Data Privacy and Security Addendum ("DPSA") to the Purchase Order agreed between the Buyer and the Seller (the "Agreement")

This DPSA shall be incorporated into and form part of the Agreement between Buyer and Seller, under which Agreement Seller provides the agreed Services to Buyer. Terms not defined herein shall have the meaning set forth in the Agreement. In the event of a conflict between the DPSA and Agreement, the terms and conditions of the DPSA shall prevail with regard to the parties' data protection obligations.

All Buyer Data shall be deemed "Confidential Information" under the Agreement. The parties' confidentiality obligations under this DPSA shall survive five years after the termination or expiration of the Agreement, except that Personal Data must be treated as Confidential Information in perpetuity.

1. Definitions.

1.1 "Buyer Data" means non-public or proprietary information and data in any form, including Personal Data and Highly Restricted Data, provided by Buyer and its authorized agents or subcontractors or otherwise Processed by Seller personnel in connection with the provision of goods and/or services under this Agreement.

1.2 "Controller or Data Controller" means the party which alone or jointly with others has the authority to make decisions with respect to the Processing of Personal Data, in particular the authority to determine the purposes and the means of the Processing of such Personal Data.

1.3 "Data Protection Laws" means the provisions of mandatory law of a country containing rules for the protection of individuals with regard to the Processing of Personal Data.

1.4 "Data Subject": shall mean the person to whom the Personal Data relates.

1.5 "EEA": shall mean the European Economic Area.

1.6 "EU Data Protection law": shall mean: (i) up to 25 May 2018, the Data Protection Directive 95/46/EC; and (ii) from 25 May 2018 onwards the General Data Protection Regulation (EU) 2016/679 **("GDPR")**

1.7 "Highly Restricted Data" shall mean Social Security or other government issued identification numbers, medical or health information, account security information, unique biometric identifiers, individual financial account information, credit/debit/gift or other payment card information, account passwords, individual credit and income information, intellectual property, proprietary business models, pricing, customer infrastructure/system information or data flows.

1.8 "Personal Data" shall mean any data relating to (i) an identified or identifiable natural person or (2) an identified or identifiable legal entity, where such information is protected similarly as personal data under applicable Data Protection Laws.

1.9 "Personal Data Breach" shall mean (i) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed and/or (ii) any security breach and any incident that compromises the security, integrity, confidentiality or availability of Buyer Data or Buyer systems.

1.10 "Process" or "Processing" or "Processed" means any operation or set of operations performed or to be performed upon Buyer Data or upon Personal Data, whether or not by automatic means, such as creation, access, collection, recording, organization, structuring, storage, loading,

employing, adaptation or alteration, retrieval, consultation, displaying, use, disclosure by transmission, granting remote access, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure or destruction.

1.11 "Processor or Data Processor" means the party which processes Personal Data on behalf of the Controller. In certain cases, it may also qualify as Subprocessor.

1.12 "Services" shall mean the services provided or to be provided under the Agreement.

1.13 "Subprocessor": shall mean the Seller and/or a third party entity engaged by Seller as a Processor under this DPSA and approved by the Controller (as appropriate).

1.14 "Valid transfer mechanism": shall mean a data transfer mechanism permitted by EU Data Protection Laws a lawful basis for transferring Personal Data to a recipient outside the EEA.

2. Compliance with Laws, Data Ownership of Personal Data

2.1 Seller shall comply with all Data Protection laws applicable to Seller in connection with the provision of the Services and Buyer shall comply with all Data Protection Laws applicable to Buyer in connection with its receipt of the Services.

2.2 As between the parties, all Buyer Data remains, at all times, the property of Buyer.

3. Seller's Obligations

3.1 For the purposes of this DPSA:

a) other than Buyer Data for which Buyer's clients are Data Controllers, Buyer and its affiliates shall be the Data Controllers of Buyer Data; and

b) Buyer and its affiliates shall be Data Processors of Buyer Data for which Buyer's clients are Data Controllers; and

c) Seller shall be a Data Processor of Buyer Data where Buyer is a Data Controller of that data and a Subprocessor of Buyer Data where Buyer is a Data Processor of that data.

