



SOFTWARE SUBSCRIPTION TERMS AND CONDITIONS

Effective January 13, 2022

These Software Subscription Terms and Conditions ("Agreement") apply to an Order that incorporates these terms and conditions entered into between Computer Aid, Inc., and its affiliates ("We," "Us," "Our") and the entity subscribing to the Hosted Service identified on the Order ("You," "Your").

1. Access Grant

During the term of each subscription to the Hosted Service set forth on an Order (each, a "Subscription Term"), we grant You and Your affiliates a non-exclusive, non-transferable right, subject to the terms and conditions of this Agreement and in accordance with applicable law, to grant Users (individuals authorized to access the Hosted Service) located anywhere in the world access to our hosted service ("Hosted Service"), solely in support of Your internal business operations (including but not limited to in support of Your customers) and in a manner consistent with the Documentation and terms specified on an Order. We will provide You technical support as specified on an Order and the Documentation. We will provide You access to Your Hosted Service environment by sending You an IP address or URL. If applicable, we will provide you the professional services listed on an order. "Documentation" means the then current version of the Hosted Service User Guide as posted on our website. "User" means an individual who is an employee or contractor of You.

2. Certain Obligations and Restrictions

You are responsible for Your Users' compliance with this Agreement. "Content" means, data, text, audio, video, images, or other content that You or any User uploads, creates or transfers to the Hosted Service.

Notification of Breach. You will promptly notify us immediately after you become aware of any breach of security such as unauthorized use of any password or account or any other known or suspected breach of security of the Hosted Service. In addition you shall, as applicable: (a) immediately implement appropriate controls to maintain and preserve all tangible and/or electronic evidence relating to the security breach; (b) notify CAI both telephonically and in writing immediately after becoming aware of such occurrence; (c) conduct your own internal investigation, at your cost, of the security breach; (d) cooperate with CAI in their investigation



of the security breach, including but not limited to making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable Law or as otherwise required by CAI; and (e) provide to CAI a detailed plan within ten (10) calendar days of the occurrence describing the measures you will undertake to prevent a future similar security breach.

If You become aware of any violation of Your obligations by a User, You will immediately terminate such User's access to the Hosted Service and Your Content, and You will promptly notify us immediately after you become aware of any such violation by a User. We are not responsible for unauthorized access to Your User accounts, except to the extent caused by our breach of this Agreement. Notification of a breach under this section shall include, to the extent known:

- a. Identification of each account or user involved in the breach;
- b. a brief description of what happened, including the dates of the security breach and discovery of the security breach, if known;
- c. the scope of the security breach, including a description of the types of data and accounts involved; and
- d. a description of Your current response to the security breach.

You and Your Users will not (a) modify, tamper with, repair, or otherwise create derivative works of the Hosted Service or any software included in the Hosted Service; or (b) reverse engineer or apply any other process or procedure to derive the source code of any software included in the Hosted Service; (c) interfere with or disrupt the integrity or performance of the Hosted Service; or (d) attempt to gain unauthorized access to the Hosted Service or its related systems or networks (i.e. combining separate projects into one); or (e) access or use the Hosted Service in a way intended to avoid incurring fees or exceeding usage limits or quotas; or (f) attempt to probe, scan or test the vulnerability of the Hosted Service or to breach or disable the security or authentication measures; or (g) use the Hosted Service to develop a product that is competitive with any of our product offerings; or (h) use the Hosted Service to store or transmit (a) material in violation of Third-Party¹ privacy rights; or (b) libelous, or otherwise unlawful or tortious material; or (c) material that infringes any copyright, trademark, patent, trade secret or other proprietary right of any entity or individual; or (d) viruses, Trojan horses, worms, time bombs, cancelbots, corrupted files, or any other similar software or programs.

¹ "Third Party" means any party that is not a party to this Agreement. "Third Party Solution" means any software You may use in conjunction with Our Hosted Solution. "Third Party Component" means any software We have incorporated into Our Hosted Solution.

Except for our responsibilities as expressly set forth in this Agreement, You are responsible for the development, Content, operation, maintenance, and use of Content and compliance with all Hosted Service Policies. “Hosted Service Policy” means any policy established by us or our Third-Party Component provider(s) for the Hosted Service. You are also responsible for Your use of any Third-Party Solution that You use in conjunction with using Our Hosted Solution. .

