DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM (the "**Addendum**") forms part of the Master Services Agreement (the "**Agreement**") by and between Applied Training Systems, Inc., a Delaware corporation (the "**Data Processor**") and the undersigned party to this Addendum (the "**Customer**," and collectively with the Data Processor, the "**Parties**").

Recitals

A. The Customer acts as a Data Controller, as defined in GDPR (as defined below);

B. The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor; and

C. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to the GDPR and other Data Protection Laws, and that incorporates by reference all provisions of the Standard Contract Clauses (as defined below), attached hereto as Exhibit A and incorporated herein by this reference, which are not otherwise stated herein.

NOW, THEREFORE, in consideration of the promises and agreements set forth herein, the Parties, each intending to be legally bound hereby, do promise and agree as follows:

AGREEMENT

1. Definitions. Unless otherwise defined herein, capitalized terms and expressions used in this Addendum shall have the following meaning:

"**Addendum**" means this Data Processing Addendum and all Schedules attached hereto.

"**Affiliate**" means, with respect to a party, an entity that (directly or indirectly) controls, is controlled by or is under common control with, such party, where control refers to the power to direct or cause the direction of the management policies of another entity, whether through ownership of voting securities, by contract or otherwise.

"**Customer Personal Data**" means any Personal Data processed by a contracted Data Processor on behalf of Customer pursuant to or in connection with the Agreement.

"**EEA**" means the European Economic Area.

"**GDPR**", also known as the General Data Protection Regulation, means the laws and regulations of the European Union and the EEA as applicable to the transfer and processing of Personal Data under the Agreement, including (where applicable) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

"**Data Transfer**" means a transfer of Customer Personal Data from the Customer or Customer's authorized users to the Data Processor, including any onward transfer of Customer Personal Data from a Data Processor to a subcontracted Data Processor.

"**Data Protection Laws**" means means the GDPR and, to the extent applicable, the data protection or privacy laws, regulations or legal requirements of the United Kingdom and the United States.

"**Personal Data**" means information about an individual that (a) can be used to identify, contact or locate a specific individual; (b) can be combined with other information that can be used to identify, contact or locate a specific individual; or (c) is defined as "personal data" or "personal information" by applicable laws or regulations relating to the collection, use, storage or disclosure of information about an identifiable individual.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Services**" means the services provided to the Customer by the Data Processor as described in the Agreement.

"**Standard Contractual Clauses**" means the standard contractual clauses, as updated from time to time, that apply to the transfer of Personal Data from Customer to Data Processors, as amended by incorporating the description of the Personal Data to be transferred set out in Schedule 1 to this Addendum and the technical and organizational measures to be implemented as set out in Schedule 2 to this Addendum.

"**Sub-Processor**" means any processor engaged by the Data Processor or by any other sub-processor of the Data Processor who agrees to receive from the Data Processor, or from any other sub-processor of the Data Processor Customer Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Processor after the transfer in accordance with his instructions, the terms of the this Addendum and Standard Contractual Clauses and the terms of the written subcontract.

The terms, "**Commission**," "**Controller**," "**Data Subject**," "**Member State**," "**Personal Data Breach**," and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Standard Contract Clauses

a. **Standard Contract Clauses Incorporated by Reference**. Customer (as "data exporter") and Data Processor (as "data importer") hereby enter into the Standard Contractual Clauses, which are incorporated in full by reference, and incorporate any amendments to the Standard Contract Clauses implemented by the Commission, to the extent such amendments relate to a restricted transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (a) by the Commission to or of the equivalent contractual clauses approved by the Commission under the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (b) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law. The governing law in the Standard Contractual Clauses shall be the law of the data exporter. In the event of inconsistencies between the provisions of the Standard Contractual Clauses and this Addendum, the Agreement or other agreements between the Parties as regards the Services, the Standard Contractual Clauses shall take precedence.

b. **Repeal of Standard Contract Clauses**. In the event that the Standard Contractual Clauses are replaced or repealed by the Commission or under GDPR, the Parties shall work together to negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with GDPR.

