ENTRUST ACTING AS CONTROLLER OR BUSINESS - GLOBAL

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") supplements the written or electronic agreement(s) (individually and collectively the "**Agreement**") between Entrust (as defined below) and its supplier ("**Vendor**") for the purchase, access to, and/or licensing of products, related services and/or platforms (collectively the "**Services**") by the Entrust entity identified in the Agreement to reflect the parties' agreement with regard to Vendor's Processing of Personal Data on behalf of Entrust. In the event of a conflict between the terms of the Agreement as it relates to the Processing of Personal Data and this DPA, the DPA shall prevail.

This DPA shall be effective for the duration of the Agreement (or longer to the extent required by applicable law).

1. DEFINITIONS

"**Controller**" means the entity that determines the purpose and means of Processing Personal Data.

"**Customer**" means an existing or potential customer of Entrust.

"**Data Protection Laws**" means all applicable data protection and data privacy laws and regulations, including but not limited to the EU General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the California Consumer Privacy Act (CCPA).

"**Data Subject**" means the identified or identifiable person or household to whom Personal Data relates.

"**Entrust**" means the Entrust Corporation entity that is a party to the Agreement.

"**Personal Data**" shall have the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined under Data Protection Laws.

"**Personal Data Incident**" shall have the meaning assigned by Data Protection Laws to the terms "security incident," "security breach" or "personal data breach" and shall include any situation in which Vendor becomes aware that Personal Data has been or is likely to have been accessed, disclosed, altered, lost, destroyed or used by unauthorized persons, in an unauthorized manner.

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

"**Processor**" means the entity that Processes Personal Data on behalf of the Controller.

"**Subprocessor**" means any entity appointed by the Processor to Process Personal Data on behalf of the Controller.

2. DATA PROCESSOR OBLIGATIONS

2.1. **Roles of the Parties**. Subject to the paragraph below in this section 2.1, the parties acknowledge and agree that regarding the Processing of Personal Data under the Agreement, Entrust is the Controller and Vendor is the Processor.

Vendor as Subprocessor. Where Vendor receives Customer information from Entrust, Vendor will serve as a Subprocessor and will Process Customer Personal Data in accordance with the terms of this DPA as if it were a Processor.

2.2. **Vendor's Processing of Personal Data**. Vendor shall treat Personal Data as confidential and shall only Process Personal Data on behalf of and in accordance with Entrust's instructions and for the following purposes: (i) Processing in accordance with the Agreement and (ii) Processing to comply with other documented reasonable instructions provided by Entrust where such instructions are consistent with the terms of the Agreement. Vendor shall immediately inform Entrust if, in Vendor's opinion, an instruction is in violation of Data Protection Laws. For the avoidance of doubt, Vendor will not collect, retain, use, sell, or otherwise disclose Personal Data for any purpose other than for the specific purpose of performing the Services.

2.3. **Details of the Processing.** The subject matter of Processing Personal Data by Vendor is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data Processed and the categories of Data Subjects for whom Personal Data is Processed are set forth in Schedule 1.

2.4. **Personnel**. Vendor shall ensure only authorized personnel who have undergone appropriate training in the protection and handling of Personal Data, and are bound in writing to respect the confidentiality of Personal Data, have access to Personal Data.

2.5. **Security Controls**. Vendor shall implement appropriate technical and organizational measures to maintain the security, confidentiality and integrity of Personal Data, including measures designed to protect against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data.

2.6. **Data Subject Requests.** Vendor shall, to the extent legally permitted, promptly notify Entrust of any requests from Data Subjects seeking to exercise their rights under Data Protection Laws and, taking into account the nature of the Processing, assist Entrust by implementing appropriate technical and organizational measures, insofar as this is possible, to assist with Entrust's obligation to respond to such requests. To the extent that Personal Data is not accessible to Entrust, in its use of the Services, Vendor shall, where legally permitted and upon Entrust's request, provide commercially reasonable efforts to assist Entrust in responding to such requests if responses to such requests are required by Data Protection Laws.

2.7. **Data Protection Impact Assessment.** Vendor shall, upon Entrust's written request and taking into account the nature of Processing and information available, provide reasonable assistance to Entrust in connection with obligations under Articles 32 and 36 of the GDPR or equivalent provisions under Data Protection Laws.

2.8. **Return or Deletion of Personal Data.** Vendor shall, upon Entrust's written request, promptly destroy or return any Personal Data after the end of the provision of Services, unless storage of the Personal Data is required by applicable law.

2.9. **Data Processor Point of Contact**. If Entrust has any questions regarding Processing of Personal Data by Vendor, Entrust may send such questions to the following email: _____.