3. Intellectual Property Ownership

We, our affiliates and our licensors own all right, title and interest in and to the Hosted Service. Each party will own and retain all rights in its trademarks, logos, and other brand elements (collectively, “Trademarks”). To the extent a party grants any rights or licenses to its Trademarks to the other party in connection with this Agreement, the other party’s use of such Trademarks will be subject to the reasonable trademark guidelines provided in writing by the party that owns the Trademarks. You will be and remain the owner of all rights, title, and interest in and to Content that You create.

4. Suspension of Access; Removal of Content

We reserve the right to suspend Your access to the Hosted Service if You or any of Your Users breach a material provision of this Agreement, and to remove any improper Content uploaded or transferred to the Hosted Service in violation of this Agreement.

5. Term and Termination

Orders may only be terminated according to this section. You may terminate any Order at any time by providing written notice to us. We may terminate any Order upon written notice to You (a) if You breach a material provision of this Agreement and fail to cure the breach within thirty (30) days following such notice; or (b) pursuant to the “Indemnification” and “Limited Warranties and Remedies” sections. Upon termination of all Orders, this Agreement will terminate and (a) we will make all Content available for Your download in the file format in which it was stored as part of the Hosted Service for 30 days after termination, after which time it will be deleted; and (b) all fees that You are obligated to pay as of the date of termination will be immediately due and payable. You are not entitled to any refund of fees paid due to a termination of the Agreement or an Order under this section.

6. Indemnification

We will indemnify, defend and hold you harmless , at our expense, against any claim, demand, suit, or proceeding (collectively, “Claim”) brought against You by a Third-Party alleging that the Hosted Service infringes or misappropriates an intellectual property right of the Third-Party and

will indemnify You for and hold You harmless from any damages finally awarded to the Third-Party claimant or agreed to in settlement of the Claim, provided that You (a) promptly give us written notice of the Claim; and (b) give us sole control of the defense and settlement of the Claim (provided that we may not settle any Claim that imposes liability on, or contains any admission of fault by, You without Your consent); and (c) provide to us all available information and reasonable assistance necessary for us to defend or settle the Claim; and (d) have not compromised or settled the Claim without our written approval. If Your use of the Hosted Service is enjoined in connection with the Claim, we may choose to either modify the Hosted Service to be non-infringing (while substantially preserving its utility and functionality) or obtain a license to allow for continued use of the Hosted Service, or if these alternatives are not commercially reasonable, we may terminate Your subscription to and use of the Hosted Service and refund any unused, prepaid fees paid for the Hosted Service.

We will have no indemnification obligation for any Claim to the extent the Claim arises from or is based upon (i) Your Content or (ii) Your use of a Third-Party Solution; or (iii) the use of the Hosted Service in an unlawful or unauthorized manner; or (iv) the combination of the Hosted Service with any Third-Party Solutions, services or business processes not provided or approved by Us as part of the Hosted Service if the Claim would not have arisen without such combination, or (v) inaccurate Content or misinterpretation of the Content delivered by the Hosted Service.

You will defend us, at Your expense, against any Claim brought against us by a Third-Party (a) alleging that the use of Content infringes or misappropriates an intellectual property right of the Third-Party or (b) arising from a breach of the “Certain Obligations and Restrictions” section or the “Data Protection” section of this Agreement by You or Your Users, and will indemnify us for and hold us harmless from any damages finally awarded to the Third-Party claimant or agreed to by You in settlement of the Claim, provided that we: (i) promptly give You written notice of the Claim; and (ii) give You sole control of the defense and settlement of the Claim (provided that You may not settle any such Claim that imposes liability on, or contains any admission of fault by, us, or affects our operation of the Hosted Service, without our consent); and (iii) provide to You all available information and reasonable assistance necessary for You to defend or settle the Claim; and (iv) have not compromised or settled the Claim without Your written approval.

The provisions of this section state the sole, exclusive and entire liability of the indemnifying party to the indemnified party, and are the indemnified party’s sole remedy, with respect to each type of Claim described in this section.

