STANDARD CONTRACTUAL CLAUSES

FOR

COASTAL TRAINING TECHNOLOGIES CORPORATION AS PROCESSORS

FOR

_____ AS CONTROLLER

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: _____

Address: _____

Tel. _____

("**the data exporter**")

- And –

Name of the data importing organization: **Coastal Training Technologies Corporation ("Coastal")**

Address: 500 Studio Drive, Virginia Beach, VA 23452

Tel. 1-800-861-7668; Facsimile: 757-498-3657

("**the data importer**")

each a '**party**'; together '**the parties**',

HAVE AGREED on the following Contractual Clauses (the 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*.

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[1];

(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

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; EN L 39/10 Official Journal of the European Union 12.2.2010

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 sub-processor 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 sub-processor 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; EN 12.2.2010 Official Journal of the European Union L 39/11

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational 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, unauthorized 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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[2]

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;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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 organizational security measures specified in *Appendix 2* before processing the personal data transferred; EN L 39/12 Official Journal of the European Union 12.2.2010

(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 unauthorized access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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, namely _____.

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

Sub-processing

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 sub-

processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[3]. Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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, namely _____ EN L 39/14 Official Journal of the European Union 12.2.2010

4. The data exporter shall keep a list of sub-processing 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 sub-processor 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 sub-processor 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.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter: _____.

Name (written out in full):.....

Position: .....

Address: .....

Signature .....

On behalf of the data importer; Coastal Training Technologies Corporation:

Name (written out in full): .....

Position: .....

Address: .....

Signature .....

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 _____, who will be implementing online training services for the benefit of their internal employees.

Data importer

The data importer provides training services for the purposes of environmental, health and safety education. It processes the data exporter's personal data in order to administer and track training programs, and to identify learning gaps and opportunities.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Client employees, former employees and contractors

Categories of data

The personal data transferred may concern the following categories of data based upon the service agreement and client's preferences:

Name (first name, last name), language, email address.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

None.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Client data is input into select Coastal systems for the implementation and management of training programs including user registration, user login support, training assignment, generation of training reports including trends and analyses, and delivery of service related communications.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Security Standards

Data Importer maintains and enforces various policies, standards and processes designed to secure personal data and other data to which Data Importer employees are provided access. Following is a description of some of the core technical and organisational security measures implemented by Data Importer:

1. **Information Security Policies and Standards**

The Data Importer will implement security requirements for staff and all subcontractors, vendors, or agents who have access to personal data. These are designed to:

- Prevent unauthorized persons from gaining access to personal data processing systems (physical access control);
- Prevent personal data processing systems being used without authorization (logical access control);
- Ensure that persons entitled to use a personal data processing system gain access only to such personal data as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorization (data access control);
- Ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of personal data by means of data transmission facilities can be established and verified (data transfer control);
- Ensure the establishment of an audit trail to document whether and by whom personal data have been accessed, modified, or removed from systems (entry control);
- Ensure that personal data are Processed solely in accordance with the Instructions of the data controller (control of instructions);
- Ensure that personal data are protected against accidental destruction or loss (availability control);
- Ensure that personal data impacted due to security incidents are managed appropriately.

These rules are kept up to date, and revised whenever relevant changes are made to the information system that uses or houses personal data, or to how that system is organized.

2. **Physical and Environmental Security**

The Data Importer will maintain commercially reasonably security in compliance with ISO 27002-13: 10.1.2.

Standards define controls for: physical perimeter security, physical entry controls, securing work areas and facilities, protecting against external and environmental threats, delivery and loading areas, equipment citing and maintenance, supporting and protecting utilities such as telecommunications and electricity, removal of assets, security of equipment and assets off premises and travelling, secure disposal or re-use of equipment, locking mechanisms of user equipment to prevent unauthorized access and a clear desk and clear screen policy.

3. **Communications and Network Security**

The Data Importer maintains communications and network security in compliance with ISO27002-2013:13.1.1 and ISO27002-2013:10.1, 10.1.1. All company networks will have protection measures employed including but not limited to: logging and monitoring, network and personal firewalls, industry standard techniques for data transmissions and data at rest, intrusion detection and/or prevention mechanisms, and appropriate network authentication based upon risk.

