addendum, Subscriber may object to such changes and the process and time periods for a Material Adverse Change set forth in the Subscription Agreement shall apply.



14.7 *Severability.* Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended or construed as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.



## APPENDIX 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Appendix 1 includes certain details of the Processing of Subscriber Personal Data and Personal Data Processed for iCIMS Business Operations as required by Data Protection & Privacy Laws, including the information required for Annex I of the Standard Contractual Clauses, when applicable.

### A. LIST OF PARTIES

**Subscriber/Data exporter(s):** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

**Name:** The entity identified as Subscriber in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s), as applicable, and any applicable Subscriber Affiliate (to the extent authorized under the Subscription Agreement).

**Address:** The address of Subscriber specified in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s), as applicable.

**Contact person's name, position, and contact details:** The name, position, and contact details of Subscriber's contact person specified in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s), as applicable.

Activities relevant to the data processed, including the data transferred, under these Clauses:

Subscriber's/Data exporter's subscription to the iCIMS Talent Cloud products identified in the Subscription Agreement, product addenda, and iCIMS Business Operations.

**Signature and date:** The signature and date set forth in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s) shall be deemed the signature and date applicable here.

**Role (controller/processor):** Controller

**iCIMS/Data importer(s):** *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

**Name:** The entity identified as iCIMS in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s), as applicable, and any applicable iCIMS Affiliate.

**Address:** Bell Works, 101 Crawfords Corner Road, Suite 3-100, Holmdel, NJ 07733

**Contact person's name, position, and contact details:** The name, position, and contact details of iCIMS' contact person specified in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s), as applicable.

Activities relevant to the data processed, including the data transferred, under these Clauses:

Provision by data importer of the iCIMS Talent Cloud products which Process Personal Data, where such data is Subscriber Data (as defined in the Subscription Agreement and/or product addenda), upon the instruction of the Subscriber/data exporter in accordance with the terms of the Subscription Agreement, product addenda and the Addendum, and iCIMS Business Operations.



Signature and date: The signature and date set forth in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s) shall be deemed the signature and date applicable here.

Role (controller/processor): Processor (for Subscriber Personal Data), Controller (for Personal Data Processed for iCIMS Business Operations)

## **B. DESCRIPTION OF PROCESSING, INCLUDING TRANSFERS**

*Categories of data subjects whose personal data is processed, including the data transferred*

Data subjects include the Subscriber's/data exporter's Candidates and Users as those terms are defined in Section 1 of the Subscription Agreement, product addenda and/or other employees, contractors, or agents of Subscriber/data exporter.

*Categories of personal data processed, including the data transferred*

The Personal Data relating to the Subscriber's/data exporter's Candidates and Users and/or other employees, contractors, or agents of Subscriber/data exporter that is transferred to iCIMS via the Subscription or in connection with iCIMS Business Operations.

*Sensitive data processed, including the data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

Subscriber/data exporter may submit special categories of data to the Subscription (in accordance with the Subscription Agreement), the extent of which is determined and controlled by the Subscriber/data exporter in its sole discretion. If applicable, Subscriber/data exporter agrees that it has reviewed and assessed the restrictions and safeguards applied to the special categories of Personal Data, including the measures described in Appendix 2 and has determined that such restrictions and safeguards are sufficient.

*The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).*

Subscriber/data exporter transfers Personal Data to iCIMS via the Subscription on a continuous basis in accordance with the frequency of the Subscription's use by Subscriber's/data exporter's Candidates and Users. Subscriber/data exporter transfers Personal Data to iCIMS in connection with iCIMS Business Operations on a continuous basis.

*Nature of the processing*

Subscriber Personal Data will be Processed by data importer to provide the Subscription to Subscriber/data exporter in accordance with the Subscription Agreement and/or product addenda. Other Personal Data of Subscriber/data exporter will be Processed by data importer in connection with iCIMS Business Operations.

*Purpose(s) of the data transfer and further processing*

Subscriber Personal Data will be transferred and further Processed for the purposes of enabling Subscriber/data exporter to use the Subscription in accordance with the Subscription Agreement and/or product addenda. Other Personal Data of Subscriber/data exporter will be transferred and further Processed for the purposes of iCIMS Business Operations.





*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

Subscriber Personal Data is retained in accordance with any retention periods configured by Subscriber/data exporter via the Subscription, or if such retention periods are not configured, in accordance with the Subscription Agreement and/or product addenda. Other Personal Data of Subscriber/data exporter Processed for iCIMS Business Operations is retained for as long as required to provide the Subscription to Subscriber/data exporter or for as long as required for data importer's legitimate business purposes or by applicable laws and regulations, in accordance with the [iCIMS Services Privacy Notice](#).

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

Details of Sub-Processors used to provide the Subscription are available at <https://www.icims.com/subprocessors/>.

### **C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

An Coimisiún um Chosaint Sonraí / Data Protection Commission (Ireland)



## APPENDIX 2: SUBSCRIBER DATA SECURITY ADDENDUM

### TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The description of the technical and organizational measures implemented by iCIMS/the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons, to protect Subscriber Data Processed under the Subscription Agreement and/or product addenda, including Subscriber Personal Data, and Personal Data Processed for iCIMS Business Operations, are set forth in the Subscriber Data Security Addendum that may be accessed at <https://www.icims.com/gc>. iCIMS reserves the right to update the Subscriber Data Security Addendum from time to time, provided however, iCIMS shall not make changes to the Subscriber Data Security Addendum that materially diminish the protections for Subscriber Data set forth therein.



## APPENDIX 3: STANDARD CONTRACTUAL CLAUSES

### STANDARD CONTRACTUAL CLAUSES

#### 1. European Union and European Economic Area

In relation to transfers of Personal Data protected by the GDPR, the applicable Standard Contractual Clauses are the clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"). As between Subscriber and the entity identified as iCIMS in the Addendum, the Subscription Agreement, product addenda, and/or applicable Order Form(s), as applicable, and any applicable iCIMS Affiliate, the EU SCCs are completed as follows:

- a. Module One will apply where iCIMS Processes Personal Data for iCIMS Business Operations. Module Two will apply to Subscriber Personal Data. Modules Three and Four shall be deleted in their entirety;
- b. Clause 7 (optional docking clause) will apply;
- c. For Module Two, Clause 9(a), Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Section 6.2 of the Data Processing Addendum;
- d. In Clause 11(a), the optional language will apply;
- e. In Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of Ireland;
- f. In Clause 18(b), disputes shall be resolved before the courts of Ireland;
- g. Annex I of the EU SCCs shall be deemed completed with the information set out in Appendix 1 to the Data Processing Addendum, as applicable; and
- h. Annex II of the EU SCCs shall be deemed completed with the information set out in Appendix 2 to the Data Processing Addendum.

#### 2. Switzerland

In relation to transfers of Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with Section 1 above, with the following modifications:

- a. Any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;
- b. References to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and
- c. References to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland,

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA in which case the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("**Swiss SCCs**") shall instead be incorporated by reference and form an integral part of the Data Processing Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Appendix 1 and Appendix 2 to the Data Processing Addendum, as applicable.