7. Insurance

We will maintain, at our expense, sufficient types of insurance coverage, including commercial general liability, workers' compensation, automobile liability, employee fidelity, and professional liability / errors and omissions on standard policy forms and with insurance companies with at least an A.M. Best Rating of A-VII authorized to do business in the jurisdictions where our services are to be performed.

Upon Customer's written request, we will provide a certificate of insurance evidencing the coverages.

8. Limited Warranties and Remedies

We warrant that (a) the Hosted Service will perform in substantial conformance with the functions set forth in the TrueProject product information as occasionally amended during a Subscription Term; and (b) our employees and contractors will perform any services listed on an Order in a manner conforming to generally accepted industry standards and practices. For any breach of the warranties set forth in subsection (a) above, Your exclusive remedy, and our entire liability, will be (i) the correction of the Hosted Service errors that caused the breach of the warranty; or (ii) if such correction cannot be reasonably effected by us, the termination of this Agreement and all Orders and the refund of any unused, prepaid fees paid for the Hosted Service. For any breach of the warranty set forth in subsection (c) above, Your exclusive remedy and our entire liability will be re-performance of the services at no cost to you.

Each party warrants that any individual who signs this Agreement and any Order governed by the Agreement on behalf of such party has the authority to enter into this Agreement or any such Order on behalf of such party, and that it will comply with all applicable statutes, laws, rules and regulations in the exercise of its rights and the performance of its obligations under this Agreement.

You acknowledge that the direct or indirect transfer of products provided as part of the Hosted Service contrary to United States law is prohibited. You warrant that (i) You are not a Restricted Party; and (ii) You are not controlled by or acting on behalf of any Restricted Party; and (iii) neither You nor any of Your employees, agents or contractors will transfer or allow any Product to be transferred to any Restricted Party. "Restricted Party" means any person or entity that is (1) listed on any of the lists of persons or entities maintained by the United States government that prohibit such persons or entities from receiving exports or services; or (2) a national or resident of, or an entity or governmental authority in, any country or territory that is or becomes

subject to United States export controls for anti-terrorism reasons or with which United States persons are generally prohibited from engaging in financial transactions.

NO OTHER WARRANTIES OR COMMITMENTS, EXPRESS OR IMPLIED, ARE MADE WITH RESPECT TO THE HOSTED SERVICE INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SYSTEMS INTEGRATION, TITLE, SATISFACTORY QUALITY AND NON- INFRINGEMENT.

9. Limitation of Liability

EXCEPT FOR OUR OBLIGATIONS UNDER THE “INDEMNIFICATION” SECTION, THE CUMULATIVE AGGREGATE LIABILITY OF US AND ALL OF OUR AFFILIATES AND LICENSORS TO YOU AND ALL OF YOUR AFFILIATES RELATED TO THIS AGREEMENT WILL NOT EXCEED THE AMOUNT OF THE FEES PAID OR PAYABLE TO US IN THE TWELVE (12) MONTHS PRIOR TO THE FIRST CLAIM MADE BY YOU. SUBJECT TO THE FOREGOING, OUR MAXIMUM LIABILITY FOR ANY CLAIM MADE BY YOU, TO THE EXTENT THE CLAIM ARISES FROM OR IS BASED UPON THE USE OF A THIRD-PARTY SOLUTION, WILL NOT EXCEED THE AMOUNT OF THE APPLICABLE THIRD-PARTY SOLUTION PROVIDER’S LIABILITY TO US RELATED TO THE CLAIM. IN NO EVENT WILL WE OR ANY OF OUR AFFILIATES OR LICENSORS BE LIABLE TO YOU OR ANY OF YOUR AFFILIATES FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHERWISE, EVEN IF WE OR ANY OF OUR AFFILIATES OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF AN AGREED REMEDY FAILS OF ITS ESSENTIAL PURPOSE OR IS HELD UNENFORCEABLE FOR ANY OTHER REASON.