3.2 Seller shall Process Personal Data in accordance with Buyer documented instructions as set out in Annex I. Buyer may provide additional instructions to Seller to Process Personal Data. Seller shall not process the Personal Data for any other purpose, including but not limited to marketing Seller's products or services, unless specifically instructed by Buyer in writing. Seller shall immediately inform Buyer if it cannot comply with an instruction or, in its opinion, an instruction infringes applicable Data Protection laws.

3.3 To the extent Seller is authorized by Buyer to collect Personal Data directly from individuals in connection with the provision of the Services under the Agreement, Seller shall provide a privacy notice in an intelligible and easily accessible form, using clear and plain language and obtain explicit consent, if required, in accordance with applicable laws. The notice, at a minimum, should describe the purpose of the collection, intended use, disclosure of collected Personal Data, how the Personal Data will be protected, and the right to withdraw consent, if consent is the basis for Processing.

3.4 Seller shall encrypt Highly Restricted Data at all time, including at time of collection, and during use, transmission and storage.

3.5 Seller shall maintain records of Processing activities, including, but not limited to,

a) the name and contact details of the Seller and any other subcontractors and, where applicable, of the Buyer' or Seller's representative, and the data protection officer;

b) the categories of Processing carried out on behalf of Buyer;

c) where applicable, information on cross-border transfers, including transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers outside of the legally specified transfer mechanisms, the documentation of suitable safeguards for the Personal Data; and

d) a general description of the technical and organizational measures. Seller agrees to make such records of Processing available upon request to Buyer and regulators.

3.6 The records referred to above shall be in writing, including in electronic form. Seller shall provide the records and additional information about Seller and its Processing of Buyer Data as reasonably requested by Buyer for the purpose of assisting Buyer and Buyer clients (where Seller acts as a Subprocessor and Buyer as a Processor) in complying with Buyer' and relevant client's (as applicable) obligations under applicable Data Protection laws or contracts, including the exercise of data subject rights, data protection impact assessments, prior consultation and Personal Data Breach notification obligations as well as investigations and as necessary for Buyer and relevant clients (as applicable) to demonstrate compliance with applicable Data Protection Laws.

3.7 Seller shall assist Buyer and Buyer clients (where Seller acts as a Subprocessor and Buyer as a Processor) to allow Buyer and Buyer client (as appropriate) to comply with their respective obligations under applicable Data Protection laws, including responding to Data Subjects' rights, data protection impact assessments, prior consultation, security and security breach notification as well as investigations. Seller shall also allow Buyer and Buyer clients, upon reasonable advance written notice, to check and audit its data processing facilities, procedures and records, either itself or through a third independent contractor at Buyer' or client's (as appropriate) expense, in order to ascertain compliance with Data Protection Laws and the terms of this DPSA, the Agreement and the agreement between Buyer and the client (where Seller acts a Subprocessor under the terms of this DPSA). Seller and its personnel shall fully cooperate with reasonable audit requests by providing access to relevant knowledgeable personnel, physical premises, documentation, infrastructure and application software. In addition, Seller will provide, at no cost to Buyer or client (as applicable), copies of any routine or other Service Organizational Control (SOC) reports, including SOC 1, Type 2, and SOC 2 reports or equivalent and other data security or data protection related audits, as applicable to the Services. After conducting an audit, Buyer will notify Seller of any non-compliance. Upon such notice, Seller shall promptly take the necessary measures to remedy such non-compliance. Buyer is allowed to share all audit results and documentation provided by Seller to Buyer to the Controller (Client) where Buyer is the Processor under the contract.

3.8 Seller shall provide Buyer with the name and contact details of its DPO if it has appointed one or otherwise another person who is responsible for data protection compliance within Seller's organization.

3.9 Buyer is responsible for responding to Data Subject Requests for access, correction, deletion or restriction of that person's Personal Data ("**Data Subject Request**"). If Seller receives a Data Subject Request, Seller shall promptly redirect the Data Subject Request to Buyer and enable Buyer to meet its obligations under applicable Data Protection Laws by providing reasonable cooperation and assistance in responding to the Data Subject.

