[EDC ACTING AS PROCESSOR - GLOBAL]

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") supplements and forms part of the written or electronic agreement(s) (individually and collectively the "**Agreement**") between Entrust Datacard (as defined below) and Customer (as defined below) for the purchase, access to, and/or licensing of products, services and/or platforms (collectively the "**Services**") to reflect the parties' agreement with regard to the Processing (as defined below) of Personal Data (as defined below). 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).

In the course of providing the Services to Customer pursuant to the Agreement, Entrust Datacard may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

1. DEFINITIONS

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer**" means the entity that is a signatory to the Agreement.

"**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 Protection Policy" means Entrust Datacard's Data Protection Policy, as updated from time to time, and accessible on www.entrustdatacard.com.

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

"**Entrust Datacard**" means the Entrust Datacard entity that is a signatory 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 Entrust Datacard becomes aware that Personal Data has 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 a Processor engaged by Entrust Datacard to process Personal Data for which Entrust Datacard is a Processor.

2. PERSONAL DATA PROCESSING

2.1. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data under the Agreement, Customer is the Controller and Entrust Datacard is the Processor.

2.2. **Customer's Instructions for the Processing of Personal Data.** Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

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

2.4. **Details of the Processing.** The subject matter of Processing of Personal Data by Entrust Datacard 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.

2.5. **Personnel**. Entrust Datacard 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.

2.6. **Security Controls**. Entrust Datacard 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.

2.7. **Data Subject Requests.** Entrust Datacard shall, taking into account the nature of the Processing, assist the Customer, as Data Controller, by appropriate technical and

organizational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests from a Data Subject exercising his/her/their rights under Data Protection Laws.

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

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

2.10 **Data Processor Point of Contact**. If Customer has any questions regarding Processing of Personal Data by Entrust Datacard, Customer may send such questions to the following email: privacy@entrustdatacard.com.

3. SUBPROCESSORS

3.1. **Appointment of Subprocessors**. Customer acknowledges and agrees that Entrust Datacard may engage Subprocessors in connection with provision of the Services. Entrust Datacard 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**. The current list of Subprocessors for the Services can be found at www.entrustdatacard.com/sub-processors.

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

3.4. **Objection to New Subprocessors**. Customer may object to Entrust Datacard's use of a new Subprocessor by notifying Entrust Datacard in writing within ten (10) business days after receipt of Entrust Datacard's communication advising of the new Subprocessor. In the event Customer reasonably objects to the use of a new Subprocessor, Entrust Datacard will use reasonable efforts to address Customer's objections. If Entrust Datacard is unable to make available such change within a reasonable period, which shall not exceed ninety (90) days, Customer may terminate the applicable Agreement with respect only to those Services which cannot be provided by Entrust Datacard without the use of the objected-to new Subprocessor by providing written notice to Entrust Datacard. Entrust Datacard will refund Customer 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 Customer.

3.5. **Liability.** Entrust Datacard shall be liable for the acts and omissions of its Subprocessors to the same extent Entrust Datacard would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

4. PERSONAL DATA INCIDENTS

4.1. Entrust Datacard shall notify Customer without undue delay after becoming aware of a Personal Data Incident. Entrust Datacard shall identify the cause of such Personal Data Incident and take those steps reasonably necessary in order to remediate the cause of such a Personal Data Incident.

5. INTERNATIONAL DATA TRANFERS

5.1. **Personal Data Transfers**. Customer 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 Entrust Datacard 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, Entrust Datacard shall transfer Personal Data 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, Entrust Datacard 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. On no more than an annual basis and upon thirty (30) days' notice in writing by Customer, Entrust Datacard, to the extent that it is acting as a Data Processor to Customer, shall make available to Customer information necessary to demonstrate compliance with the obligations set forth under Data Protection Laws, provided that Entrust Datacard shall have no obligation to provide confidential and/or proprietary information. On no more than an annual basis and upon thirty (30) days' notice in writing, Entrust Datacard shall, to the extent that it is acting as a Data Processor to Customer, following a request by Customer and at Customer's expense, further allow for and contribute to off-site audits and inspections by Customer 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 Entrust Datacard and Customer prior to initiation. Customer shall promptly notify Entrust Datacard with information regarding non-compliance discovered during the course of an audit, and Entrust Datacard 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

The parties' authorized signatories have duly executed this DPA:

On behalf of Customer:

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

On behalf of Entrust Datacard:

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

Position: **General Counsel**

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

Signature: 

SCHEDULE 1 - DETAILS OF PERSONAL DATA PROCESSING

Nature and Purpose of Processing

Entrust Datacard 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 Customer in its use of the Services.

Duration of Processing

Entrust Datacard will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or as required by applicable laws.

Categories of Data Subjects

Customer may submit Personal Data to Entrust Datacard, the extent of which is determined and controlled by Customer in its sole discretion (but in accordance with Data Protection Laws) , and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's employees, clients, agents and subcontractors
- Customer's end users authorized by Customer to use the Services

Categories of Personal Data

Customer may submit Personal Data to Entrust Datacard, the extent of which is determined and controlled by Customer in its sole discretion (but in accordance with Data Protection Laws), and which may include, but is not limited to the following categories of Personal Data:

- Business contact details (name, title/position, address, telephone number, fax number, email address, location) of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use the Services
- Connection data (IP address, username, ID data used for authentication purposes) of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use 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 described 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 it 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 Agreement.