#### 3. United Kingdom

In relation to transfers of Personal Data protected by the UK GDPR and for the purposes of localizing the EU SCCs between the Parties to UK law, the Parties agree to the following:

- a. "**IDTA**" means the International Data Transfer Agreement issued by the UK Information Commissioner's Office ("**ICO**") and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as modified by the ICO from time to time.



- b. For transfers from the UK that are not subject to an adequacy decision or exception, the Parties hereby incorporate the IDTA by reference and, by signing this Data Processing Addendum, also enter into and agree to be bound by the Mandatory Clauses of the IDTA.
- c. Pursuant to Sections 5.2 and 5.3 of the IDTA, the Parties agree that the following information is relevant to Tables 1 – 4 of the IDTA and that by changing the format and content of the Tables neither Party intends to reduce the Appropriate Safeguards (as defined in the IDTA).
  - i. Table 1: The Parties' details, key contacts, data subject contacts, and signatures are in Appendix 1 to the Data Processing Addendum, as applicable.
  - ii. Table 2:
    - (a) The UK country's law that governs the IDTA is: England and Wales.
    - (b) The primary place for legal claims to be made by the Parties is: England and Wales.
    - (c) The statuses of the Data Exporter and Data Importer are described in Appendix 1 to the Data Processing Addendum.
    - (d) The Data Importer represents and warrants that the UK GDPR does apply to its Processing of Personal Data under the Subscription Agreement and for iCIMS Business Operations.
    - (e) The relationship among the agreements setting forth data protection terms among the Parties is described in the Addendum and the Subscription Agreement and/or product addenda.
    - (f) The duration that the Parties may Process Personal Data is the period for which the Subscription Agreement and/or product addenda is in force and for no longer than is necessary for iCIMS Business Operations.
    - (g) The IDTA is coterminous with the Addendum. Neither Party may terminate the IDTA before the Addendum ends unless one of the Parties breaches the IDTA or the Parties agree in writing.
    - (h) The Data Importer may transfer Personal Data to another organization or person (who is a different legal entity) if such transfer complies with the Subscription Agreement, the Addendum, and the IDTA's applicable Mandatory Clauses.
    - (i) The Data Importer may only forward Personal Data to its Sub-Processors as specified in the Subscription Agreement and the Addendum. No specific restrictions other than any restrictions that apply under the Subscription Agreement and the Addendum apply to such onward transfers.
    - (j) The Parties will review the Security Requirements listed in Table 4, and the extra protection clauses (if any), to this Addendum each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment.
  - iii. Table 3: The categories of Personal Data, special categories of Personal Data, Data Subjects, and purposes of Processing are described in Appendix 1 to the Data Processing Addendum, as applicable. The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.
  - iv. Table 4: The security measures adopted by the Parties are described in Appendix 2 to the Data Processing Addendum, as updated from time-to-time by the Data Importer in compliance with the terms set forth in the Subscription Agreement and the Addendum. The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.
- d. Pursuant to Part 2 (Extra Protection Clauses) of the IDTA, the Parties agree that Data Importer will adopt the technical and organizational measures set forth in Appendix 2 to the Data Processing Addendum.



#### 4. **Other International Transfers of Personal Data**

If: (i) the Standard Contractual Clauses are recognized under applicable Data Protection & Privacy Laws as an adequacy mechanism or other comparable instrument for the transfer of Personal Data originating in any country outside of the EEA, Switzerland, and UK (each an “**Additional Country**”); and (ii) iCIMS or its Sub-Processor(s) Process Personal Data originating from an Additional Country in a country that has not been found to provide an adequate level of protection under applicable Data Protection & Privacy Laws of such Additional Country, then the Parties agree that this Addendum (including its Appendices) shall also apply *mutatis mutandis* to iCIMS’ Processing of such Personal Data. Where applicable, references to EU Member State law or EU supervisory authorities in the EEA and Swiss Controller to Processor Standard Contractual Clauses shall be modified to include the appropriate reference to the Additional Country’s applicable Data Protection & Privacy Laws and supervisory authorities.





## Subscriber Data Security Addendum

The obligations in this Subscriber Data Security Addendum (“**Security Addendum**”) provide details about and are a part of iCIMS’ technical and organizational measures to protect Subscriber Data (including Subscriber Personal Data) and Personal Data processed for iCIMS Business Operations (collectively, “**Protected Data**”) that are processed pursuant to or in connection with the Subscription Agreement and Data Processing Addendum, and for assisting Subscriber Group Members with fulfilling their obligations to respond to Data Subjects’ requests for exercise of their rights under Data Protection & Privacy Laws. iCIMS maintains a comprehensive set of policies and processes related to information security and privacy that comply with the ISO 27001, ISO 27701, & SOC2 standards. The following identifies key controls used to protect Protected Data.

Unless otherwise defined below, all capitalized terms have the meaning given to them in the Subscription Agreement (“**Subscription Agreement**”) and/or Data Processing Addendum (“**Data Processing Addendum**”) between iCIMS and Subscriber. Any examples in this Security Addendum are illustrative and not the sole examples of a particular concept.

### **1. Measures of anonymization/pseudonymization and encryption of Protected Data**

All Protected Data shall be encrypted at rest and in transit by iCIMS or the iCIMS platform across any public network, using industry-standard measures.

- a. Protected Data at rest: Shall use at least the AES 256-bit or stronger for encryption. Data at rest includes Backups, as defined in iCIMS’ [Support & Maintenance Policy](#).
- b. Protected Data in transit: Shall use TLS 1.2 or better for encryption.
- c. Hashed data: Hashed data shall use bcrypt or stronger (as aligned to industry standards, including File Intrusion Prevention Systems (FIPS) approved and/or NIST recommended algorithms).
- d. Key exchange and digital signatures:
  - i. Key exchange shall use RSA, DH, or stronger cryptographic algorithms with a minimum key length of 2048 bits.
  - ii. Digital signatures shall use specifications defined in the DSS with a minimum key length of 2048 bits and minimum digest length of 256.
- e. Anonymization and pseudonymization: iCIMS has an internal data analytics policy that requires iCIMS to use some or all of the following safeguards and techniques to render Subscriber Personal Data anonymous, de-identified, and/or non-personal, as applicable:
  - i. Suppression - removes the identifying values from a record (e.g., removing the first and last name from a record).
  - ii. Generalization - replaces a data element with a more general element (e.g., removing the day and month from a birthdate and leaving only the year).
  - iii. Noise Addition - replaces actual data values with other values that are selected from the same class of data (e.g., the actual data may be salted to create a new value, where the salt value would be considered the addition of noise).
  - iv. Differential Privacy - requires the use of the k-anonymity method to ensure that within a dataset there are at least k individuals or customers who have exactly the same values for data elements that might become identifying for each individual or customer. iCIMS’ policy requires a minimum value of k=20, which is consistent with current practices for public data release from other highly conservative organizations.
  - v. Outlier Removal - removes all outliers to minimize the extent to which those outliers allow for reidentification of an individual or customer.



