Data Processing Addendum Addressing Article 28 GDPR (Processor Terms) and Incorporating Standard Contractual Clauses for Controller to Processor Transfers of Personal Data from the EEA to a Third Country

Version Date: 5 May 2018

This Data Processing Addendum ("**Addendum**") forms part of the Terms and Conditions ("**Principal Agreement**") between: (i) Rebellion Training **("Vendor"** or "**Rebellion Training**"**)** acting on its own behalf and as agent for each Vendor Affiliate; and (ii) You ("**Company**") acting on your own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

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

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Company Group Member**" means Company or any Company Affiliate;

1.1.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.5 "**Contracted Processor**" means Vendor or a Subprocessor;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 below;

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.12 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 13.4;

1.1.13 "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.14 "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

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

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

3. Processing of Company Personal Data

3.1 Vendor and each Vendor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2 not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Company Group Member:

3.2.1 instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal Data to any country or territory,

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

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Vendor and Vendor Affiliate Personnel

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

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for

the rights and freedoms of natural persons, Vendor and each Vendor Affiliate shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. **Subprocessing**

6.1 Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.

6.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this Addendum, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 5 business days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

Neither Vendor nor any Vendor Affiliate shall appoint (nor disclose any Company Personal Data to) the proposed Subprocessor except with the prior written consent of Company.

6.4 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:

6.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.4.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

6.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

6.4.4 provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.5 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Vendor shall:

7.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. **Personal Data Breach**

8.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Company Personal Data

10.1 Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within 30 calendar days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

10.2 Subject to section 10.3, Company may in its absolute discretion by written notice to Vendor within 30 days of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within 30 days of the Cessation Date.

10.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 within 60 days of the Cessation Date.

11. Audit rights

11.1 Subject to sections 11.2 to 11.4, Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiilate undertaking an audit has given notice to Vendor or the

relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or

11.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

11.3.3.1 Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this Addendum; or

11.3.3.2 A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 Vendor warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not a Vendor Affiliate, Vendor's or the relevant Vendor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf of that Subprocessor will have been duly and effectively authorised (or subsequently ratified) by that Subprocessor.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

13.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Company may:

13.4.1 by at least 30 (thirty) calendar days' written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Company gives notice under section 13.4.1:

13.5.1 Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and

13.5.2 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6 If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or

alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

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

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data

Nature and purpose includes cloud based storage, retrieval, support, and authentication of encrypted data designated by Data Exporter for purposes of:

- Service Improvement
- Future Service Development
- Customer Support
- Security, Safety, and Dispute Resolution
- Business Operations
- Communications and Marketing

The personal data transferred concern the following categories of data:

Types of data include first name, last name, street address, city, state, postal code, country, phone number, email address, territory, image, video content, audio content, and the content of your chats and other communications with Rebellion Customer Care.

The categories of Data Subject to whom the Company Personal Data relates

Data subjects include the individuals about whom data is provided to Vendor via the Services (as defined in the Terms of Service and/or Subscription Service Agreement) by (or at the direction of) Data Exporter.

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization is the End User, as defined in the Rebellion Training Subscription Services Agreement (the "SSA") and/or the Terms of Service made by and between End User and Rebellion Training, Inc. End User shall be referred to herein as the Data Exporter. Rebellion Training, Inc. shall be referred to herein as the Data Importer or Rebellion Training. Data Importer and Data Exporter may each be referred to herein as a "Party" or collectively, as the "Parties". These Contractual Clauses (these "Clauses") shall be incorporated into and become a part of the SSA and/or Terms of Service by reference therein.

The Parties HAVE AGREED on the following Clauses in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is:
an individual or business located within the European Union who has selected data importer as its end point storage provider.

Data importer
The data importer is:
a Nevada corporation headquartered in Reno, Nevada USA. The data importer is a global enterprise SaaS provider of video-based training.

Data subjects
The personal data transferred concern the following categories of data subjects:
the individuals about whom data is provided to Vendor via the Services (as defined in the Terms of Service and/or Subscription Service Agreement) by (or at the direction of) Data Exporter.

Categories of data
The personal data transferred concern the following categories of data:
first name, last name, street address, city, state, postal code, country, phone number, email address, territory, image, video content, audio content, and the content of your chats and other communications with Rebellion Customer Care

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

Processing operations
The personal data transferred will be subject to the following basic processing activities:

cloud based storage, retrieval, support, and authentication of encrypted data designated by Data Exporter for purposes of:
Service Improvement
Future Service Development
Customer Support
Security, Safety, and Dispute Resolution
Business Operations
Communications and Marketing

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

The description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Any capitalized term not otherwise defined herein shall have the meaning given in the SSA.