3. Processing of Customer Personal Data

a. **Data Processor Responsibilities**. Data Processor shall:

i. comply with all applicable Data Protection Laws, as applicable, in the Processing of Customer Personal Data;

ii. not Process Customer Personal Data other than on the relevant Customer's documented instructions, including as set forth in the Agreement;

iii. upon request from Customer, make available to Customer the current list of Sub-Processors with their country of location, and types of Personal Data Processed by such Sub-Processor; and

iv. otherwise comply with the Standard Contract Clauses as applicable to the Processing of Customer Personal Data as stated in this Addendum and Agreement.

b. **Customer Responsibilities**. The Customer shall:

i. comply, at all times with the applicable Data Protection Laws with respect to the processing of Personal Data in connection with its obligations under the Agreement;

ii. instruct throughout the duration of the Services the Data Processor to process the Customer Personal Data transferred only on the Customer's behalf and in accordance with the applicable Data Protection Law and the Standard Contract Clauses;

iii. ensure that the legally binding consents to the collection, access, use, maintenance, and/or disclosure of the Personal Data in accordance with the applicable Data Protection Laws and Customer policies and procedures have been obtained from each individual and entity to whom the Personal Data relates;

iv. promptly inform Data Processor of any policies it implements with respect to the Processing and protection of Personal Data with express instructions as to how these policies should be implemented by Data Processor;

v. promptly inform Data Processor of any request for erasure with respect to Data Subject's Personal Data with detailed instructions as to how Data Processor should address the request; and

vi. provide to Data Processor and also promptly update, when necessary, the following information: (a) identity and contact information of the Data Protection Officer or other contact of the Customer; (b) identity and contact information of the EU representative of the Customer; (c) types of Personal Data to be Processed; and (d) categories of Data Subjects to whom the Personal Data relates.

c. **Consent to Processing**. The Customer authorizes and instructs Data Processor to process Customer Personal Data in accordance with this Addendum and Agreement. Customer hereby acknowledges that such Customer Personal Data shall be Processed in the United States, and shall be maintained on servers located in the United States.

d. **Consent to Sub-Processing**. Customer hereby authorizes Data Processor to continue to use those Sub-Processors already engaged by Data Processor as at the date of this Addendum. Data Processor shall notify Customer of the appointment of any new Sub-Processor. Customer may reject (on reasonable grounds) the proposed appointment. The Parties shall work together to address the objections raised by any Customer. If no agreement can be reached by the Parties, then Data Processor and Customer shall work together in good faith to terminate the contract. Data Processor shall ensure that the arrangement between Data Processor and the Sub-Processor is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of the GDPR and applicable Data Protection Laws.

4. Data Processor Personnel. Data Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Data Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Data Protection Laws in the context of that individual's duties to the Data Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security.

a. Security Systems. 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, Data Processor shall in relation to the Customer Personal Data implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the: (a) applicable Data Protection Laws; (b) harm that might result from unlawful or unauthorized processing or accidental loss, damage, alteration, disclosure or destruction of the Personal Data; and (c) nature of the Personal Data.

b. GDPR Requirements. Data Processor shall, with regard to Personal Data, implement and maintain appropriate technical and organizational security measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in the GDPR, and particularly those related to possible Personal Data Breaches. Specifically, Data Processor shall:

i. have in place and comply with a security policy which: (a) defines security needs based on a regular impact assessments; (b) allocates responsibility for implementing the policy to a specific individual or members of a team, including having a Data Protection Officer ("**DPO**");

ii. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

iii. ensure its storage of Personal Data conforms with the industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled; and

iv. have secure methods in place for the transit of Personal Data within the customer support portal (for instance, by using encryption).

6. Data Subject Rights.

a. Data Subject Requests. Data Processor shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making (each a "**Data Subject Request**"). Taking into account the nature of the Processing, Data Processor shall assist Customer by appropriate technical and organizational measures, to the extent possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under GDPR or applicable Data Protection Laws. Except to the extent required by applicable law, Data Processor shall not respond to any such Data Subject Request without Customer's prior written consent except to confirm that the request relates to Customer. Further, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Data Processor shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Data Processor is legally permitted to do so and provided that such Data Subject Request is required under GDPR or applicable Data Protection Laws. Any costs arising from such provision of assistance shall be the responsibility of Customer, to the extent legally permitted.

b. **Government Requests**. The Personal Data processed pursuant to the Agreement may be subject to disclosure upon a valid request and as legally required by any law enforcement agency, whether located in the United States or EEA. Data Processor shall immediately notify Customer of any third-party request to release Customer Personal Data. Data Processor will cooperate with Customer to keep such Customer Personal Data confidential. At any time, Customer is entitled to suspend the transfer of data and/or terminate the Agreement citing its concern of the applicability of this Section.