## 2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- a. Background checks: Where required and/or permitted by applicable law, iCIMS shall conduct a preemployment background and/or criminal records check on all new hires. Employment at iCIMS is contingent upon a satisfactory background and/or criminal records check, including where applicable:
  - i. Social Security number, National Insurance number, Personal Public Service number, or other national identification number.
  - ii. Education.
  - iii. Work Experience.
  - iv. Criminal Background Check.
  - v. Credit Check, if relevant to the position.
  - vi. Reference Check.
  - vii. Where required and/or permitted by applicable law, iCIMS may also conduct background and/or criminal records checks on its employees throughout the course of their employment. Generally, this shall occur in circumstances involving transfer to a position of high-level security or responsibility.
- b. Ongoing confidentiality: Confidentiality obligations as specified in the Subscription Agreement.
- c. Security and privacy training: During onboarding and at least once per calendar year thereafter, iCIMS shall require all iCIMS personnel with access to Protected Data to complete training on iCIMS' information security and privacy policies.

## 3. Measures for ensuring the ability to restore the availability and access to Subscriber Data in a timely manner in the event of a physical or technical incident

- a. Incident Management: iCIMS has in place an incident response policy and process to be followed in the event of any security or privacy incident, including any Personal Data Breach. iCIMS' incident response policy and process includes:
  - i. Roles and responsibilities: Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to security or privacy incidents, including formation of a security or privacy incident response team (SIRT) with an incident response leader.
  - ii. Incident Response Process: Based on NIST 800-61 Rev.2, includes:
    1. Preparation: Establish an incident response capability aimed at preventing incidents by ensuring effective control frameworks and compliance.
    2. Detection & Analysis: Identify security or privacy event(s) and determine potential impact to iCIMS and subscribers.

After consulting with iCIMS leadership and when warranted or required by judicial action, applicable law, regulation, or like jurisdictional requirement, iCIMS shall use reasonable efforts to provide notice to applicable iCIMS personnel and/or affected subscribers about a security or privacy incident. Additionally, notification is required within 24 hours of identification of a confirmed Personal Data Breach or Abnormal Activities. "**Abnormal Activities**" means unsuccessful attacks that appear particularly significant based on iCIMS' understanding of the risks it faces.



3. Containment Eradication & Recovery: Mitigate the root cause of the security or privacy incident to prevent further damage or exposure. Remove vulnerabilities causing the security or privacy incident, and any associated compromises. Restore the affected system(s) to operation after the issues that gave rise to the security or privacy incident, and the consequences of the security or privacy incident, have been corrected.
4. Post-incident Activities: Address notification and communication requirements, cooperate with external parties, information sharing, follow-up lessons learned, record keeping, and improvements.

b. Disaster recovery and business continuity: As specified in iCIMS' [Support & Maintenance Policy](#).

#### 4. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing

a. Access controls:

i. iCIMS shall:

1. Follow the principles of least privilege through a role-based access control model when granting iCIMS personnel access to Protected Data.
2. Limit access to Protected Data to iCIMS personnel with a legitimate need to access Protected Data to provide the services in accordance with the Subscription Agreement.
3. Periodically (no less than quarterly) review iCIMS personnel's access to Protected Data.
4. Promptly terminate an iCIMS personnel's access to Protected Data if such individual's access is no longer required.
5. Review and disable user accounts after 90 days of inactivity.

b. Network controls: Access to internal and external network services that contain Protected Data shall be controlled through a combination of the following types of controls:

- i. Network access control lists (NACLs), or equivalent.
- ii. Firewall policies, or equivalent.
- iii. Security groups, or equivalent.
- iv. IP whitelists, or equivalent.
- v. A multi-tier architecture that prevents direct access to data stores from the internet.
- vi. Usage of role-based access controls (RBAC) shall be implemented to ensure appropriate access to networks.
- vii. Two-factor or multi-factor authentication (TFA or MFA) for remote access shall be implemented.

c. Vulnerability management and patch management: iCIMS shall implement and maintain a vulnerability management program designed to identify and remediate vulnerabilities affecting production networks, systems, and applications that store or process Protected Data. The program shall include:

- i. Penetration tests, conducted by an accredited third party selected by iCIMS, of iCIMS products and infrastructure that contain Protected Data occur at least once per calendar year. Upon Subscriber's reasonable written request, iCIMS shall provide Subscriber an executive attestation of the test results. Subscriber shall treat such information as iCIMS' confidential information in accordance with 'Section 7 - Confidential Information' of the Subscription Agreement.
- ii. Routine vulnerability scans on all iCIMS products and infrastructure that contain Protected Data or that are used by iCIMS to gain access to Protected Data.
- iii. If vulnerabilities are detected from such tests and scans, iCIMS shall remediate and apply applicable and necessary patches as follows:
  1. Server operating systems shall be patched within 30 days of a critical and/or security patch release.



2. Workstations and Laptops shall be patched within 30 days of a critical and/or security patch release.
  3. Network devices shall be patched within 30 days of a critical and or security patch release.
  4. Zero-day patches shall be applied on all systems containing Protected Data and critical systems within 14 days, and all other systems within 30 days.
  5. Patches shall be tested prior to rollout in the production environment. Less critical systems shall be patched first.
  6. Application patches shall be applied in accordance with iCIMS' [Support & Maintenance Policy](#).
- d. iCIMS Software Development Practices: With respect to the software development lifecycle, iCIMS shall maintain and follow a written software development life cycle program based on the Open Web Application Security Project (OWASP) Top 10 standards.

Assigned iCIMS personnel who are responsible for secure application design, development, configuration, testing, and deployment receive appropriate training regarding iCIMS' secure application development practices. Development practices shall include:

- i. Managing all code through a version control system to allow viewing of change history and content.
  - ii. Ensuring agile teams are performing testing using a multi-phase quality assurance release cycle that includes security testing.
  - iii. Delivering security fixes and improvements aligning to a pre-determined schedule based on identified severity levels.
  - iv. Performing source code vulnerability scanning in the CI/CD pipeline and conduct risk appropriate remediation activities based on business impact and subsequent prioritization of the findings prior to software release as appropriate to the priority.
  - v. Ensuring that software is released only via production managed change control processes, with no access or involvement by the development and test teams
  - vi. Conducting awareness training regarding secure coding at least once per calendar year.
- e. Malware controls: iCIMS shall install and maintain reasonable and current controls designed to protect the networks, systems, and devices used by iCIMS to access Protected Data from malware and unauthorized software.
- f. Security and privacy assessments: Upon written request of Subscriber no more than once in any twelve (12) month period, the Subscriber may reassess iCIMS' information security and privacy program. iCIMS agrees to provide reasonable cooperation with respect to any such assessment by providing reasonable and appropriate documentation; provided, however, responses to assessment requests may take up to forty-five (45) days for iCIMS to complete. Assessments described in this Section: (i) should not be considered an audit, and as such, iCIMS may not provide information that is customarily provided in an audit; and (ii) do not include and shall not permit Subscriber to conduct vulnerability/penetration tests.
- g. Security certification and attestation: See Section 12 of this Security Addendum.

## 5. Measures of user identification and authorization

- a. Access control: iCIMS personnel shall:
- i. Establish process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.
  - ii. Ensure that administrators shall only log into systems with user IDs attributable to them or follow processes that would not break attribution.
  - iii. Ensure that access to databases containing Protected Data shall always be authenticated.
  - iv. Ensure all logins to the Subscription are secured through an encrypted connection (e.g., HTTPS) and appropriately authenticated.