A. Purpose.

This Addendum, in addition to the information security standards set forth in the SSA, describes the minimum information security standards that Rebellion Training shall have and maintain in order to protect Confidential Information and User Data from unauthorized use, access, disclosure, theft, manipulation, reproduction, Security Incident or otherwise during the term of services outlined in the SSA and for any period thereafter during which Rebellion Training has possession of or access to any Confidential Information and/or User Data. Rebellion Training's ongoing adherence to a security program based on an Industry Recognized Framework, as defined below, is a condition to End User doing business with Rebellion Training. The requirements set forth in this Security Exhibit are in addition to any set forth in the SSA. To the extent of any conflicts, this Addendum shall govern.

B. Definitions.

1. Business Continuity Plan:A collection of procedures and information that is developed, compiled and maintained in readiness for use in the event of an emergency or disaster.

2. Change Management: A formal process used to ensure that changes to Rebellion Training hardware, software, and other systems are introduced in a controlled and coordinated manner. This reduces the possibility that unnecessary changes will be introduced, that faults or vulnerabilities are introduced, or that unauthorized changes made by other users are introduced.

3. Confidential Information: Information which may be considered confidential and/or trade secret information which includes information: (i) regarding the Rebellion Training Subscription Services; (ii) that is clearly and conspicuously marked as "confidential" or with a similar designation at time of disclosure; (iii) that is identified as confidential and/or proprietary before, during, or promptly after presentation or communication; and (v) that should be reasonably understood to be confidential or proprietary to a disclosing party, given the nature of the information and the context in which disclosed. The term "Confidential Information" does not include User Data.

4. Data Breach: Any use, disclosure, loss, acquisition of, or access to, User Data that is not in accordance with the terms of the SSA.

5. Industry Recognized Framework: A global industry recognized information security management system ("ISMS"), such as but not limited to ISMS standard ISO/IEC 27001– Information technology – Security techniques – Information security management systems – Requirements, as published by the International Organization for Standardization and the International Electrotechnical Commission ("ISO 27001").

6. Security Incident : means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

7. SOC2: A third-party AICPA report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy. These reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization. These reports are performed using the AICPA Guide: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy and are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls. These reports can form an important part of stakeholders:

- Oversight of the organization;
- Vendor management program;
- Internal corporate governance and risk management processes; and
- Regulatory oversight

8. System: An assembly of components that supports an operational role or accomplishes a specific objective. This may include a discrete set of information resources (network, server, computer, software, application, operating system or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

9. Vendor : Collectively and individually, any third party to whom Rebellion Training intends to grant access to Confidential Information and User Data in accordance with the SSA and this Addendum, including any contractor, offshore service provider, outsourcer, cloud service providers or any platform service provider that may have access to Confidential Information and User Data.

C. Disclosure of Confidential Information and User Data.

Rebellion Training shall not use, access, or disclose Confidential Information and User Data in any manner that would constitute a violation of Applicable Law or SSA terms (including, without limitation, by means of outsourcing, sharing, retransfer, access, or use) to any person or entity, except to: (1) Employees who actually and legitimately need to access or use Confidential Information and User Data in the performance of Rebellion Training's duties under the SSA; or (2) Vendors or contractors after such Third Party has been vetted though an appropriate vendor due diligence process.

D. Use of, Storage of, or Access to, Confidential Information and User Data.

Rebellion Training shall only use, store, or access Confidential Information and User Data: (1) In accordance with and only to the extent permissible under the SSA (including this Addendum); and (2) In full compliance with any and all Applicable Laws.

E. Rebellion Training Privacy Policy.

Rebellion Training shall collect and use personal data in a manner consistent with its privacy policy which can be found at www.rehearsal.com/privacy. Rebellion Training's may change its privacy policy from time to time and its sole discretion.

F. Safeguarding Rebellion Training Data.

Rebellion Training agrees that the use, storage, and access to Confidential Information and User Data shall be performed with the degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. Rebellion Training shall implement and maintain safeguards necessary to ensure the confidentiality, integrity, and availability of Confidential Information and User Data.

Such safeguards shall include as appropriate, and without limitation, the following:

1. Access Control. Rebellion Training must ensure controls restrict unauthorized user access to Confidential Information and User Data. Rebellion Training must use authentication and authorization services to access Confidential Information and User Data. Rebellion Training must provide and ensure IT administrators use separate and unique accounts for administration and non-administration responsibilities.