7. Personal Data Breach

a. **Notification of Breach**. Data Processor shall, in accordance with the GDPR and applicable Data Protection Laws, notify Customer without undue delay upon Data Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. Data Processor's notification of or response to a Personal Data Breach under this Section 0 will not be construed as an acknowledgement by Data Processor of any fault or liability with respect to the Personal Data Breach. Notification(s) of Personal Data Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Data Processor selects, including via e-mail. It is Customer's sole responsibility to ensure it maintains accurate contact information on Data Processor's support systems at all times.

b. **Data Processor Mitigation**. Data Processor will use reasonable efforts to identify the cause of such Personal Data Breach and shall promptly and without undue delay: (a) investigate the Personal Data Breach and provide Customer with information about the Personal Data Breach, including if applicable, such information a Data Processor must provide to a Data Controller under the GDPR to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach to the extent the remediation is within Data Processor's reasonable control The obligations herein shall not apply to any breach that is caused by Customer or Customer's authorized users.

c. **Cooperation**. Data Processor shall co-operate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Deletion or Return of Customer Personal Data; audit rights.

a. **Deletion or Return of Personal Data**. Upon termination of the Services after the end of the provision of the Services, Data Processor shall, at the choice of the Customer, delete all Personal Data processed on behalf of the Customer and certify to the Customer that it has done so, or return to the Customer all Personal Data processed on its behalf and delete existing copies. Notwithstanding the foregoing, Data Processor may retain Customer Personal Data to the extent required by Data Protection Laws, and any other applicable laws of the United States (collectively, "**Applicable Laws**"), and only to the extent and for such period as required by such Applicable Laws and Data Processor shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose. The Parties agree that the certification of deletion of Personal Data that is described in the Standard Contractual Clauses shall be provided by the data importer to the data exporter only upon data exporter's request.

b. Audit. Data Processor shall make available to the Customer on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the contracted Data Processors. Information and audit rights of the Customers only arise under section to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws.

9. Limitation of Liability. Each Party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section of the Agreement.

10. Insurance. In addition to any requirements set forth in the Agreement, Customer shall procure and, throughout the term of the Agreement, maintain cyber liability insurance to cover any Personal Data Breach affecting Customer Personal Data, or other losses suffered by Data Processor or any member of the same group as Data Processor resulting from any action or inaction on Customer's part in an amount of no less than €1,000,000 per occurrence. The policy that provides liability coverage shall name Applied Training Systems, Inc. as an additional insured.

11. Miscellaneous

a. Notices. All notices and communications given under this Addendum must be sent in accordance with the Agreement.

b. Amendments. No alteration, amendment, or modification of this Addendum will be valid unless in writing and signed by an authorized representative of both Parties.

c. Governing Law and Jurisdiction. With respect to the Standard Contract Clauses, Processing, privacy, and security of Customer Personal Data, the governing law shall be the law of the Customer. For all other claims or disputes arising out of this Addendum or Agreement, the governing law and venue shall be in accordance with the terms of the Agreement.

d. Severability. Should any provision of this Addendum be found invalid or unenforceable pursuant to any applicable law, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Addendum will continue in effect.

e. Ambiguity. Any ambiguity in the terms of this Addendum will be resolved to permit Data Processor to comply with Applicable Laws.

f. Entire Agreement and Conflict. This Addendum is the entire and complete agreement between the Parties with respect to the privacy and security of Personal Data and supersedes any other agreements, representations, or understandings whether oral or written. All clauses of the Agreement, that are not explicitly amended or supplemented by the clauses of this Addendum, and as long as this does not contradict with compulsory requirements of GDPR and applicable Data Protection Laws, under this Addendum, remain in full force and effect and shall apply, including, but not limited to: Governing Law and Dispute Resolution, Jurisdiction, Limitation of Liability (to the maximum extent permitted by the GDPR).