3.10 The Buyer may from time to time require the Seller to comply with any additional terms required by any of its clients in respect of any Processing of Personal Data where the Seller acts as a Subprocessor and the Buyer as a Processor of that Personal Data.

4. Subprocessor

4.1 If Seller uses a Subprocessor to fulfill its obligations under this DPSA, it will:

a) Conduct reasonable due diligence to ensure that the Subprocessor can meet the obligations set out herein and in particular provides sufficient guarantees to implement technical and organizational measures in such a manner that the processing will meet the requirements of the applicable data protection laws;

b) Obtain prior written specific or general written authorization from Buyer; In the case of general written authorization, Seller shall inform Buyer of any intended changes concerning the addition or replacement of other processors, thereby giving Buyer the opportunity to object to such changes.

c) Execute a written contract detailing the terms of the sub-processing activities and provide a copy to Buyer;

d) Ensure that no personal data are transferred outside the EU/EEA, except with prior authorization from Buyer and under a Valid Transfer mechanism; and

e) Ensure any sub-processor adheres to the terms of this DPSA as if it were a party to it.

4.2 Seller shall be liable for the acts and omissions of any Subprocessor to the same extent as if the acts or omissions were performed by Seller.

5. Seller Personnel

5.1 Seller shall take reasonable steps to require screening of its personnel who may have access to Personal Data and shall require such personnel (i) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data and (ii) to agree to comply with confidentiality obligations which shall survive the termination of employment.

5.2 Seller will ensure that access to Personal Data is strictly limited to employees who have complied with clause 5.2 above and who need access to Personal data for the agreed Processing.

5.3 If disclosure of Buyer Data is required by applicable law or a compulsory legal process, Seller shall, unless prohibited by applicable law: (i) notify Buyer promptly in writing before complying with any such disclosure request in order to provide Buyer an opportunity to intervene, if appropriate; and (ii) disclose the minimum amount of Buyer Data necessary to comply with applicable law or a compulsory legal process.

6. Return or Destruction of Buyer Data

6.1 Upon termination or expiration of the Agreement for any reason, or if any part of the Buyer Data retained by Seller ceases to be required by Seller to perform its Processing obligations under the DPSA, Seller shall promptly return and delete all Buyer Data in accordance with the relevant provisions of the Agreement and certify in writing to Buyer that it has destroyed or returned all Buyer Data.

7. Security Measures.

7.1 Seller warrants and undertakes to have in place and shall implement and maintain appropriate organizational and technical processes and procedures designed to protect against any unauthorized or unlawful access, processing, loss, destruction, theft, damage, use or disclosure of Buyer Data or systems, including, at a minimum, the technical and organizational measures set forth in Annex II to this DPSA. Buyer reserves the right to restrict, monitor and/or terminate access to its systems and network at any time.

8. Personal Data Breach and Response

8.1 Seller shall promptly notify Buyer of a Personal Data Breach without undue delay and no later than 24 hours upon Seller becoming aware of the Personal Data Breach. Seller should notify Buyer by telephone to Seller's primary business contact and via email at **unisysglobalprivacy@unisys.com** if it has knowledge that there is, or reasonably believes that there has been, a Personal Data Breach. Notice must include the following:

a) the nature of the Personal Data Breach,

b) the categories and numbers of Data Subjects concerned, and the categories and numbers of records concerned;

c) the name and contact details of Seller's DPO or other relevant contact from whom more information may be obtained;

d) the likely consequences of the Personal Data Breach; and

e) the measures taken or proposed to be taken to address the Personal Data Breach.

8.2 Seller shall (i) cooperate with Buyer in the manner reasonably requested by Buyer and in accordance with law to investigate and resolve the Personal Data Breach, and mitigate any harmful effects (ii) promptly implement any necessary remedial measures to ensure the protection of Buyer Data or Buyer systems; and (iii) properly document responsive actions taken related to any Personal Data breach, including, without limitation, post-incident review of events and actions taken to make changes in business practices to ensure the ongoing protection of Buyer Data.