- v. Ensure that the Principle of Least Privilege using role-based access control (RBAC) is followed for all users. “**Principal of Least Privilege**” means restricting access to systems and data based on job role or function while ensuring that no additional, unneeded access is granted.
- vi. Control addition, deletion, and modification of usernames, credentials, and other identifier objects.
- vii. Ensure users (including temps, consultants, and contractors) formally request access to systems with only the rights necessary to perform their job functions.
- viii. Ensure that a manager or above and the system owner formally approve user roles and access requests. System administrators shall act as the final gatekeeper to ensure access is granted appropriate to the identified role.
- ix. Conduct periodic review of users’ access and access rights to ensure that they are appropriate for the users’ role.
- x. Use two-factor authentication (TFA) or multi-factor authentication (MFA) for any services remotely accessible by iCIMS personnel and/or authorized third parties
- b. Intrusion detection and performance assurance: iCIMS shall monitor production networks, systems, and applications that store or process Protected Data for unauthorized access using traffic and activity-based monitoring systems.
- c. Passwords: iCIMS will manage passwords in alignment with NIST 800-63b standards, for iCIMS managed digital identity at iCIMS.
- d. See Section 9.a.v of this Security Addendum for alerting and monitoring.

## 6. Measures for the protection of Protected Data during transmission

- a. Encryption: As specified in Section 1 of this Security Addendum.

## 7. Measures for the protection of data during storage

- a. Encryption: As specified in Section 1 of this Security Addendum.
- b. Data segregation: iCIMS shall keep Subscriber Data at a minimum logically segregated from data belonging to iCIMS’ other subscribers and shall implement measures and controls designed to ensure that Subscriber Data is not accessible by iCIMS’ other subscribers.

## 8. Measures for ensuring physical security of locations at which Protected Data are processed

- a. Data center security: iCIMS uses data centers operated by third parties, for example Amazon Web Services, to provide the Subscription and, requires such third parties to maintain controls that provide reasonable assurance that access to physical servers at the data center is limited to authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:
  - i. Logging and monitoring of all authorized and unauthorized access attempts to the data center by the data center security personnel.
  - ii. Camera surveillance systems at critical internal and external entry points to the data center.
  - iii. Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment.
  - iv. Uninterruptible Power Supply (UPS) modules and backup generators, including fuel delivery services that provide back-up power in the event of a power failure.
  - v. Consideration taken to ensure environmental concerns are addressed such as fire, flood, and natural disaster.
  - vi. All on-site visitors (to iCIMS site locations) shall always be accompanied by iCIMS personnel.



- vii. Requirement that data centers perform SOC 2 or equivalent audits on an annual basis while remediating any findings in a reasonable timeframe.

## 9. Measures for ensuring events logging

- a. Auditing, logging, and monitoring controls: iCIMS shall implement and maintain measures designed to secure, control, and monitor iCIMS' networks, systems, and applications that process or store Protected Data, including:
  - i. Firewalls and related technology and authentication controls.
  - ii. Intrusion detection or prevention systems to monitor associated networks
  - iii. A centralized logging system (including security information and event management (SIEM)) controlled by iCIMS information security team, with log retention of one year.
  - iv. Secure, protected audit trails that cannot be modified.
  - v. Monitoring and alerting systems used to record login attempts/failures, successful logins and changes made to systems with associated alerting in place.
  - vi. Monitoring of all external ingress/egress connections.
  - vii. Anti-virus/anti-malware protection for iCIMS managed assets.

## 10. Measures for ensuring system configuration, including default configuration

- a. Change and configuration management: iCIMS maintains policies and procedures for managing changes to iCIMS' production systems, applications, and databases which process Protected Data. Such policies and procedures include:
  - i. Processes for documenting, testing, and approving the promotion of changes into production.
  - ii. A security patching process that requires patching systems in a timely manner based on a risk analysis.
  - iii. A process for iCIMS to perform security assessments of changes into production.
  - iv. Hardening standards based on industry best practice (e.g., Center for Internet Security standards)
  - v. A vulnerability management program to audit and verify appropriate configuration (See Section 4.b of this Security Addendum).
  - vi. Mobile device management policies and processes to ensure devices shall comply with iCIMS internal acceptable use policy, employee handbook, and information security policies if used to access Protected Data.

## 11. Measures for internal IT and IT security governance and management

- a. Governance: iCIMS shall designate one or more employees to maintain iCIMS' information security program.
  - i. iCIMS' senior leadership shall review and approve any material changes to the information security program.
  - ii. iCIMS shall review the information security program at least once per calendar year or upon a material change in iCIMS' business practices.
- b. Information security measures: As specified in the "Data Security" section of iCIMS' [Support & Maintenance Policy](#).
- c. Modifications: iCIMS may modify its security controls and processes from time to time, so long as such modifications:
  - i. Do not materially reduce the overall level of protection afforded by iCIMS to Subscriber.
  - ii. Where applicable, are consistent with iCIMS' then current SOC-2 statement.
  - iii. Where applicable, remain compliant with the ISO 27001 and ISO 27701 standards.

## 12. Measures for certification/assurance of processes and products





- a. Security certifications, audits, and attestations: iCIMS shall maintain the following industry standard certifications, audits, and attestations:
  - i. ISO 27001 certification, or equivalent, ensuring that iCIMS information security management system (ISMS) continues to perform in alignment with the standard, for the processing of Subscriber Data.
  - ii. ISO 27701 certification, or equivalent, ensuring that iCIMS privacy information management system (PIMS) continues to perform in alignment with the standard, for the processing of Subscriber Data.
  - iii. SOC 2, Type II attestation, ensuring that internal controls provided by iCIMS meet American Institute of Certified Public Accountants (AICPA) standards (i.e., SSAE-19, TPS-100), for the processing of Subscriber Data.
  - iv. Penetration testing attestations regarding the performance, findings, and remediation resulting from internal and external penetration tests.

### 13. Measures for ensuring data minimization

- a. Subscriber Data: Subscribers control the nature and scope of the Subscriber Data that is transferred to iCIMS via the Subscription. The subject matter, duration, nature, purpose of the Processing of the Subscriber Personal Data, as well as the types of Subscriber Personal Data and categories of Data Subjects, are set out in the Subscription Agreement and the Data Processing Addendum. iCIMS' access to Subscriber Personal Data is strictly limited to those individuals who need to know/access the relevant Subscriber Personal Data, as strictly necessary for the purposes of the Subscription Agreement and to comply with Data Protection & Privacy Laws. Subscriber Personal Data is retained in accordance with any retention periods configured by Subscriber via the Subscription, or if such retention periods are not configured, in accordance with the Subscription Agreement. Where applicable (such as data analytics), the level of detail used for the Processing of Subscriber Personal Data is limited as described in Section 1.e of this Security Addendum.
- b. Personal Data Processed for iCIMS Business Operations: Personal Data processed for iCIMS Business Operations is limited to the context of data generated to assist in iCIMS Business Operations incident to administration and delivery of the Subscription. iCIMS' access to Personal Data processed for iCIMS Business Operations is limited to those individuals and teams who need to know / access the relevant data, as necessary for iCIMS' legitimate business operations incident to administration and delivery of the Subscription to Subscriber, and for its other legitimate purposes relating to iCIMS' business operations. iCIMS will only process such Personal Data for the purposes that are compatible with those contained in the definition of iCIMS Business Operations and not use the Personal Data for any other purpose. Personal Data processed for iCIMS Business Operations is retained in accordance with iCIMS' documented data storage and retention policies and procedures.