[Signatures on next page.]

IN WITNESS WHEREOF, this Data Processing Addendum is entered into with effect from the date executed by both Parties (the "**Effective Date**").

Data Processor:
Applied Training Systems, Inc.

By:__________________________________
Name: Julie Rieken
Title: CEO
Date: 06 / 10 / 2022
Email: julie@trakstar.com
Phone Number: 303-882-9113

Data [ ]:
[ ]

By:__________________________________
Name:__________________________________
Title:__________________________________
Date:__________________________________
Email: __________________________________
Phone Number: __________________________

EXHIBIT A
TO
DATA PROCESSING ADDENDUM

STANDARD CONTRACTUAL CLAUSES
[____________________] (CONTROLLER) TO APPLIED TRAINING SYSTEMS, INC. (PROCESSOR)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORIZATION. The data importer has the data exporter’s general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III
LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer 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. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV
FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of ___________________________..

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of ___________________________.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

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: ______________________________________

Address: ____________________________________

Contact person's name, position and contact details: ______________________________________

Activities relevant to the data transferred under these Clauses: ______________________________

Signature and date: ____

Role (controller)

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

Name: Applied Training Systems, Inc.

Address: 113 Cherry St., PMB 57615, Seattle, WA, 98104-2205

Contact person's name, position and contact details: Chris McClave, CTO, legal@trakstar.com

Activities relevant to the data transferred under these Clauses: The data importer is a processor of data exporter's data and will provide services to data exporter as described in more detail in the Agreement.

Signature and date: Christopher R McClave 06 / 10 / 2022

Role (processor)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Categories of data subjects on the Trakstar Platform include Employees, Applicants, Hiring Managers, Trainees, and Trainers.

Categories of personal data transferred:

- Human Resources Data including:
- Employee and Candidate demographic data
- Employee notes and performance reviews, ratings and competencies
- Goal attainment and progress
- 360 reviews
- Employee engagement surveys and results

- Organization structures
- Succession planning information
- Training records, quiz assessment results, and course completion data
- Course content and modules consisting of videos, PowerPoint presentations, audio, text documents, SCORM content
- Files submitted by employees, trainees, and candidates
- Resumes and contact information
- Candidate feedback and email exchanges
- Job descriptions and postings

Sensitive 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:

The Trakstar Platform does not store sensitive data for EU customers or data subjects.

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

Data is transferred to the Trakstar Platform on a continuous basis.

Nature of the processing:

The Trakstar Platform processes the data required to support HR teams with their talent development needs including: applicant tracking and workflow, resume capture and parsing, performance management, goal setting, engagement surveys, training and assessments.

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

The Trakstar Platform provides information storage and retrieval capabilities for Data Controllers under the contractually agreed upon services, for the purpose of talent development. The processing of data subject information is required for Data Controllers to conduct workforce management including applicant tracking, onboarding, learning management, and performance management.

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

Data is retained for the duration of the contract with the Data Controller. At the conclusion of the contract, Data Controllers may request the deletion of data stored by the Trakstar Platform. Trakstar makes no guarantee that data will be retained beyond 30 days from the conclusion of a contract.

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

The Trakstar Platform uses the sub-processors identified in Schedule A-4. Please see that section for a description of the purpose of the processing for each sub-processor and the subject matter.

C. COMPETENT SUPERVISORY AUTHORITY

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

ANNEX II

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

The technical and organizational measures must be described in specific detail and not in generic terms. In particular, clearly indicate which measures apply to each transfer or set of transfers.

1.1. Compliance

1.1.1. Trakstar SOC Reports. Trakstar is audited for compliance with the SOC 2 standard on an annual basis. This comprehensive audit conducted by a licensed CPA firm provides a full accounting of the Trakstar organization and product tools, methods and processes for security, availability, integrity, confidentiality, and privacy. Our SOC 2 report is available to customers upon request.

1.1.2. Trakstar GDPR Compliance. Trakstar is compliant with the EU's General Data Protection Regulation. During 2021, Trakstar (under the parent umbrella organization of Applied Training Systems Inc., and with our former brands Trakstar, Reviewsnap, Recruiterbox, and Mindflash) was certified for the EU-U.S. Privacy Shield Framework. With the Schrems II judgement of July 2020 and subsequent rulings in 2021, Trakstar adapted its compliance to include the Standard Contractual Clauses within our Data Processing Addendum (DPA). We execute DPAs for customers located in the EU or other companies with EU based employees covered by the GDPR.