8.3 Except as required by applicable Data Protection Law, Seller agrees that: (i) it shall not inform any third party of any Personal Data Breach without first obtaining Buyer' prior written consent, other than to inform a complainant that Buyer shall be/has been informed of the Personal Data Breach; and (ii) Buyer shall have the sole right to determine whether notice of the Personal Data

Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others and the contents of any such notice.

8.4 If the Personal Data Breach was a result of Seller's or Authorized Persons' negligence or breach of the requirements of this DPSA, Seller shall bear all costs associated with (i) the investigation and resolution of the Security Breach; (ii) notifications to individuals, regulators, or others; and (iii) any other remedial actions required by law, recommended by a governmental body or agreed to by the Parties.

If the Personal Data Breach affected Personal Data of US Data Subjects in addition to the above and where available, Seller agrees to bear the costs associated with i) the provision of two years of credit monitoring by a reputable provider from the date of notification to the individual; and (ii) establishing a toll-free number and call center for affected individuals to receive information.

9. Cross-Border Transfer of Personal Data

9.1 Seller shall not Process Buyer Personal Data in a jurisdiction outside of the agreed Processing location as set out in Annex [I] without the written consent of Buyer. To the extent that Buyer provides written consent to the Processing of Personal Data in a third country or in case the Processing activities involve the transfer of Buyer Personal Data from the EEA or Switzerland to locations outside of the EEA (not being countries or territories formally recognized by the European Commission as providing an adequate level of data protection ("Adequate Countries")), Seller agrees to comply with a Valid Data Transfer mechanism and inform Buyer thereof prior to Processing outside the agreed location(s).

9.2 If Privacy Shield is utilized to validate the cross-border transfer of Personal Data, Seller agrees to comply with the terms of the Privacy Shield Framework in relation to data transfers covered by this DPSA, and shall duly assist, cooperate and provide Buyer with all necessary information and records to allow Buyer and its clients as the case may be to comply with their respective obligation under applicable law. Seller will remain certified for the term of the Agreement provided that the Privacy Shield is recognized as a Valid Transfer Mechanism.

9.3 The Seller further acknowledges and agrees that on the request of a competent supervisory authority, enforcement or other public or regulatory authority, client, court or tribunal, Buyer may make available to them a summary or representative copy of this DPSA and relevant provisions in this DPSA.

10. General provisions

10.1 **Affiliates**: Buyer is entering into this DPSA also on behalf of its Affiliates specified in Annex I. Buyer will coordinate all communication with Seller on behalf of its Affiliates with regard to this DPSE. Buyer represents that it is authorized to issue instructions as well as make and receive any communications or notifications in relation to this DPSA on behalf of its Affiliates. Buyer Affiliates may enforce the terms of the DPSA directly against Seller subject to the following provisions: (i) Buyer will bring any legal action, suit, claim or proceeding which that Affiliate would otherwise have if it were a party to the Agreement (each an Affiliate Claim) directly against Seller on behalf of such Affiliate, except where the Data Protection Laws or other applicable laws to which the relevant Affiliate is subject require that the Affiliate itself bring or be party to such Affiliate Claim and (ii) for the purpose of any Affiliate Claim brought directly against Seller by Buyer of behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate

may be deemed to be losses suffered by Buyer. If needed for local legal reasons Seller agrees to enter into a local DPSA with the relevant local Affiliate.

10.2 **Termination**: the term of this DPSA will end simultaneously and automatically at the later of (i) the termination of the Agreement or (ii) when all Processing activities under the DPSA have ended.

ANNEX I: Description of the Processing Activity

ANNEX I: Description of the Processing Activity

Subject-matter of the processing

Seller's provision of the Services to Buyer as set forth in the Agreement/Purchase Order.

Duration of the processing

The term of the Agreement plus the period from the expiration of the Agreement until deletion of all Personal Data by Seller in accordance with the Agreement.

Nature and purpose of the processing

The Personal Data transferred to Seller will be subject to the following basic processing activities, all of which are necessary to provide the Services and are further detailed in the Agreement/Purchase order:

Use of Personal Data to provide the Services, to provide assistance and/or technical support

Additional details may be provided here.