4. Access Control and Asset Management

The Data Importer maintains access controls in compliance with ISO27002-2013:9.1.1.

Access to Company information assets will be controlled through both procedural and technological means. Requirements for access control to company information assets must adhere to relevant legislation or applicable contracts.

Asset owners are responsible for classification and subsequent protection requirements of data within their scope of responsibility. Only authorized staff (asset owners) will determine appropriate access control rules, access rights and restrictions for user roles that may utilize their assets including those assets that use or house personal data. Asset owners must ensure that parties granted access are aware of the security requirements around those information assets.

All employees of the Data Importer are assigned unique User-IDs.

Access rights are implemented adhering to the "least privilege" or "need to know" principle. All access must be reviewed annually to ensure continued business need. Privileged access will be reviewed quarterly.

5. Controls Against Malware

The Data Importer maintains controls against malware in compliance with ISO27002-2013:12.2.1. To protect the integrity of software and information, precautions are required to prevent, detect, and cleanse the introduction of malicious software. The following controls must be applied to all work stations used for Company business:

- A formal policy requiring compliance with software licenses and prohibiting the use of unauthorized software,
- Company supplied anti-virus detection and repair software which must be installed on any work station connected to the Company network,
- Virus definition files on personal computers and servers connecting to the Company network will be updated within 24 hours post release of the new definition files by the anti-virus vendor,
- Hard drives will be scanned for viruses at least weekly,
- Inbound and Outbound eMail to the Internet will be scanned for known viruses,
- Anti-virus software must be configured to activate at boot-up time,
- If supported by anti-virus software, automatic scanning must be enabled including: scan of any inserted portable media device, scan any files on untrusted electronic media or received over untrusted networks before use, and scan any electronic mail attachments and downloads for malicious software prior to use.

6. Personnel Information Security education, training, and awareness

The Data Importer provides information security education, training and awareness in compliance with ISO27002-2013:7.2.2. Security training and awareness will be provided on a recurring basis for all Company personnel by the Information Security Organization. Training plans will be developed and executed based upon roles within the Company and shall be provided to personnel throughout their tenure of work.

The Data Importer implements a security awareness program to train personnel about their security obligations. This program includes training about where to find security information and standards, security contacts, data classification obligations; physical security controls; recognizing security incidents and reporting.

7. Supplier Relationships

The Data Importer assesses suppliers in compliance with ISO27002-2013:15.1.1, 15.1.2. Prior to arranging agreements between the company and other entities, risk assessments will be performed in order to identify potential threats to company information assets. Contractual agreements between the company and third parties must contain security considerations.

8. Incident Management

The Data Importer manages incidents in compliance with ISO27002-2013:16.1.1. Incident Management Procedures will be established to handle all potential types of security events. These procedures will supplement the Business Contingency Plans and cover issues such as:

- Documenting the incident
- Investigating the incident
- Identifying the validity of an incident
- Ensuring proper notification of the events/incident take place in a timely manner
    a. Management
    b. Legal/HR
    c. Law enforcement, as appropriate
    d. Activating appropriate Business Contingency Plans
    e. Collecting audit trails and other supporting information related to the incident
    f. Analyzing the incident
        i. Identifying the cause of the incident
        ii. Identifying contributing causes
        iii. Preparing a report and recommendations to prevent recurrence

9. Business Continuity

The Data Importer maintains business continuity plans in compliance with ISO27002-2013:17.1, 17.1.2. The Company will establish processes to maintain business continuity through the enterprise. These processes will address business impacts ranging from minor business interruptions within a work center through disasters that affect an entire site.

10. Audit and Compliance

The Data Importer conducts internal audits in compliance with ISO27002-2013:18.1.1. Audit areas include but are not limited to safeguarding of organizational records, privacy and protection of personally identifiable information, encryption controls, adherence to security policies and standards, and system and network security.