1.1.3. AWS SOC Reports. The Trakstar products and platforms are hosted on the Amazon Web Services platform. All AWS compliance and audit reports are available to AWS customers, under an NDA. AWS holds multiple certifications including SOC 2, ISO 27001:2013, GDPR, and more. To review the AWS SOC 2 reports, please refer to the AWS Artifact service.

1.2. Organizational

1.2.1. Privacy. The Trakstar team prioritizes customer data privacy and security. We employ a proactive approach to limit access to customer data by Trakstar staff. Our policies, training, and monitoring processes are regularly reviewed and enforced to protect customer data. For more information, see our privacy policy which may be updated from time to time by Trakstar.

1.2.2. Security and Data Policies. Each year, and as warranted, the security team at Trakstar reviews and updates our IT security policies and training program. These policies are distributed to all employees and compliance is mandatory. For data security and handling, employees are required to undergo training which covers the types of data and safeguards that must be taken to protect that data. These security and training programs cover key topics such as change management, asset usage, computer security, password and credential management, loss and theft, usage monitoring, and infrastructure protection. It is the responsibility of all Trakstar employees to handle the integrity and security of customer data.

1.2.3. Security Training. All Trakstar new employees are required to undergo security and awareness training, and to retake that course on an annual basis. Training consists of common mistakes and threats, as well as industry specific concerns related to SaaS companies. Team members are tested and knowledge is verified through a rigorous program of quizzes as well as response to real world threat examples.

1.2.4. Background Checks, Code of Conduct, and Oversight. Employees undergo background checks prior to employment. The process includes verification of criminal records, reference and education checks. For certain personnel, more extensive screening requirements are in place. All employees must also agree to an employee handbook which includes a code of conduct and policies governing use of company equipment, adherence to IT and Security policies and other policies. Applied Training Systems (i.e. Trakstar and the Trakstar brands including Trakstar Hire, Trakstar Learn, Trakstar Perform and Reviewsnap) are overseen by a board of directors that govern the operations and management of the business.

1.3. Infrastructure and Endpoint Security

1.3.1. Cloud Security. All Trakstar products and services are deployed on Amazon Web Services (AWS). The Trakstar engineering team has implemented multiple controls and monitoring/compliance tools to ensure property security procedures are being adhered to including risks such as insecure Security Groups, IAM account credential and encryption key rotation, use of MFA for authentication, secure VPN connection for access to network infrastructure and more. The engineering team has deployed multiple monitoring tools to identify changes and alerts with redundant notifications to team members. Trakstar engineering uses segmented accounts and isolated access credentials to restrict scope and use a least privilege pattern for operational activity.

1.3.2. Encryption. Communications with the Trakstar platform are conducted over the Internet by customers and their users with a minimum TLS 1.2 secured connection. HTTP connections are not permitted. All data in transit is encrypted with this standard or better. Data at rest is encrypted and isolated using strong encryption algorithms. Additionally, all data stored on employee laptops is fully encrypted and redundantly stored and encrypted using backup solutions.

1.3.3. Passwords. Any user with access to production system is required to use complex, long passwords, and secure password management tools with regular rotation. The same policy applies to local laptops and SSO integrated software. Laptops are locked when unattended. Automatic screensavers with password protection are also included. Phishing drills and policies ensure staff are honoring the policies and trained to respond appropriately to security threats.

1.3.4. Network Security. All AWS production accounts utilize firewalls and application threat detection to identify and block threats to the infrastructure or applications. Direct connectivity is prohibited for internal systems. For external facing systems, connectivity is blocked unless explicitly authorized. Networks are separated using VPCs and security groups to isolate systems. For office environments as well as remote staff, all networks are untrusted and treated as a public connection; laptops and all other devices that connect are configured accordingly.