2. User Access Management. End User authorizes access to Confidential Information and User Data on a need-to-know basis. When the data resides physically or logically within End User-managed environments, Rebellion Training access will be subject to End User's access management policies and procedures. End User must authorize all decisions for access to Confidential Information and User Data residing within End User-managed environments. Rebellion Training may not extend access to Confidential Information and User Data residing within End User-managed environments to third parties without prior written consent. All user accounts used to access Confidential Information and User Data must be unique and clearly associated with an individual user. Rebellion Training must ensure unique assignment of User IDs, tokens, or physical access badges provided to employee or contingent staff. Rebellion Training must ensure all user, System, service, and administrator accounts and passwords are never shared. Rebellion Training is responsible for reviewing authorization privileges assigned to its employees and contingent staff on a quarterly basis to ensure that access is appropriate for the user's functioning role. Access authorization should follow "principles of least privilege." Rebellion Training must ensure procedures exist for prompt modification or termination of access rights in response to organizational changes. Rebellion Training must identify and disable inactive user accounts within 10 business days. Rebellion Training must immediately notify End User in writing if a Rebellion Training employee or Rebellion Training contractor with access to End User-managed Systems terminates, no longer requires access to the End User account, or requires changes to the user account. Notification must include name and User ID of the accounts or Systems the person has access to.

3. Password management & authentication controls. Rebellion Training must ensure Systems that access Confidential Information and User Data have a secure authentication method. Rebellion Training must ensure that access to Confidential Information and User Data meet the following additional requirements at all times: Rebellion Training must encrypt authentication credentials during storage and transmission, Rebellion Training must prohibit its users from sharing passwords, and Rebellion Training must change passwords immediately for accounts suspected of compromise.

4. Remote Access Control. If, in providing agreed upon Support, Rebellion Training requires remote access to End User's Systems, Rebellion Training must always use an End User approved method when connecting. Connecting equipment must implement controls to ensure that Systems maintain current patch levels, have anti-virus software installed with current signatures and scanning engines, and have an operable personal firewall. Remote access equipment must have the capability of meeting End User's security requirements for remote management, encryption, certificate authentication, and credential storage before connecting to End User's network.

5. Network, Operating System, and Application Control. All Rebellion Training Systems or networks connecting to End User networks and/or accessing Confidential Information and User Data must employ safeguard controls capable of monitoring and blocking unauthorized network traffic. Rebellion Training must enable logging on network activity for audit, incident response, and forensic purposes. Where such controls are not available, Systems or networks used to access Confidential Information and User Data must be physically or logically separate from other Rebellion Training networks.

6. Logging of System Use. Rebellion Training must configure all Rebellion Training systems used to access, process, or store Confidential Information and User Data to enable basic forensic accountability. In the case of a Security Incident involving Rebellion Training-supplied laptops, desktops, or removable or portable data storage media used to access, process, or store Confidential Information and User Data, Rebellion Training must provide access to the equipment or media to End User or End User's representatives upon request, along with all relevant encryption/decryption keys necessary to enable forensic analysis, except when the Security Incident involves the actual loss or destruction of the equipment or media. Rebellion Training servers used to access, process, or store Confidential Information and User Data must maintain sufficient audit logging to enable forensic analysis, including logging of Security Incidents, connectivity to services and sessions, and modification to user and configuration settings. Audit logs must be maintained for a minimum of three months. In the case of a Security Incident involving Rebellion Training Systems used to access, process, or store Confidential Information and User Data, Rebellion Training must provide access to the relevant audit logs to End User or End User's representatives upon request to enable forensic analysis.

7. System Security. A System that is owned or supported by Rebellion Training and contains Confidential Information and User Data will be secured as follows:

a. Rebellion Training must establish and maintain configuration standards, which address currently known security vulnerabilities and industry best practices, for all network devices and hosts. These standards must address configuration with all applicable security parameters to prevent misuse. Rebellion Training must remove or disable any non-essential functionality such as scripts, drivers, features, subsystems, or file systems (e.g. unnecessary web servers, default or sample files, etc.). Rebellion Training must ensure that software used in operational systems maintain current level of patching support by its supplier.

b. Rebellion Training must validate and test Software and related application source code against vulnerabilities and weaknesses before deploying code to production. All software development done on behalf of End User must follow a documented software development process or life cycle (SDLC) with appropriate security checkpoints.

c. Rebellion Training warrants that its System is free of any System settings or defects that would create a potential Data Breach.

d. Rebellion Training shall provide to End User in writing the specifications and configuration settings of the System, including: hardware, operating system, applications, communication ports and protocols.

e. The System shall use secure protocols (e.g. SSH, SSL, SFTPS, TLS, IPSec) to safeguard Confidential Information and User Data in transit.

f. If the System may be placed on a public network, the System must be sufficiently protected from compromises and attacks.

g. The System shall not be deployed with default passwords and shall allow the changing of System and user passwords.