10. Orders and Payment

You will be invoiced upon execution of and according to the terms of an Order. All fees due to Us will be payable, in full and in the currency listed on an Order, thirty (30) days from the date of the invoice and will be deemed overdue if they remain unpaid thereafter. All fees are net of any taxes, which will be Your responsibility, except for taxes on our income. Any dispute to an invoice must be raised within thirty (30) days from the date of invoice or the invoice will be deemed correct. If any undisputed invoice governed by this Agreement remains unpaid for thirty (30) or more days after it is due, we may, without limiting our other rights and remedies, accelerate all unpaid fee obligations under such Orders so that all amounts payable by You become immediately due and payable. In addition, any amounts which remain unpaid after the due date will be subject to a late charge equal to one and one-half percent (1.5%) per month or the highest rate allowable by law, whichever is lower, from the due date until such amount is paid. Except as otherwise noted, all Orders are firm and not subject to cancellation, return,

refund or offset by you. You may not reduce the quantities purchased during a subscription term. If Your usage of a Third-Party Component exceeds the allowable usage of the Third-party Component as set forth on an Order, You will pay us for any additional fees our Third-party Component provider charges Us for that excess usage.

11. Audit

You will keep accurate and complete records relating to Your activities under this Agreement, including records related to Your use of the Hosted Service and other information necessary to demonstrate Your compliance with this Agreement (“Records”). Within ten (10) days following our written request, You will certify to us in writing and signed by an officer of Your company that Your use of the Hosted Service complies with the terms of this Agreement and will provide us any Records we specify in such request. In addition, within ten (10) days following our written request, we may audit Your Records and Your use of the Hosted Service.

12. Data Protection

You will not transfer to us or provide us any access to any data or information that is subject to regulation under Applicable Data Protection Law (“Protected Data”) in connection with this Agreement, including without limitation Personal Data, Protected Health Information and Personally Identifiable Information (as such terms are defined in Applicable Data Protection Law), except for Protected Data related to the Users’, or Your customers’ contact persons or which is uploaded or transferred to the Hosted Service. “Applicable Data Protection Law” means all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security of Protected Data including, without limitation, the European Union Directives and Regulations governing general data protection and all applicable industry standards concerning privacy, data protection, confidentiality or information security.

As between You and us, for purposes of this Agreement and Applicable Data Protection Law, You are the “data controller” and we are acting on Your behalf as a “data processor” with respect to Protected Data that You or Your Users upload or transfer to the Hosted Service. We have implemented appropriate technical, organizational, and security measures designed to safeguard and protect Protected Data provided by You to us and we may access, use and transfer such Protected Data to our affiliates and Third-Parties (including those located outside of the European Economic Area) only for the purposes of fulfilling our obligations and exercising our rights, providing information to You and complying with our legal and auditing requirements.



You are responsible for providing any notices and obtaining any consents and approvals required to collect, process, transfer, maintain and use the data collected by You in connection with Your use of the Hosted Service. We are not responsible for unauthorized access to data or reports through lost or misplaced reports or unsecured devices. You will enable encryption of all data in transit and at rest in Your possession.

We and our Third-Party Component providers may access and use Content, Usage Information and any other anonymous data collected in connection with the Hosted Service solely in accordance with the relevant Hosted Service Policy. “Usage Information” means anonymous information generated in connection with Your use of Our products that we may collect about You and Your Users, as further described in the Hosted Service Policy applicable to those products. For the avoidance of doubt, in no instance will Usage Information be deemed to include Content.

We reserve the right to access Your production data solely for investigation, resolution of technical support cases and system maintenance. In the event We need to make a copy of Your production data We will provide Your support liaison notice of any such action. For example, We do not want to conduct technical support testing on production data. We will promptly destroy all copies of production data after it is no longer needed.

We will provide to you the Hosted Service, any services ancillary thereto, and any other services set forth on the Order in accordance with our Data Security Policy, which is attached hereto as Annex A and made a part hereof.

13. Confidentiality

Under this Agreement, Confidential Information may be accessed or disclosed between the parties. “Confidential Information” means any information identified as confidential at the time of disclosure, or that reasonably should be understood to be confidential in view of the information’s nature or circumstances around its disclosure, and will in all cases include pricing terms, the terms of this Agreement or any Order governed by this Agreement, software, technology, business plans, technical specifications, product development plans, marketing plans, financial information, Content, education materials, customer lists, and generic tools and objects related to our products created by us during the provision of consulting services. Confidential Information will not include information that (a) is or becomes a part of the public domain through no act or omission of the receiving party; or (b) was in the receiving party’s lawful possession prior to the disclosure; or (c) is lawfully disclosed to the receiving party by a Third-Party without restriction on the disclosure; or (d) is independently developed by the receiving party.