1.3.5. Intrusion Detection and Prevention. The Trakstar engineering team has deployed a suite of tools designed to identify and proactively stop intrusions, scans, and malicious payloads from penetrating our security perimeter. This includes production systems, application security, email, device threats, and rogue user behaviors such as privilege escalation. In addition to these measures, audit trails and logging systems are leveraged to identify and alert on anomalous behaviors. Changes in infrastructure configuration are monitored, alerted, and investigated.

1.3.6. Antivirus. Across the Trakstar portfolio, antivirus and malware protections have been deployed and are monitored to mitigate common threats and vulnerabilities. These systems update frequently with new malware signatures and continuously scan for malicious activity. Implementation on employee laptops is secured and managed remotely by the Trakstar security team.

1.3.7. Identity and Access Management. Following a principle of least privilege, the Trakstar engineering team restricts access to systems to a minimum basis. This includes accounts with privileged access such as system root or admin accounts. In addition, the team monitors privilege and accounts on a monthly basis with alerts that detect unusual activity.

1.3.8. Authentication. Two factor authentication is used across the Trakstar organization. The requirements for 2FA are enforced and reviewed periodically. Acceptable methods include physical tokens such as YubiKeys or app generated passcodes. Staff are also required to use a managed SSO solution for access to devices and systems that support an enterprise SSO integration.

1.4. Physical Security

1.4.1. Offices. Trakstar employees are typically remote, with the exception of a Denver office. Employees are trained on procedures such as VPN access to secure systems, a protocol for handling laptops and reporting any lost or stolen devices. No mission critical systems or sensitive data are maintained within a physical office environment. Employee laptops are fully secured and remotely managed. Access can be revoked and data can be remotely destroyed.

1.5. Security Operations

1.5.1. Vulnerability Management. Several processes and tools are in place to identify, prioritize, and remediate vulnerabilities. Trakstar engineering reviews discovered vulnerabilities which are identified by automated scanning and other methods, to identify the threat level and classification. Vulnerability detection begins at the source code, with scanners equipped to identify threats such as the OWASP Top 10 vulnerabilities.

1.5.2. Patching. A monthly patch cycle is enforced that brings tools, operating systems, and other software current with releases that resolve vulnerabilities. For high severity issues, patching is conducted on demand to remediate any potential threats.

1.5.3. Vulnerability Disclosure Policy. Trakstar publishes a vulnerability disclosure policy, which may be updated from time to time by Trakstar, covering our response to externally identified vulnerabilities. Trakstar does not compensate ethical hackers for their contributions, though they are appreciated. The policy covers expectations, reporting policy, scope, and disclosure methods.

1.5.4. Penetration Testing. All Trakstar products undergo annual penetration testing by a third-party auditor. Trakstar can provide an executive summary of the tests conducted by the auditors, however it is against Trakstar policy to disclose the findings (if any) generated by the penetration test, for security reasons.

1.5.5. Change Management. A change control policy and procedure is used to properly review the impact of any change to code or infrastructure prior to deployment. Procedures exist to ensure multiple staff have reviewed the change and approval has been given by engineering management. All changes are documented and tied to specific change control tickets for audit purposes.

1.5.6. Software Development Process. The engineering group leverages several checkpoints during the software development process to ensure the security and integrity of the Trakstar products. These include pull requests with code reviews, infrastructure as code, isolation of configuration and security parameters to secured storage (parameterized) and a full automated test suite to ensure the quality controls and standards are met. Development is supported by a full ticketing and agile development process to document requirements, the QA process, and deployments.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to Customer and, for transfers from a processor to a sub-processor, to ATSI.

ANNEX III

LIST OF SUB-PROCESSORS

Sub-Processor. Customer has authorized the use of the following sub-processor(s). Data Processor may amend this list and will provide notice to Customer within 10 days of any changes, and Customer shall have 10 days following receipt of such notice to object to the changes. Include the identity and contact details of the Sub-Processor(s), and, where applicable, the Sub-Processor(s) Data Protection Officer:

Name: Chris McClave, CTP

Address: Applied Training Systems, Inc., 113 Cherry St., PMB 57615, Seattle, WA 98104-2205

Contact person's name, position and contact details:

Chris McClave, CTO, legal@trakstar.com

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): (see below in chart)