### 14. Measures for ensuring data quality

- a. Measures for ensuring data quality: The requirements for the conditions, scenarios, and responsibilities for processing Subscriber Data are specified in the Data Processing Addendum and the "Subscriber Data" section of the Subscription Agreement. The process for the exercise of data subject rights is specified in the Data Processing Addendum.

### 15. Measures for ensuring limited data retention

- a. Deletion after termination or expiration of the Subscription: Unless specified otherwise in the Data Processing Addendum or Subscription Agreement, Subscriber Data in iCIMS' possession or under its control shall be deleted within thirty (30) days after termination or expiration of the Subscription and, with respect to Backups, no more than twelve (12) months after the month in which the Subscription Agreement terminates or expires.



- b. Data destruction: Media containing Subscriber Personal Data shall be disposed of so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing, or overwriting.
  - i. Subscriber Personal Data in iCIMS' possession or under its control shall be deleted using techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization"), where possible.
  - ii. iCIMS shall certify the destruction of Subscriber Personal Data by issuing a certificate of destruction, upon Subscriber's written request.
  - iii. Certificates of destruction shall be maintained for at least one year.
- c. Retrieval of Subscriber Data: As specified in the Data Processing Addendum and Subscription Agreement.

#### 16. Measures for ensuring accountability

- a. Governance: iCIMS shall designate one or more employees to maintain iCIMS' privacy program.
  - i. iCIMS' senior leadership shall review and approve any material changes to the privacy program.
  - ii. iCIMS shall review the privacy program at least once per calendar year or upon a material change in iCIMS' business practices and/or Data Protection & Privacy Laws.
- b. Liability for acts, errors, and omissions of sub-processors: As specified in the Data Processing Addendum and the Subscription Agreement.
- c. Disciplinary policy: iCIMS shall maintain and enforce a disciplinary policy for violations of iCIMS' information security and privacy programs by iCIMS personnel.
- d. Vendor Audit: iCIMS maintains a review process for vendors that process Protected Data.

#### 17. Measures for allowing data portability and ensuring erasure

- a. Storage on portable devices: iCIMS shall not store any Subscriber Data on portable devices or removable media, including laptops, smartphones, and tablets, without Subscriber's prior written approval.
- b. Data subject rights of erasure and portability: The process for the exercise of data subject rights is specified in the Data Processing Addendum.

#### 18. Applied restrictions or safeguards for sensitive data (if applicable)

- a. To provide data confidentiality in the event of accidental or malicious data loss, all Protected Data that includes sensitive data shall be encrypted at rest and in transit (See Section 1 of this Security Addendum).



## SUPPORT & MAINTENANCE POLICY

This Support & Maintenance Policy (“SMP”) is part of the Subscription Agreement by and between Subscriber and iCIMS (“Agreement”). In the event of a conflict between the SMP and the Agreement, unless otherwise expressly provided, the Agreement will control. All capitalized terms not defined herein have the meaning ascribed to them in the then-current Subscription Agreement found at [www.icims.com/gc](http://www.icims.com/gc). This SMP applies to the support and maintenance practices for the Subscription once implementation for such Subscription is completed.

Support and maintenance practices specific to Power-Ups are set forth in our then current Power-Up Support & Maintenance Policy, incorporated into this SMP by reference and available at [www.icims.com/gc](http://www.icims.com/gc).

### Definitions

- **“Backup”** means an encrypted backup of the servers, including Subscriber Data, log files, configurations, and any control files required to restore Subscriber’s configuration of the Subscription in the event of a Disaster.
- **“Demarcation Point”** means iCIMS’ border router which is used to establish connectivity from the Hosted Environment to the public Internet.
- **“Disaster”** means any act of nature (e.g., fire, earthquake, natural disaster), act of government (e.g., war, terrorism, embargo), or any other act or circumstance that is beyond the reasonable control of iCIMS that results in partial or total failure or destruction of computer hardware, communications capabilities, or facilities of the Hosted Environment.
- **“Hosted Environment”** means the hosted locations of the iCIMS applications, networks, and servers supporting the Subscription. Specific details regarding the Hosted Environment are available at [www.icims.com/gc-it](http://www.icims.com/gc-it).
- **“Issue”** means a condition that inhibits the use and/or performance of the Subscription, including, but not limited to, an event that results in performance degradation, function unavailability, errors, security exposure, or other defects, such that the Subscription, taken as a whole, does not operate substantially as described in the Documentation.
- **“Maintenance Period”** means the time period during which the Subscription may not be available because of required system maintenance, upgrades, and other Hosted Environment requirements.
- **“Normal Business Hours”** means 24x5 (9:00 PM ET Sunday – 9:00 PM ET Friday; 2:00 AM GMT Monday – 2:00 AM GMT Saturday), excluding iCIMS recognized holidays.<sup>1</sup>
- **“Other Support Request”** means (i) a request to change to an existing configuration, (ii) a question regarding usability, Documentation, training, or another knowledge enhancement question; (iii) an enhancement request; or (iv) any other incidental matter that delays Subscriber from completing business functions that are not critical to Subscriber’s business and for which there is a work-around or alternative solution.
- **“Resolution”** means one of the following:
  - A correct answer to the question regarding the configuration, use, and/or operation of the Subscription;
  - A configuration change consistent with the Subscription Documentation that substantially meets the request;
  - A patch, correction, or bug fix such that the Subscription substantially conforms to its Documentation; or
  - Notice that an Issue is caused by a non-iCIMS provided product or service.

---

<sup>1</sup> ET – Eastern Time; GMT – Greenwich Mean Time. Please note that all business hours are iCIMS’ local business hours for the regional help desk, subject to local holidays. A listing of iCIMS’ recognized local holidays for an applicable year is available on the iCIMS Community at [iCIMS Holiday Schedule](#).

- “Subscription Availability”** means the availability of the Subscription at the Demarcation Point for use by Subscriber without a Severity 1 Issue, 24 hours per day, 7 days per week, 365 days per year (24x7x365) less the Maintenance Period and Recovery Time Objective, and represents the combined availability of networks and servers supporting the Subscription.
- “System Administrator(s)”** are Users the Subscriber designates as primary liaisons between Subscriber and iCIMS for technical support who act as primary system administrator(s) and shall have the ability to make system wide changes to workflow, reporting, login groups and user privileges.
- “Updates”** means updates, enhancements, revisions, fixes, patches, or other changes to the Subscription that iCIMS makes generally available to all Subscribers with an active Subscription but does not include additional modules or components and other applications separately sold under an Order Form. Each Update is deemed a part of the Subscription once placed in a production environment. For clarity, an Update does not include a release of an upgraded version of a module, component, and/or application that may be available at an additional fee sold under an Order Form.
- “Uptime Percentage”** means 99.9%.