Each party agrees to hold the other party's Confidential Information in confidence during the term of this Agreement and for a period of five (5) years after the termination of this Agreement, and to disclose such Confidential Information only to those employees or agents who have a need to know such Confidential Information and are required to protect it against unauthorized disclosure. Notwithstanding the foregoing, either party may disclose the other party's Confidential Information to a federal or state governmental entity to the extent such disclosure is required by law, so long as the receiving party notifies the disclosing party in advance of the required disclosure, where lawfully permitted and as soon as reasonably practicable to allow the disclosing party to contest the disclosure.

Upon termination of this Agreement and except for electronic copies made in the course of normal network backups or as otherwise set forth in this Agreement, the receiving party will promptly destroy or return, at the sole discretion of the disclosing party, all Confidential Information of the disclosing party in the receiving party's possession or control.

14. Notices

We shall give You contractual and legal notices regarding the Hosted Service by means of an email and/or commercial overnight courier. All contractual and legal notices will be in writing and sent to the address in the Notices section of the TrueProject Order Form and will be deemed to have been given when (a) personally delivered; (b) sent by a commercial overnight courier signature required; or (c) via email with return receipt.

You shall provide notices to: Computer Aid, Inc, ATTN: Contract Management, 1390 Ridgeview Drive, Allentown, PA 18104, ContractManagement@cai.io

15. Assignment

This Agreement may not be assigned or otherwise transferred in whole or in part by you, including by operation of law, without our prior written approval.

16. Non-Solicitation

Except for hiring an employee (or agent) of the other party to fill a job opening that was publicly announced and to which the applicable employee (or agent) responded, during the term of this Agreement and for one (1) year following termination of this Agreement, neither party will hire or directly or indirectly, solicit any employee (or agent) of the other party who has provided services or performed obligations under this Agreement in the previous twelve (12) months.

17. Survival

Sections 3, 6, 7, 8, 9, 10, 11, 12, 13, 16, and 18 will survive the termination of this Agreement.

18. Other Provisions

All of the terms and provisions of this Agreement shall be binding upon, inure to the benefit of, and be enforceable by, the parties hereto and their respective heirs, successors, legal representatives and permitted assigns. The terms of this Agreement and any applicable Order will supersede the terms in any purchase Order or other ordering document that You generate and provide to us. Any terms of trade stated or referenced in any such purchase order (except for names, quantities, and addresses) will not be binding on us. As between this Agreement and an Order, the latter prevails but only with respect to that Order. Neither party will be responsible for delay of performance due to causes beyond its control.

No joint venture, partnership, employment, or agency relationship exists between You and Us as a result of this Agreement or Your use of the Hosted Service. The failure of either You or us to enforce any right or provision in this Agreement will not constitute a waiver of such right or provision unless acknowledged and agreed to in writing by the party otherwise entitled to exercise or enforce it. There are no Third-Party beneficiaries of this Agreement.

Governing Law, Attorney's Fees and Waiver of Jury Trial

This Agreement and the parties' relationship under it will be interpreted under and governed by the laws of the Commonwealth of Pennsylvania and controlling United States federal law, without regard to the choice or conflicts of law provisions of any jurisdiction. This Agreement will not be subject to the United Nations Convention on the International Sale of Goods. Any disputes, actions, claims or causes of action arising out of or in connection with this Agreement, the parties' relationship under it or the Hosted Service will be subject to the exclusive jurisdiction of the Courts of Common Pleas of Lehigh County or the United States District Court for the Eastern District of Pennsylvania. Both parties hereby irrevocably consent to the exclusive jurisdiction of and venue in such courts and waive any right to a jury trial in any such proceeding. In any dispute, the prevailing party will be entitled to recover its cost of enforcing its claim, including but not limited to reasonable attorney fees.

If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, then such provision will be construed, as nearly as possible, to reflect the intentions of the invalid or unenforceable provision, with all other provisions remaining in full force and effect.