3. SUBPROCESSORS

3.1. **Appointment of Subprocessors**. Entrust acknowledges and agrees that Vendor may engage Subprocessors in connection with provision of the Services. Vendor shall enter into a written agreement with any engaged Subprocessor that contains data protection obligations no less protective than those contained in this DPA.

3.2. **List of Current Subprocessors**. Vendor shall make available to Entrust the current list of Subprocessors for the Services. The Subprocessor list shall include the identities of all Subprocessors and their country of location.

3.3. **Notification of New Subprocessors.** Vendor will notify Entrust in writing of any changes to this list of Subprocessors.

3.4. **Objection to New Subprocessors**. Entrust may object to Vendor's use of a new Subprocessor by notifying Vendor in writing within ten (10) business days after receipt of Vendor's communication advising of the new Subprocessor. In the event Entrust reasonably objects to the use of a new Subprocessor, Vendor will use reasonable efforts to address Entrust's objections. If Vendor is unable to make available such change within a reasonable period, which shall not exceed ninety (90) days, Entrust may, in its full discretion, terminate the applicable Agreement in full or with respect only to those Services which cannot be provided by Vendor without the use of the objected-to new Subprocessor by providing written notice to Vendor. Vendor will refund Entrust any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Entrust.

3.5. **Liability.** Vendor shall be liable for the acts and omissions of its Subprocessors to the same extent Vendor would be liable if performing the services of each Subprocessor directly under the terms of this DPA.

4. PERSONAL DATA INCIDENTS

4.1. Vendor shall notify Entrust without undue delay (and in any event within forty-eight (48) hours) after becoming aware of a Personal Data Incident. Vendor shall identify the cause of

such Personal Data Incident and take those steps necessary in order to remediate the cause of such a Personal Data Incident.

5. INTERNATIONAL DATA TRANFERS

5.1. **Personal Data Transfers**. Entrust agrees to allow transfer of Personal Data outside the country from which it was originally collected provided that such transfer is required in connection with the provision of Services under the Agreement and such transfers take place in accordance with Data Protection Laws, including, without limitation, completing any prior assessments required by Data Protection Laws.

5.2. **European Specific Provisions.** Where Vendor transfers Personal Data collected in the European Economic Area to a country outside of the European Economic Area and without an adequacy finding under Article 45 of the GDPR, at least one of the transfer mechanisms listed below shall apply:

5.2.1. **Binding Corporate Rules**. To the extent Vendor has adopted Binding Corporate Rules, it shall maintain such rules and promptly notify Entrust in the event that the rules are no longer a valid transfer mechanism between Vendor and Entrust.

5.2.2. **EU Standard Contractual Clauses**. The EU Standard Contractual Clauses pursuant to 2010/87/EU (the European Commission's decision 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (the "EU Standard Contractual Clauses"). The EU Standard Contractual Clauses (Schedule 2) are hereby incorporated in their entirety into this DPA and, to the extent applicable, Vendor shall ensure that its Subprocessors comply with the obligations of a data importer (as defined in the EU Standard Contractual Clauses). To the extent there is any conflict between this DPA and the EU Standard Contractual Clauses, the terms of the EU Standard Contractual Clauses shall prevail.

6. CERTIFICATIONS AND AUDITS

6.1. Upon written request by Entrust, Vendor, to the extent that it is acting as a Data Processor to Entrust, shall make available to Entrust all information necessary to demonstrate compliance with the obligations set forth under Data Protection Laws, provided that Vendor shall have no obligation to provide commercially confidential information. On no more than an annual basis, Vendor shall, to the extent that it is acting as a Data Processor to Entrust, following a request by Entrust and at Entrust's expense, further allow for and contribute to audits and inspections by Entrust or its authorized third-party auditor. The scope, timing, cost and duration of any such audits, including conditions of confidentiality, shall be mutually agreed upon by Vendor and Entrust prior to initiation. Such agreement will not be unreasonably withheld or delayed by Vendor. Entrust shall promptly notify Vendor with information regarding non-compliance discovered during the course of an audit, and Vendor shall use commercially reasonable efforts to address any confirmed non-compliance.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: EU Standard Contractual Clauses

Schedule 3: Information Security Requirements

The parties' authorized signatories have duly executed this DPA:

On behalf of Vendor:

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

On behalf of Entrust:

Name (written out in full): **Lisa J. Tibbits**

Position: **Chief Legal and Compliance Officer**

Address: **1187 Park Place, Shakopee, Minnesota 55379-3817 USA**

Signature: 

SCHEDULE 1 - DETAILS OF PERSONAL DATA PROCESSING

Nature and Purpose of Processing

Vendor will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Services-related documentation, and as further instructed by Entrust in its use of the Services.