**Support**

Subscriber shall designate and maintain at least one (1) System Administrator for all support Issues under this Agreement. A secondary System Administrator may also be designated by Subscriber. Additional System Administrators per Subscription may be considered upon request, which iCIMS may grant in its sole and reasonable discretion. All support Issues must be submitted by a System Administrator via the iCIMS Community at: <https://community.icims.com/>. System Administrators can also utilize the iCIMS product suite links provided in the platform which will direct the System Administrator to the iCIMS Community and allow the System Administrator to submit support cases, view past support cases, and access the iCIMS Knowledge Base for training, tips & tricks, and FAQs. Subscriber shall notify iCIMS to request the transfer of System Administrator designation to another User by contacting their Account Team or submitting a case through the iCIMS Community.

**Hosting**

Subscription Availability, measured on a calendar month basis, will be greater than or equal to the Uptime Percentage. Notwithstanding Subscriber/User-side network issues, the Subscription will respond to User requests in an average of less than one (1) second.

In support of the foregoing performance standards, iCIMS is connected to the internet backbone via multiple ultra-high-speed fiber optic connections. State-of-the-art routers provide autonomous load-balancing and fail-over. These routers are configured to instantly fail over if any given connection goes down. Each connection follows a different path to the internet backbone, such that the route automatically fails over to the best available connection.

**Issues**

When a designated System Administrator is submitting a case, the following information must be provided:

- Subscriber name, System Administrator name, email address, and telephone number (including area code);
- Information about the nature of the Issue;
- Information about the location of the Issue;
- Any Subscription error messages associated with the Issue and the steps leading up to the Issue occurrence;
- Detailed description of the Issue; and
- Business impact of the Issue.

In the event iCIMS becomes aware and/or Subscriber notifies iCIMS of an Issue, iCIMS shall address the Issue based on its severity level, which is determined by iCIMS in its sole and reasonable discretion. iCIMS shall use commercially reasonable efforts to respond to Subscriber within the timeframe specified for the respective severity level, acknowledging receipt of the Issue notification and the status of an initial action plan to accomplish Issue Resolution. iCIMS shall use commercially reasonable efforts, in light of the severity and complexity of the Issue, to provide an Issue Resolution within the time frames specified for the respective severity level.

**Severity Definitions and Response Times<sup>2</sup>**

These times reflect the targeted time period between iCIMS’ technical support team receiving notice of the Issue or Other Support Request through Subscriber’s submission of a case via the iCIMS Community to the initial response and Resolution, respectively, by iCIMS.

Severity	Definition	Initial Response	Status Update	Escalation (as set forth in the table below)	Work Around (if available)	Resolution
Severity 1	Any Issue that (i) compromises the integrity or security of the Subscription or Subscriber Data, or (ii) completely prevents the operation of the Subscription or precludes work by Users from reasonably continuing, and for which there is no reasonable work-around.	Thirty (30) Minutes	Every Hour	To the Highest Escalation Contact Within Eight (8) Hours	Four (4) Hours	One (1) Day
Severity 2	Any Issue that (i) substantially restricts the operations of the Subscription, but for which an alternative solution or work-around exists, or (ii) does not substantially restrict the operations of the Subscription, but for which an alternative solution or work-around does not exist.	Two (2) Hours	Every Day	To the Next Escalation Contact on a Daily Basis	One (1) Day	One (1) Week
Severity 3	Any Issue that does not substantially restrict the operations of the Subscription and for which there is an alternative solution or work-around.	Eight (8) Hours	Every Week	To the Next Escalation Contact on a Quarterly Basis	N/A	Next Update <sup>3</sup>
Severity 4	Any Other Support Request	Twenty-Four (24) Hours	As Deemed Practical	N/A	N/A	As Deemed Practical

**Escalation & Prevention**

In the event of an escalation, iCIMS’ internal escalation contacts are as follows:

Level	Role
1 <sup>st</sup> Level	Manager within Customer Service
2 <sup>nd</sup> Level	Manager within Labs – Engineering, Director within Customer Service, and/or Manager within Cloud Hosting (as applicable)
3 <sup>rd</sup> Level	Director/VP within Labs – Engineering, and/or Director/VP, Cloud Hosting (as applicable)
4 <sup>th</sup> Level	VP, Services and/or Chief Technology Officer (as applicable)

<sup>2</sup> Notification of an Issue to iCIMS’ through Subscriber’s submission of a case via the iCIMS Community are deemed to be “received” by iCIMS at the beginning of the next business hour.

<sup>3</sup> “Next Update” may include, but does not require, minor updates, enhancements, revisions, fixes, patches or other changes to the Subscription that iCIMS makes generally available to all Subscribers with an active Subscription. For clarity, minor updates will be designated through changes in the decimal of the previous version.

### **Reporting**

For all Severity 1 Issues, iCIMS shall, upon request, make available to the System Administrator an Issue report within five (5) business days after an investigation into the Issue has been concluded, which may include the actions taken by iCIMS to achieve Issue Resolution, the response time, and the resolution time. iCIMS shall retain Issue reports for at least one (1) month for later reference by the System Administrator.

### **Maintenance**

iCIMS furnishes Updates that include Issue Resolutions promptly after availability of the Issue Resolution. Updates that include enhancements or other improvements are typically provided within thirty (30) days following general availability of such Update.

### **Data Security**

The servers and network supporting the Subscription are located in the Hosted Environment which is secured by 24x7x365 security, controlled ingress and egress to registered parties only, and multiple layers of logical security via firewalls, router management, and User passwords. Specific details regarding the Hosted Environment are available at <https://www.icims.com/gc-it>. Further, iCIMS makes use of clustering, load-balancing, and fail-over technologies on the servers supporting the Subscription. All servers are configured with redundant storage solutions.

The Subscription uses authentication and authorization mechanisms, including the use of access control lists, to ensure that Subscriber Data can only be accessed by Users who have been so authorized by Subscriber. The recommended Subscription configuration utilizes encryption in transit, Subscriber authentication and authorization, and encryption at rest. iCIMS uses commercially available software, and other tools to reasonably maintain security of the Subscription.

iCIMS monitors its systems 24x7x365 through a combination of third-party and proprietary tools to provide early detection and notification of potential Issues, with on-call technical personnel available to prevent Issues or correct an Issue quickly if it arises.

iCIMS conducts a Backup at least daily and prior to any Update to the Subscription. iCIMS maintains seven (7) days of encrypted daily Backups with high availability and transfers encrypted Backups to a secured storage location daily. iCIMS also sends encrypted transaction logs to its disaster recovery facilities throughout the day. iCIMS maintains encrypted Backups for approximately one (1) year.

### **Backup & Disaster Recovery**

iCIMS maintains a comprehensive disaster recovery plan to help ensure availability of Subscriber Data in the event of a Disaster. iCIMS tests this recovery plan annually. The majority of iCIMS technical infrastructure has been architected for the cloud and leverages best practices such as high availability and replication of services across multiple locations.

iCIMS' Hosted Environment provides first-level protection for disaster recovery through redundancy at all levels of the operation. Specific details regarding the Hosted Environment are available at <https://www.icims.com/gc-it>.

iCIMS makes use of clustering, load-balancing, and failover technologies within its architecture. This serves to help minimize any noticeable impact as a result of the failure of a specific server. The majority of iCIMS' technical infrastructure has been architected for the cloud and leverages best practices such as high availability and replication of services across multiple locations.