Data exporter

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

Data importer

The data importer is Entrust Datacard.

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 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):

Reliability of Personnel: Entrust Datacard conducts background checks on all employees before employment, and employees and contractors receive information security training during onboarding as well as on an ongoing basis. All employees are required to read and sign Entrust Datacard's information security policies.

Compliance, audits, and certifications: Entrust Datacard, with the full commitment of its senior leadership, strongly believes that the fundamental principle to its success in innovation is its information security strategy. This strategy is based on adherence to enterprise-wide world-class governance, a set of controls and strict compliance with federal, financial, international, and industry regulations and policies such as:

- ISO 27001
- NIST 800-53
- Certificate Authority Browser (CAB) Forum Webtrust (may not apply for some products)

To ensure that the information security strategy is effective, Entrust Datacard enforces information security policies and procedures across its entire organization, as well as all business and technical projects. Governance, Risk and Compliance (GRC), Threat and Vulnerability Management (TVM), Security Architecture, Security Operations Center, Disaster Recovery, Business Continuity and Incident Response are the integral components of this strategy.

Incident Response:

At an operational level, Entrust Datacard has instituted a Security Incident Response Plan to oversee data security events identified or detected by the various technologies used to monitor and alert based on specific thresholds or circumstances. The objectives of the Security Incident Response Plan are to manage and coordinate data security incidents throughout all aspects of the Entrust Datacard computing environment regardless of location, product or process, as well as provide opportunities for educating our colleagues on risks and security controls in place.

Security Operation Center (SOC):

Entrust Datacard is committed to protecting the interest of stakeholders by maintaining a robust Security Operation Center (SOC). The SOC is a centralized unit that monitors the confidentiality, integrity, and availability of information technology infrastructure and deals with security on an organizational level.

Threat and Vulnerability Management (TVM):

Entrust Datacard has a continuous vulnerability discovery and remediation program. This process is built on industry certified tools and procedures and is facilitated by competent and experienced professionals. The Threat and Vulnerability Management (TVM) controls and measures are audited several times a year by qualified auditors to ensure we are compliant with applicable laws and industry standard frameworks.

Disaster Recovery:

Entrust Datacard is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust Datacard therefore maintains a comprehensive organization-wide business continuity program to protect staff, safeguard corporate assets and environments, and to ensure continuous availability of its products and services. To support the Business Continuity Program, Entrust Datacard also maintains a Crisis Communications and Incident Response Plan to help strengthen our emergency response capability.

Business Continuity:

Entrust Datacard is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust Datacard therefore maintains a comprehensive organization-wide Business Continuity Program that is consistent with the guidance issued by the (U.S.) National Fire Protection Association (NFPA) 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs, and (International) ISO 22301 – Societal security – Business continuity management systems standards. The Business Continuity Plan identifies the functional roles and responsibilities of internal and external agencies, organizations and departments.

Product Security Pipeline Standard:

This document is a component of Entrust Datacard's information security program that includes Secure Software Delivery Lifecycle (SDLC) and vulnerability management as well as minimum baseline development (where applicable) for software and firmware products enterprise-wide. Vulnerability identification and remediation are a central focus with the goal to minimize the number of security flaws in Entrust Datacard products and services, and to minimize the impact to Customer when such flaws are discovered. The processes described herein apply to Entrust Datacard products and services and components of a partner system that may be used in conjunction with an Entrust Datacard product or service. The program will ensure that SDLC processes are consistent with Entrust Datacard information security goals and expectations. Additionally, system baselines will be established to support Entrust Datacard software and firmware within the lifecycle (e.g., source repositories) and to support deployment into production environments. Where practical, system baselines will be aligned with compliance requirements.

Network Security:

Entrust Datacard maintains access controls and policies to manage what access is allowed to the Entrust Datacard network and systems from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Entrust Datacard will maintain corrective action and incident response plans to respond to potential security threats.

Physical and Environment Security:

Entrust Datacard facilities hosting technology information assets are equipped with appropriate controls to restrict physical access to the facility. Physical entry controls include a means to identify personnel and visitors, and ensure the individual is authorized to access the secured area prior to entry. All entry to secured areas are logged and logs reviewed periodically. Personnel are informed of, and subject to, the guidelines established for working within secured areas. Access points such as delivery or loading areas, and other points where unauthorized persons may enter the facility, are controlled to restrict further entry, and, to the extent it is practical, isolated from information processing areas. Physical security measures include the capability to monitor company facilities to detect unauthorized or unlawful use. Entrust Datacard has a physical security plan that incorporates a defined procedure to report suspicious activity, identified security weaknesses, or potential security events, as well as an escalation procedure to communicate events to local law enforcement as appropriate. Facility staff and visitors are informed regarding these physical security procedures and their responsibility to report security events.

Information Transfer Policy:

Information to be transferred shall at all times be properly secured, in accordance with its classification, regardless of the media employed to carry the information or the transmission mechanism. All information to be transferred shall be subject to inspection for malicious software code and other potential hazards to confidentiality, integrity or availability. When the use of encryption is required for safekeeping, such use shall be subject to all applicable security requirements as well as legal or regulatory controls. Information to be transferred shall be subject to established retention and disposal requirements. Information transfer facilities shall comply with all applicable laws and regulations. Information and software shall not be transferred with external parties until all relevant contractual and security requirements are satisfied, including formal written agreements where required.