Duration of Processing

Vendor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or required by applicable law.

Categories of Data Subjects

Entrust may submit Personal Data to Vendor, the extent of which is determined and controlled by Entrust in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

For vendors that supply a product, service or solution to Entrust for incorporation into Entrust products, services or solutions:

- Customers
- Customers' employees, clients, agents and subcontractors
- Customer's end users authorized by Customer to use Entrust products, services or solutions

For vendors that supply a product, service or solution to Entrust personnel:

- Entrust personnel
- Customers
- Entrust suppliers or contractors

Categories of Personal Data

Entrust may submit Personal Data to Vendor, the extent of which is determined and controlled by Entrust in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Personal Data related to or relevant to the employment of Entrust personnel
- Business contact details of Customers, suppliers and contractors (name, title/position, address, telephone number, fax number, email address, location)
- Connection data (IP address, username, ID data used for authentication purposes)
- Any other personal data required to be processed in relation to the Services

SCHEDULE 2 – EU STANDARD CONTRACTUAL CLAUSES

These Standard Contractual Clauses are attached to and made part of the DPA.

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.

The data exporter and data importer are as defined in Appendix 1 to this Schedule 2, and

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;

(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:

(e) 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,

(f) any accidental or unauthorised access, and

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

(h) 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;

(i) 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;

(j) 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;

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

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

(m) 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 or 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 its third-party beneficiary 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 has been agreed by the parties by virtue of their signing the DPA.

Data exporter

The data exporter is Entrust.

Data importer

The data importer is the legal entity that has executed the DPA and as a result has accepted the Clauses as a data importer.

Data subjects

The personal data transferred concern the following categories of data subjects:

- See Schedule 1

Categories of data

The personal data transferred concern the following categories of data:

- See Schedule 1

Processing operations

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

- The performance of the Services pursuant to the Agreement

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and has been agreed to by the parties by virtue of their signing the DPA.

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

[TO BE COMPLETED BY VENDOR. At a minimum, vendor must adhere to Entrust's Schedule 3 requirements. See next page.]

SCHEDULE 3

Information Security Requirements

Third Party will, and will cause any of its affiliates and subsidiaries to, adhere to the following operational procedures and responsibilities. Any reference to Third Party herein shall also include its Affiliates.

1. Definitions

"**Entrust**" refers to Entrust Corporation as well as its affiliates and subsidiaries.

"**Entrust Data**" means any information, household data, or products (including source code), (including, information and data of Entrust customers, partners, licensors, contractors, or other service providers in Entrust's possession or control) provided by Entrust to Third Party. Without limiting the generality of the foregoing, Entrust Data shall include information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable data protection laws and regulations).

"**Third Party**" means an individual or organization and its affiliates and subsidiaries that is involved in a transaction but is not one of the principals and has a lesser interest.

"**Third Party Systems**" shall mean any Third Party computer system, network, or software that accesses, maintains, stores or transmits Entrust Data.

"**Security Incident**" means the attempt or successful unauthorized access, use, disclosure, modification, or destruction of Entrust Information or interference with the operations of any of the Third Party Systems.

"**Breach**" means a Security Incident that results in confirmed disclosure of Entrust Data to an unauthorized party.

2. Access Control and Authorization

Third Party agrees to protect and maintain the security of Entrust Data with commercially reasonable security measures commensurate with the sensitivity of the Entrust Data.

Third Party shall not permit access to Entrust Data by any individual or entity, other than Third Party personnel or subcontractors (provided Entrust has been notified of and has not objected to the use of the subcontractor) with a need to know in order for Third Party to provide services or deliverables to Entrust.

Third Party agrees not to use any tracking software in the provision of Services or Deliverables to Entrust.

3. Privacy/Compliance

Third Party shall implement appropriate procedures to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

Third Party agrees to implement policies and procedures to protect against reasonably foreseeable access to, or disclosure of, Entrust Data, and to prevent other reasonably foreseeable events that would result in substantial harm to Entrust.

4. Encryption and Key Management

Third Party shall have a policy and process for managing encryption keys which shall include security requirements for key creation, use, storage, and protection.

Third Party shall use industry standard encryption technologies for data contained within, accessed by, or transmitted through the Third Party Systems.

5. Security Incident Response and Notification

Third Party shall establish responsibilities and procedures to ensure a quick, effective and orderly response to Security Incidents and Breaches.