In the event of a Disaster, iCIMS shall use commercially reasonable efforts to re-establish access to the Subscription within twenty-four (24) hours ("**Recovery Time Objective**") utilizing the most recent Backups. Actual recovery times will vary based on the nature and extent of the Disaster. iCIMS shall use commercially reasonable efforts to recover Subscriber Data from a Backup made less than or equal to twenty-four (24) hours prior to the Disaster (the "**Recovery Point Objective**").

In the event of a partial Disaster, iCIMS and/or iCIMS' managed service provider will be notified of the Disaster and will take steps to address any affected infrastructure/service or hardware, if applicable. Should a partial Disaster affect any component of iCIMS' cloud infrastructure, iCIMS technical personnel will be notified by internal and external monitoring software. iCIMS technical personnel will review the affected infrastructure/service and will take necessary action. Should a partial Disaster affect one of iCIMS' Hosted Environments, iCIMS will be notified by Hosted Environment personnel as to the arrangements being made to replace or fix the affected system. The clustering, load-balancing, and fail-over technologies used by iCIMS help to mitigate certain noticeable effects that certain partial Disasters might have otherwise had on the Subscription. In certain situations, the Subscription will remain fully functional while the partial Disaster is addressed.

In the event of a complete Disaster (e.g., earthquakes, explosions, fires, other natural disasters that result in physical destruction of the Hosted Environment), iCIMS will be notified by the managed service provider as to the extent of the Disaster. Based on this information, iCIMS will initiate rebuilding the infrastructure in the appropriate disaster recovery environment. Subscriber Data will then be restored from Backups, as necessary. Once the systems are back online, iCIMS will conduct testing to ensure everything was properly recovered to the expected state.



**Remedy**

It is iCIMS' practice to review the root cause, response times, and Issue Resolutions for all Severity Level 1 and 2 Issues and develop preventative measures, as appropriate. Accordingly, in the event iCIMS fails to meet any obligation in this Policy (a "**Service Level Obligation Failure**" or "**SLO Failure**"), iCIMS shall use commercially reasonable efforts to promptly correct and further prevent such SLO Failure. In the event of an SLO Failure extending for, and for which the underlying Issue has not been resolved, within sixty (60) consecutive days or for any one-hundred and twenty (120) days in any three hundred and sixty (360) day period, Subscriber will have the right upon prior written notice to iCIMS, as its sole and exclusive remedy for such breach, to terminate the specific Subscriptions (i.e., the particular product(s), offering(s), portal(s), module(s), line item(s) to which such SLO Failure pertains) ("**Affected Subscription**") for convenience and receive a refund of any pre-paid, but unused amounts specific to the Affected Subscription.



## ACCEPTABLE USE POLICY

This Acceptable Use Policy (the “**Acceptable Use Policy**”) is part of the Subscription Agreement by and between Subscriber and iCIMS, Inc. (the “**Agreement**”). In the event of a conflict between this Acceptable Use Policy and the Agreement, unless otherwise expressly provided, the Agreement will control. All capitalized terms not defined herein have the meaning ascribed to them in the then-current Subscription Agreement found at <https://icims.com/gc/>.

### 1. Proper Use

Subscriber shall, and shall ensure that its Users, comply with this Acceptable Use Policy, the Agreement and all Documentation. iCIMS may deny Subscriber or any User use of the Subscription as may be required by iCIMS to effectuate its rights and obligations under or otherwise enforce this Acceptable Use Policy or the Agreement. iCIMS shall use commercially reasonable efforts to give Subscriber advance notice of any denial of such use, if practicable and not injurious to the legitimate commercial interests of iCIMS and its Affiliates. iCIMS shall not be responsible or liable for any use of the Subscription by the Subscriber, its Affiliates or Users that violates the terms of this Acceptable Use Policy.

### 2. Restrictions

Subscriber understands, acknowledges and agrees that it shall not, except as otherwise set forth in Agreement or expressly agreed to by iCIMS in writing: (i) copy or reproduce any Subscription in any form or medium; (ii) modify, reverse engineer, decompile, adapt, restructure, rearrange, reorganize, recompile, reformat, create derivative works of, change, or add to any Subscription or in any way attempt to reconstruct or discover any source code or algorithms of the Subscription, or any portion thereof, by any means whatsoever; (iii) remove any copyright, proprietary rights, or restrictive legends, or bypass or disable any protections that have been put in place against unlicensed use of the Subscription and/or third party data; (iv) remove iCIMS’ or its Affiliate’s, or licensor’s legends and notices on any and all permitted copies, adaptations, and rearrangements of the Subscription (or part thereof); (v) provide, or otherwise make available, the Subscription to any third party; (vi) fail to take appropriate action with its employees, agents, and subcontractors, by agreement or otherwise, necessary to satisfy its obligations under this Acceptable Use Policy or the Agreement with respect to the use, copying, protection, and security of the Subscription and/or Subscriber Data; (vii) engage in any use, including copying, modification, redistribution, publication, display, performance or retransmission, of any portions of any Subscription, other than as expressly permitted by this Agreement, without the prior written consent of iCIMS, which consent iCIMS may grant or refuse in its sole and absolute discretion; (viii) use in the Subscription any robot, spider, automatic device or technology to act as a headless user that is able to execute automations using the same interactions and interface as a human; (ix) use the Subscription to send messages that violate applicable laws, rules, and regulations; or (x) use the Subscription to collect, process, or store Subscriber Personal Data (as defined in the Data Processing Addendum) pertaining to minors in violation of applicable laws, rules and regulations. iCIMS, in its sole discretion, may delete and/or remove any Subscriber Data used in connection with the Subscription which violates the terms of this Acceptable Use Policy.

### 3. Prohibited Uses

Subscriber understands, acknowledges and agrees that it shall not use any Subscription to knowingly: (i) impersonate any person or entity or falsely state or otherwise misrepresent affiliation with any person or entity; (ii) intercept any data not intended for Subscriber or its Users; (iii) perform any hack (ethical or of any other nature), including probing, scanning, or testing (or attempt to do any of the foregoing), loads, penetration, technical security, or other vulnerability of the Subscription or otherwise breach security or authentication measures; or (iv) use the Subscription for any illegal or unlawful activity. Subscriber agrees that it shall not use any Subscription to upload, post, email, transmit, store, distribute or otherwise make available: (a) any content, or engage in any behavior, action, or conduct, that is unlawful, harmful, untrue, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, fraudulent, deceptive, illegal, invasive of another’s privacy, hateful, racist, or otherwise objectionable; (b) any unsolicited or unauthorized messaging (as further set forth in Section 7 below); (c) any Subscriber Data, or otherwise provide material support or resources (or to conceal or disguise the nature, location, source, or ownership of material support or resources), to any person(s) or organization(s) designated by the United States government as a foreign terrorist pursuant to section 219 of the Immigration and Nationality Act or otherwise in violation of any U.S. export control restrictions; (d) any Subscriber Data or otherwise provide material support or resources (or to conceal or disguise the nature, location, source, or ownership of material support or resources), to any person(s) or organization(s) in countries sanctioned by the U.S., United Kingdom or European Union (EU) or to those individuals or entities named to a restricted person or party list of the U.S., United Kingdom, or EU, including the sanctions lists maintained by the U.S. Office of Foreign Assets Control or the Denied Persons List or Entity List maintained by the U.S. Department of Commerce, in violation of applicable sanctions law(s); (e) a time bomb, worm, virus, malware, ransomware, lock, drop-dead device, or other similar component of software or electronically stored information that is intended in any manner to: (1) damage, destroy, alter, or adversely affect the operation of the Subscription or any software, hardware, or a service in connection with which the Subscription is used; or (2) reveal, damage, or alter any Subscriber Data, or

any other software, hardware, or information of or relating to another person or entity; or (f) any incorrect or misleading Subscriber Data.