Use

When You access any Third-Party Solution with connectors included as part of the Hosted Service, We agree and acknowledge that (a) You may download Content from the Third-Party Solution provider; and (b) Your access to the Third-Party Solution with such connectors will be for the purpose of utilizing the Third-Party Solution in conjunction with the Hosted Service. You agree and acknowledge that we are not responsible for interruptions of service caused by the Third-Party Solution. You may not remove or obscure any patent, copyright, trademark, proprietary rights notices, and/or legends contained in or affixed to any output of the Hosted Service. You will indemnify, defend, and hold Us harmless from any liability, damage, or other costs incurred by Us as a result of Your use of the Third-Party Solution.

Data Privacy and Protection

We will collect anonymous usage data related to Your use of the Hosted Service; for clarity, such data will not include Protected Data. Our and our Third-Party hosting provider(s) security products are not designed to manage physical or logical access to facilities or systems where delay in or failure of such access could threaten health or safety, or cause property, environmental or similar damage.

Representation and Warranties

You represent and warrant that Your decision to purchase a subscription to the Hosted Service is not based on (a) any oral or written comments made by us with respect to functionality or features not currently offered in our latest generally available version of the Hosted Service; or (b) any expectation that any additional features or functionality presented as part of a demonstration, beta evaluation or roadmap presentation of the Hosted Service may be included in a future update or release of the Hosted Service; or (c) demonstrations of any software that is not currently generally available. You further acknowledge that the development, release and timing of any additional features or functionality for the Hosted Service remain at our sole discretion. You are responsible for the proper operation of Your network and Your equipment used to connect to the Hosted Service. This Agreement comprises the entire agreement between You and Us and supersedes all prior or contemporaneous negotiations, discussions, agreements or statements, whether written or oral.



Annex A: Data Privacy and Security Addendum **PRIVACY AND SECURITY REQUIREMENTS**

For purposes of this Agreement.

The term “Personal Data” shall mean any data, information or record that directly or indirectly identifies a natural person or relates to an identifiable natural person or is otherwise subject to any Privacy Law (as defined below), including, but not limited to, name, home address, telephone number, personal e-mail address, payment/credit card data, Social Security Number (SSN), Tax Identification Number (TIN), driver’s license number, national ID number, bank account data, passport number, combination of online username and password, medical and health-related information and any other Personally Identifiable Information that CAI or any Third-Party acting on CAI’s behalf processes in connection with the Services provided to Customer or Customer by CAI.

The term “Customer Data” shall refer to any and all data that is owned or created by Customer as it relates to Customer’s finances, business operations, intellectual property, human resources, or its Customer.

The term “Customer Data” shall refer to any data belonging to Customer’s Customer which would be classified in similar fashion to Customer’s Data (e.g., customer finances, customer business operations, customer intellectual property, etc.). Customer may be maintaining Customer data within Customer’s infrastructure; however, this data is still to be defined as Customer Data.

The terms “Personal Data”, “Customer Data” and “Customer Data” are collectively referred to as “Data”.

The term “Information Security Incident” means actual or suspected (i) loss or theft of Data; (ii) unauthorized use, disclosure, acquisition, transmission of or access to, or other unauthorized processing of Data that reasonably may compromise the privacy or confidentiality of the Data; or (iii) unauthorized access to or use of, inability to access, or malicious infection of, CAI systems that reasonably may compromise the privacy or confidentiality of Data.

The terms “process,” “processing” or “processed” in relation to Data include, without limitation, receipt, collection, creation, recording, organization, storage, retrieval,

consultation, use, manipulation, amendment, transmission, disclosure, discarding, destruction and/or erasure.

CAI agrees, covenants, and warrants to Customer that at any and all times during which it processes Data, CAI will:

- a) Take all appropriate and commercially reasonable measures, including, without limitation, the administrative, physical, technical (including electronic), and procedural safeguards set forth in the Data Privacy and Security Addendum, including but not limited to encryption that meets storage industry standards of data at rest and in transit, to protect the Data against any Information Security Incident. For information processed in electronic form, CAI agrees that such safeguards must include, without limitation, electronic barriers (e.g., “firewalls” or similar barriers) and password-protected access to the Data. For information in written or other tangible form, CAI agrees that such safeguards must include secured storage and secure destruction of the Data in accordance with applicable law and applicable privacy standards;
- b) Maintain or cause to be maintained a reasonable and commercially feasible information security program that complies with all applicable laws and is designed to reasonably ensure the security and confidentiality of all Data;
- c) Comply with all applicable laws and industry standards that relate in any way to the privacy, data protection, electronic storage, confidentiality, processing or security of Data and apply to CAI or Customer – including without limitation (i) state security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Data; and all other similar federal, state, local and international requirements; (ii) electronic storage industry standards concerning privacy, data protection, confidentiality or information security; and (iii) U.S. state data protection laws including, without limitation Massachusetts 201 CMR 17.00 – 17.05 Standards for the Protection of Personal Information of Residents of the Commonwealth, California Consumer Privacy Act (CCPA) of 2018 as of 1 January 2020 (collectively, “Privacy Laws”) and EU General Data Protection Regulation (GDPR) of 25 May, 2018.
- d) Not transfer Data outside the United States of America for processing without the prior express written consent of Customer;
- e) Not sell, share, or otherwise transfer or disclose any Data, to any other party, without prior express written consent from Customer, except as specifically permitted under the Data Privacy and Security Addendum or required by law;

- f) Not use Data in any manner not specifically permitted under this Agreement without prior express written consent from Customer;
- g) Not send or provide any marketing or promotional communications to Customer or Customer employees or consumers without Customer's or Customer's explicit written consent;
- h) Not aggregate or combine Data with any other data without prior express written consent from Customer;
- i) Not subcontract any of its rights or obligations under this Data Privacy and security Addendum without the prior express written consent of Customer. Where CAI, with the consent of Customer, subcontracts its obligations under this Data Privacy and Security Addendum, it shall do so only by way of a written agreement with its subcontractor that imposes the same privacy and security obligations on the subcontractor. Whenever CAI employs the services of Third-Party service providers to assist it in performing its obligations under this Data Privacy and Security Addendum, CAI agrees that such service providers are capable of maintaining appropriate safeguards for Data and that CAI has contractually obligated such service providers to maintain appropriate safeguards designed to comply with applicable law and applicable privacy standards. Where the subcontractor fails to fulfill its obligations under any sub-processing agreement, CAI shall remain fully liable to Customer for the fulfillment of its obligations under this Data Privacy and Security Addendum;
- j) Ensure that Data are only available to CAI personnel who have a legitimate business need to access the Data, who are bound by legally enforceable confidentiality obligations, and who have received training in data protection law;
- k) Not retain Data any longer than is reasonably necessary, in accordance with Customer record retention policies, to accomplish the intended purposes for which the Data was processed pursuant to this Data Privacy and Security Addendum. When Data is no longer necessary for the purposes set forth in the Data Privacy and Security Addendum, or promptly upon the expiration or termination of the Agreement, whichever is earlier, or at an earlier time as Customer requests in writing, CAI shall take reasonable steps to return, destroy (e.g., by secure shredding and/or digitally wiping), or arrange for the secure destruction of each and every original and copy in every media of all Data in CAI's possession, custody or control. Promptly following any return or alternate action taken to comply with this paragraph, CAI shall certify in writing to Customer that such return or alternate action occurred, and the method used for such destruction. In the event that applicable law does not permit CAI to comply with the delivery or destruction of the Data, CAI warrants that it shall ensure

the confidentiality of the Data and that it shall not use or disclose any Data at or after the termination or expiration of the Agreement;

- l) Where CAI uses a Third-Party for disaster recovery or other services, CAI shall (i) disclose this to Customer in writing, including the name of the provider, purpose of the services (e.g., disaster recovery), steps taken with Third-Party to address confidentiality, privacy and security, and (ii) cause each such Third-Party to agree in writing to be bound by terms and conditions substantially similar to those in (a) – (k) above and (m) below. Additionally, CAI agrees to audit the procedural, administrative, physical and technical measures used by each such Third-Party, at least once a year, which may include or consist of, at Customer's option, a SSAE 18 audit of such Third-Party, if available;
- m) Monitor CAI's information systems for unauthorized access and implement an incident response policy that specifies actions to be taken when CAI detects or becomes aware of such unauthorized access to its information systems. CAI shall provide a copy of such incident response policy to Customer upon request;
- n) If requested by Customer, within five business days from the date upon which the request was made by Customer, either: (i) update, correct or delete Data or modify the individual's choices with respect to the permitted use by Customer of such Data; or (ii) provide access to Customer to enable it to perform the activities described in clause (i) itself;
- o) Immediately notify the Customer Chief Compliance Officer if CAI receives notice from any governmental or regulatory authority alleging that Customer or CAI has failed to comply with Privacy Laws in connection with the performance of this Agreement, or if CAI otherwise becomes aware and reasonably believes that CAI or Customer may have failed or may in the future fail to comply with Privacy Laws in connection with the performance of this Agreement; and
- p) At Customer's direction, cooperate and comply with any requests or instructions issued by any privacy or data protection authority, including any governmental or regulatory authority applicable to Customer or Data.
- q) In the event of an Information Security Incident, such notice shall summarize in reasonable detail the nature of the Information Security Incident, the suspected data that is lost, stolen or compromised, if known, the parties which have or will be informed of the Information Security Incident, and the corrective action taken or to be taken by CAI.