If there is a Breach, Third Party will (a) notify Entrust without unreasonable delay of confirmation of the Breach, (b) reasonably cooperate with Entrust with respect to any such Breach, and (c) take appropriate corrective action to mitigate any risks or damage involved with the Breach to protect Entrust and Entrust Data from further compromise. Third Party will contact the Entrust Security Operations Center (SOC) at soc@entrust.com or via phone at 855-892-8631 or 952-988-2021. Third Party will take any other actions that may be required by applicable law as a result of the Breach.

6. Security Program

Third Party shall maintain a written security program that (a) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Entrust Data, and (b) complies with all applicable laws. Third Party shall further implement, maintain and comply with generally accepted industry best practices for security monitoring of sensitive data.

7. Security Training & Awareness

Third Party shall maintain a security awareness training program to educate personnel who support the handling and/or processing of Entrust Data about their responsibilities and give them direction for creating and helping to maintain a secure workplace and security for Entrust Data.

8. Threat and Vulnerability Management and Security Testing

Third Party shall maintain a Threat and Vulnerability Management (TVM) program to monitor for vulnerabilities in the Third Party Systems that are acknowledged by vendors, reported by researchers, or discovered through vulnerability scans and personnel identification. Third Party shall provide Entrust with such information about technical vulnerabilities of the Third Party Systems and shall explain to Entrust in detail Entrust's exposure to such vulnerabilities. Third Party shall evaluate such incidents and take appropriate measures to address the associated risk. Upon request, Third Party shall provide Entrust with a validation of an independent third party vulnerability scan and penetration scan which will include a listing of the number of critical and high vulnerabilities as well as an attestation of remediation of these findings.

9. Change Management

Third Party shall maintain documented change management policies and procedures for requesting, testing, and approving Third Party Systems related changes.

Third Party shall maintain a dedicated environment separate from production for development and testing activities, and logical access controls requiring two-factor authentication and shall secure these separate environments.

10. Secure Development

Third Party shall establish and maintain a secure development lifecycle ("SDL") methodology to govern the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components. Third Party shall also limit access privileges to these source code repositories to authorized employees only.

11. Network Security

Third Party shall maintain a network perimeter defense solution, including an intrusion prevention system ("IPS") and firewalls, to monitor, detect, and prevent malicious network activity.

12. Entrust Security

Third Party agrees to communicate in writing any change in security and confidentiality requirements and operational responsibilities to Entrust. Third Party will contact Entrust Information Security team at infosec@entrust.com with the documented changes.

13. Entrust Security Audit

Upon Entrust's written request, and subject to the confidentiality obligations set forth in the Agreement, Third Party shall allow periodic security audits. Entrust may contact Third Party in accordance with the "Notices" Section of the Agreement (or as otherwise mutually agreed in writing) to request (no more frequently than once per calendar year during the Term of the Agreement) an on-site audit of Third Party's procedures relevant to the security controls listed in this Schedule 3. Before the commencement of any such on-site audit, Entrust and Third Party shall mutually agree upon the scope, timing, and duration of the audit. The audit shall be conducted at Entrust's sole cost and expense unless material non-compliance by Third Party is found, in which case Third Party shall bear the expense of the audit. Entrust shall promptly notify Third Party with information regarding any noncompliance discovered during the course of an audit, and Third Party shall use commercially reasonable efforts to address any confirmed non-compliance.

14. Entrust Risk Assessment

Third Party shall periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Entrust Data handling and processing. Third Party shall document the results of these evaluations and any remediation activities taken in response to such evaluations, and upon request Third Party shall provide Entrust the documented evaluations and remediation activities.

15. Business Continuity Management

Third Party will, at its sole expense, establish and maintain (i) written business continuity plans for the services and supporting facilities; (ii) written disaster recovery plans for critical technology and systems infrastructure; and (iii) proper risk controls (collectively, the "Contingency Plans") to enable continued performance under this Agreement in the event of a disaster or other unexpected break in services. Third Party will update and test the operability of any applicable contingency plan at least annually, and will maintain each such plan upon the occurrence of a disaster event. As used herein, a disaster is defined as an unanticipated incident or event, including, without limitation, force majeure events, technological accidents, or human-caused events, that may cause a material service or critical application to be unavailable without any reasonable prediction for resumption, or that causes data loss, property damage or other business interruption without any reasonable prediction for recovery, within a commercially reasonable time period.

16. Third Parties

Third Party shall ensure that any agent, including a subcontractor, to whom Third Party provides Entrust Data agrees to maintain reasonable and appropriate safeguards to protect such Entrust Data; provided, however, that Third Party shall not assign or delegate any obligation of Third Party owed to Entrust under this Schedule 3.