#### **4. Limitations**

Except as otherwise set forth on the applicable Order Form and/or Statement of Work, Subscriber understands and acknowledges that iCIMS may establish, as described in the Documentation, user, technical or other limits concerning Subscriber, its Affiliates and Users use of the Subscriber Data and their use or access to the Subscription (or part thereof). iCIMS shall provide Subscriber with commercially reasonable notice (which for purposes of this Limitations Section may include notice by update to the applicable Documentation in accordance with the Agreement) of any such new practices or limits to the specific Subscriptions (i.e., the particular product(s), offering(s), portal(s), module(s), line item(s) to which such new practices or limits pertain) ("**Affected Subscription**") pursuant to the terms thereof. If Subscriber provides iCIMS with written notice of any objection to such new practices or limits to the Affected Subscription within fifteen (15) days of iCIMS' notice thereof, such new practices or limits to the Affected Subscription will not be effective until Subscriber and iCIMS have reached an agreement with respect to such change, practice, or limit to the Affected Subscription. In the event an agreement cannot be reached within sixty (60) days from Subscriber's objection to such notice, such new practice or limit to the Affected Subscription will not be effective as to Subscriber for the remainder of the Subscription Period, provided that iCIMS may, in its sole discretion and upon thirty (30) days written notice to Subscriber, terminate the Affected Subscription for convenience, and Subscriber's sole remedy for iCIMS' termination hereunder will be a refund of any pre-paid but unused fees specific to the Affected Subscription.

#### **5. Named Users**

Subscriber shall ensure that only named Users access or use the Subscription and that each named User is a unique person. Use of a non-iCIMS intermediate user interface, portal, or page to aggregate data, information, or actions from multiple individuals or users into the Programs will be deemed separate named Users under this Agreement. Further, sharing of usernames and/or passwords for access to the Subscription is prohibited and Subscriber shall be responsible for its Users misuse of any usernames or passwords to access the Subscription.

#### **6. Consents & Authorizations**

Subscriber understands, acknowledges and agrees that: (i) iCIMS is not a covered entity or a business associate for purposes of the U.S. Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the regulations promulgated thereunder; (ii) Subscriber shall not, and shall ensure each User does not, use the Subscription to submit, upload, process or store any health-related information, as the basis for any health-related decisions, or in connection with performing any health care related functions or activities requiring the disclosure, processing or storing of any health-related information. Further, Subscriber is solely responsible for determining the form of and providing or obtaining any notices, consents and/or authorizations, if any, required by any applicable laws or regulations associated with the collection, use, disclosure, transfer, or other processing of, or access to, any Subscriber Data.

#### **7. E-Mail Message Compliance**

Subscriber shall comply with the following when sending e-mail messages through the Subscription: (i) use only permission-based marketing e-mail message lists (i.e., lists in which each recipient has expressly granted permission to receive e-mail messages from Subscriber by affirmatively opting-in to receiving those e-mail messages); (ii) always include a working "unsubscribe" mechanism in each e-mail message that allows the recipient to opt-out from an e-mail mailing list except as otherwise required or set forth by applicable law; (iii) comply with all requests from recipients to be removed from email mailing lists within ten (10) days of receipt of the request or the appropriate deadline under applicable law; (iv) maintain, publish, and comply with a privacy policy that meets all applicable legal requirements, whether or not Subscriber controls the sending of the e-mail message; and (v) include in each e-mail message: (a) a link to a then-current privacy policy applicable to that e-mail message, and (b) a valid physical mailing address or a link to that information. While using the Subscription, Subscriber shall not: (1) send e-mail messages to addresses obtained from purchased or rented digital message lists; (2) use third party message addresses, domain names, or mail servers without proper permission; (3) routinely send e-mail messages to non-specific addresses (e.g., webmaster@domain.com or info@domain.com); (4) send e-mail messages that result in an unreasonable number of spam or similar complaints (even if the e-mail messages themselves are not actually spam); (5) disguise the origin, or subject matter of, any e-mail message or falsify or manipulate the originating message address, subject line, header, or transmission path information for any e-mail message; (6) send offers for the purpose of obtaining personal information or generating leads for third parties; (7) send "chain letters," "pyramid schemes," or other types of messages that encourage the recipient to forward the content to strangers; (8) send to lists of addresses that are programmatically generated or scraped from the internet; (9) employ sending practices, or have overall message delivery rates, which negatively impact or has adverse effects on the Subscription; or (10) import, or incorporate into, any contact lists or any other similar lists that you may upload to the Subscription, any of the following information: social security numbers, national insurance number, credit card data, passwords, security credentials, bank account numbers, or sensitive personal, health, or financial information of any kind.

Subscriber acknowledges and understands that other terms, conditions, and policies may apply to its use of Communication Products as further detailed in Section 8 (Phone Number Providers) below.

**8. Phone Number Providers (if applicable)**

Some products used by the Subscriber as part of the Subscription may enable Subscriber to send messages through a phone number and/or short code using SMS or other methods. iCIMS engages third-party vendors to provide the phone number(s) and short code(s) that Subscriber uses to communicate through the applicable product. If Subscriber elects to use a product as part of the Subscription that involves phone number(s) or short code(s), Subscriber will be notified which third-party vendor will be providing it with the phone number(s) and/or short code(s) through its "User Preferences" page of its platform. The vendors currently used, along with a link to their respective terms, conditions, and policies are as follows:

- [Twilio](#)
- [Vonage](#)

Subscriber understands, acknowledges and agrees that its use of phone number(s) and/or short code(s) within the Subscription must conform and comply with the guidelines set forth by the [CTIA](#) (Cellular Telecommunications Industry Association), the [CWTA](#) (Canadian Wireless Trade Association), the [ETNO](#) (European Telecommunications Network Operators' Association), and the [GSMA](#) (Global System Mobile Association), as applicable. Subscriber's use of the Subscription must comply with all laws and regulations governing communications to or from message recipients, including, but not limited to, the U.S. CAN SPAM Act, U.S. Telephone Consumer Protection Act ("TCPA"), Canadian Anti-Spam Legislation, S.C. 2010, c. 23, and any other applicable federal, state, local or foreign laws.

In the event Subscriber chooses to subscribe to a product that enables sending SMS and/or similar messages utilizing phone numbers or short codes, Subscriber acknowledges and agrees that Subscriber is solely responsible for complying with all terms, conditions, guidelines and policies of the organizations listed above, and any other similar self-regulatory organizations, as applicable.