CAI shall promptly notify Customer in writing of any Information Security Incident of which CAI becomes aware and of any request for access to any Data from any third person or any



government official, including any data protection or law enforcement agency; and of any and all complaints or other communications received from any individual pertaining to CAI's confidentiality policies or procedures applied to Data and/or the processing of either. In the event of an Information Security Incident, such notice shall summarize in reasonable detail the nature of the Information Security Incident, the suspected data that is lost, stolen or compromised, if known, and the corrective action taken or to be taken by CAI. CAI shall promptly take all necessary steps to robustly investigate and remediate, including, but not limited to, conducting a Third-Party forensic analysis. CAI shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate or rectify such Information Security Incident or necessitate the disclosure of Data to a government official. All information relating to each Information Security Incident must be retained by CAI until Customer has specifically consented in writing to its destruction. If requested by Customer and subject to Customer's confidentiality obligations, CAI shall permit Customer and its agents to access CAI's facilities and/or the affected hardware or software, as applicable, to conduct a forensic analysis of each such Information Security Incident.

In the event of an Information Security Incident, CAI shall (i) promptly, after becoming aware of such Information Security Incident, notify the Customer Security Officer by telephone, email or in writing at the address below of all known facts thereof, and (ii) at Customer's option and at the direction of Customer, whether or not required by applicable law, provide written notice to the individuals whose Data was reasonably connected to the Information Security Incident, or reimburse Customer for all direct out of pocket and commercially reasonable costs it incurs in providing such notice and/or in responding to governmental authorities, including, without limitation, (1) paying for postage and copying of Customer legally required notices; (2) offering to the affected individuals and providing, to those who elect to receive it, at least two years of credit monitoring services at CAI's expense; (3) paying for costs associated with implementing a call center, and (4) paying for costs associated with any forensic or legal analysis required. To the extent a State Attorney General or other governmental/judicial authority renders a fine, penalty or judgment, or requires an alternate remedy following an Information Security Incident, such as the provision of identity theft insurance, CAI will offer and provide the required remedy at its own expense.

Information Security Incident notifications shall be provided to: Computer Aid Inc Security Officer, address: 1390 Ridgeview Dr., Suite 300, Allentown, PA 18104; email: Security@cai.io and by telephone at 610-530-5000.



Customer shall have the right to verify CAI's compliance with the terms of this section or to appoint a Third-Party under reasonable covenants of confidentiality to verify the same on Customer's behalf. CAI shall grant Customer or Customer's agents unimpeded access to the extent necessary to accomplish the inspection and review of all data processing facilities, data files and other documentation used by CAI for processing of Data in relation to this Data Privacy and Security Addendum. CAI agrees to provide reasonable assistance to Customer in facilitating this inspection function. Upon request, CAI shall provide Customer with a list of CAI personnel entrusted with processing the Data transferred by CAI, together with a description of their access rights. An inspection performed pursuant to this section shall not unreasonably interfere with the normal conduct of CAI's business.

Notwithstanding any other right or remedy which Customer may have in the event of a breach of this Data Privacy and Security Addendum (or any other contractual relationship), CAI agrees to i) indemnify Customer (and keep Customer indemnified) and ii) defend us at CAI's expense against all costs, claims, damages or expenses for which Customer may incur or become liable due to any failure by CAI (or an authorized sub-processor) or CAI's personnel or contractors to comply with any of the obligations under this Data Privacy and Security Addendum.