Signature and Accession Date: Christopher R McClave 06 / 10 / 2022

Subprocessor	Applicability	Product	Processing Activity	Corporate URL
Amazon Web Services	All Customers	All	Hosting infrastructure, database services, encryption, networking	https://aws.amazon.com/compliance/
Atlassian	All Customers	All	Engineering and customer support tickets	https://www.atlassian.com/
Backblaze	All Customers	All	Automated backups of corporate devices	https://www.backblaze.com
BambooHR	Opt-In Integration	Hire	HRIS Provider	https://www.bamboohr.com
Box	All Customers	Learn	Content storage and sourcing for LMS courses	https://www.box.com
Checkr	Opt-In Integration	Hire	Background checks for applicants	https://checkr.com/
CloudAMQP by 84Codes	All Customers	Hire	Software message queues	https://www.cloudamqp.com/
Datadog	All Customers	Learn, Hire	System and Application Logging	https://www.datadoghq.com/

Glassdoor	Opt-In Integration	Hire	Job posting board	https://www.glassdoor.com
GoodData	All Customers	Learn	Trakstar Learn reporting for course completions, trainee performance	https://www.gooddata.com
Google	All Customers	All	Workspace backoffice tools, email, calendar, office productivity	https://workspace.google.com/
Google Analytics	All Customers	All	Website analytics for usage and behavior tracking	https://analytics.google.com/analytics/web/
Help Scout	All Customers	All	Help documentation and ticketing	https://www.helpscout.com/
Honeybadger	All Customers	Perform	Platform exception and error handling and logging	https://www.honeybadger.io/
HubSpot	All Customers	All	Customer leads and contact details, customer records	https://www.hubspot.com/
Indeed	Opt-In Integration	Hire	Job posting board	https://www.indeed.com/
Intercom	All Customers	All	Sales interactions with customers	https://www.intercom.com
MailChimp	All Customers	All	Customer contacts and email addresses for notification emails	https://mailchimp.com
MailGun	All Customers	Hire	Customer contacts and email addresses for notification emails	https://www.mailgun.com
Mongo DB Atlas	All Customers	Hire	Document indexing and data storage	https://www.mongodb.com/
Namely	Opt-In Integration	Hire	HRIS Provider	https://www.namely.com
New Relic	All Customers	All	Software observability and application monitoring platform	https://newrelic.com/
PandaDoc	Opt-In Integration	Hire	Document templates and management	https://www.pandadoc.com

Pendo	All Customers	Perform, Hire	Customer application interactions and behaviors	https://www.pendo.io/
Sage Intacct	All Customers	All	Financial management platform	https://www.sageintacct.com/
Salesforce Interaction Studio	All Customers	Learn	Customer application interactions and behaviors	https://www.salesforce.com/products/marketing-cloud/customer-interaction/
Salesforce Marketing Cloud	All Customers	All	Customer contacts, leads, notes, engagements, etc.	https://www.salesforce.com
Salesforce Slack	Opt-In Integration	Hire	Candidate application notifications	https://www.slack.com
SolarWinds Loggly	All Customers	Hire	Software and infrastructure logging platform	https://www.solarwinds.com/loggly
SolarWinds Papertrail	All Customers	Perform	Software and infrastructure logging platform	https://www.papertrail.com/
Splunk Cloud	All Customers	All	Aggregated logging application	https://www.splunk.com
Stripe	All Customers	Hire	Credit card processing and payments, subscription management	https://www.stripe.com
Twilio SendGrid	All Customers	All	Customer contacts and email addresses for notification emails	https://sendgrid.com/
VMWare Pivotal Tracker	All Customers	Perform	Engineering and customer support tickets	https://www.pivotaltracker.com
Workato	All Customers	All	Communication between HRIS systems and Trakstar	https://www.workato.com
Zapier	Opt-In Integration	Learn	Communication between HRIS systems and Trakstar	https://zapier.com/
Zencoder by Brightcove	All Customers	Learn	Video encoding and compression	https://www.brightcove.com/en/products/zencoder/
Ziggeo	All Customers	Hire	Candidate videos and responses	https://ziggeo.com/

Zoom	Opt-In Integration	Hire	Integration for scheduling interviews and meetings over Zoom	https://zoom.us/
Zuora	All Customers	Learn	New account provision and subscription management	https://www.zuora.com/