8. System Maintenance and Support

a. Rebellion Training will timely review, test, and install patches essential for safeguarding the confidentiality, integrity, or availability of the System or Confidential Information and User Data.

b. Proper Change Management procedures, as defined in the SSA or as otherwise agreed upon by the Parties in writing shall be followed.

c. Rebellion Training shall ensure that the System is supported. Rebellion Training shall provide advanced notice of end of life and support before the System or any components become unsupported.

d. If necessary, Rebellion Training shall provide remote support via a mutually agreed upon secure connection method. Remote access shall be limited to an as needed or as requested basis.

e. On occasion, End User may be required to exchange with Rebellion Training databases or other files containing personally identifiable information, encryption keys, and/or other sensitive information. End User agrees that this exchange will be done in a secure fashion determined by Rebellion Training, limited in its use to only support, and promptly disposed of once the issue precipitating the exchange is resolved. End User, or its administrator or agent, submitting such information: (i) shall be knowledgeable of the information being transmitted, including any sensitivities related thereto, (ii) shall be authorized by End User to submit any such information, and (iii) will consult with End User's internal advisors so as to comply with all Applicable Laws related to the exchange of any such information.

9. Data Protections

a. Rebellion Training shall only use, store, disclose, or access Confidential Information and User Data: i) in accordance with, and only to the extent permissible under the SSA; and ii) in full compliance with any and all Applicable Laws.

b. Rebellion Training shall have documented policies and procedures to prevent unauthorized use, disclosure loss, or acquisition of, or access to, Confidential Information and User Data. This includes, but is not limited to, personnel security measures, such as background checks.

c. All transmission of Confidential Information and User Data between parties shall be performed using a mutually agreed upon secure file transfer method that includes a detailed audit log of events (e.g., who, what, where, when).

d. If any physical media is used by Rebellion Training or its Vendors to store Confidential Information and User Data, Rebellion Training shall protect the Confidential Information and User Data stored on any damaged or physically replaced media by: (i) physically destroying said media device through crushing, shredding, incineration and/or melting, prior to transferring the media device from its location, or (ii) using a digital sanitization tool to sanitize said media device, prior to transferring the media device from its location.

G. Physical and Environmental Security.

Rebellion Training must require that its Vendors implement controls that restrict unauthorized physical access to the data centers that contain equipment used to access Confidential Information and User Data.Rebellion Training must (or require its Vendors to) monitor all areas containing equipment used to access Confidential Information and User Data for attempts at unauthorized access. All secure areas must be enclosed by a perimeter that will deter unauthorized personnel from gaining access, causing damage to or interference with the business processes that take place within that area.Personnel working in secure areas must be easily identified as authorized to work in that area. Rebellion Training must implement and maintain processes to verify that only authorized personnel with an approved business need may be permitted to work in secure areas. Rebellion Training must not allow visitors access to secure areas unescorted.Rebellion Training must ensure proper disposal of all sensitive information using appropriately secured containers for shredding or other approved means.Locked “shred-it” bins must be available in all areas where sensitive information is used in physical form.

H. Incident Response.

1. Discovery, Investigation and Notification of Incident. Upon discovery or notice of any Security Incident, Rebellion Training will:

a. immediately investigate such Security Incident; and

b. notify End User of such Security Incident within a commercially reasonable time following the commencement of its investigation or receipt of notice of such Security Incident.

I. Action Following a Security Incident. Promptly following discovery or notice of any Security Incident, Rebellion Training will take:

a. corrective action to mitigate any risks or damages involved with such Security Incident and to protect the Systems and Confidential Information and User Data from any further compromise; and

b. any other actions that may be required by Applicable Law as a result of such Security Incident.

I. No Surreptitious Code.

Rebellion Training warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorized access to Confidential Information and User Data, or which may restrict End User's access to or use of Confidential Information and User Data.

J. Personnel & Human Resources Security Background & Screening Checks.

To the extent allowed by law and prior to employment only, Rebellion Training will conduct employee background screening. Background checks must be completed and the results deemed satisfactory prior to the employee being assigned to perform Professional Services under the SSA for End User where those Professional Services will involve having access to End User's facilities, Confidential Information or User Data. Upon End User's written request and to the extent allowed by local law, Rebellion Training will attest in writing to its compliance with this paragraph. Rebellion Training should not expose End User to a level of risk which is commercially unreasonable or which is higher than that to which Rebellion Training would be comfortable exposing itself. Individuals whose background checks reveal convictions for violations including computer crimes, fraud, theft, identity theft, or excessive financial defaults will not be permitted access to Confidential Information and User Data.

K. Termination Procedures.

Upon expiration or earlier termination of the SSA, Rebellion Training shall endeavour to ensure that no Security Incident occurs and shall promptly follow the data destruction requirements for Confidential Information and User Data set forth in the SSA. For the avoidance of doubt, the method of destruction shall be accomplished by "purging" or "physical destruction", in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Upon written request, Rebellion Training will promptly certify in writing to End User that such return or destruction has been completed.