The type of personal data and categories of Data Subjects

Type of Personal Data: as set out in the Agreement/PO.

Categories of Data Subjects: as set out in the Agreement/PO

Additional details may be provided here.

Location of the processing

Country/location where Services are provided to relevant Buyer entity.

Additional details may be provided here.

Plan for return of destructing

Personal data will be returned to Buyer upon request and in accordance with the Agreement/PO details.

Data Breach Notification:

POINT OF CONTACT Seller	POINT OF CONTACT Buyer
Name – To be advised by the Seller	Name – To be advised by the Buyer
Phone – To be advised by the Seller	Phone – To be advised by the Buyer
Email - To be advised by the Seller	Email 1: - To be advised by the Buyer Email 2: unisysglobalprivacy@unisys.com
Other	Other

Sub-processor details:

Provided in Agreement/PO.

Additional details may be provided here.

ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES

Seller shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and to protect the Confidential and Personal Data of Buyer and its clients that Seller processes for Buyer ("Buyer Data") against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Buyer data transmitted, stored or otherwise processed.

Section 1 – Governance

1) Management: Seller maintains a privacy and security management program that includes:

   a. Executive review and support of all related policies and procedures.

   b. Annual third party risk assessments and formal risk remediation program.

   c. Managing privacy and security incidents, including effective determination of root cause and corrective action.

   d. Regular audits to measure the effectiveness of controls.

2) Policies: Seller employs a variety of policies, standards and processes designed to support its compliance with legal and regulatory requirements for the protection of Buyer Data.

3) Standards: If Seller stores Buyer Data, such storage is in data centers that are certified to ISO 27001. Seller conducts annual internal security assessments and facilitates external independent verification and validation audits to maintain this certification. SOC 1 or SOC 2 level audits are also performed each year. Seller agrees to make available copies of the most recent ISO certifications and SOC assessment reports upon request.

Section 2 – Personnel Security

1) Pre-employment Screening: Seller conducts pre-employment screening to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

2) Confidential Agreement: Seller requires all personnel to agree to a Confidentiality Agreement as a condition of employment and to follow policies on the protection of personal data, confidential information, and information security procedures.

3) Security and Privacy Training: Seller personnel receive training, at least annually, in ethics, privacy and information security awareness with training content updated at least annually. Seller will document training completion and make available upon request to Buyer, proof of completion for Seller personnel providing services to Buyer.

4) Disciplinary Process: Seller maintains a Code of Conduct and disciplinary process that is used when personnel violate Seller security or privacy policies.

Section 3 – Admittance Controls

In order to ensure consistent security of Buyer Data, Seller adheres to at least the following admittance controls to prevent unauthorized parties from accessing Seller locations containing Buyer Data:

1) All buildings are secured with controlled access at the entry point 24 x 7 x 365. All visitors must be signed in by an authorized person with appropriate admittance privileges and escorted at all times. The time of entry and exit are also logged.

2) Entry into sensitive areas, for example, areas where databases running critical applications that contain Buyer Data are located, require multi-factor authentication, for example, a key card and entry of a designated PIN number.

3) All physical entry controls and access rights are regularly reviewed and updated.

Section 4 – Access Controls

Seller adheres to the following access controls to data and its data processing systems to prevent unauthorized parties from accessing the systems:

1) Access to Buyer Data in data processing applications and to data processing systems requires a unique user account name, User ID and password implemented using multi-factor authentication.

2) Access is based upon documented, approved requests according to a documented user access provisioning process.

3) Access is provided on a least privileges basis and based upon user role and need for access in order to perform the services. The determination of whether a person requires access is made based on the role as defined in the solution architecture of the Services.

4) Seller segregates access control duties to ensure the risk of a deliberate fraud is mitigated as the collusion of two or more persons would be required in order to circumvent controls and the risk of legitimate errors is mitigated as the likelihood of detection is increased.

5) Seller triggers automatic revocation when a user leaves the company or changes roles.

6) An access review process is managed at least annually to review the currency of the access privileges provided. Any unwanted rights are promptly removed upon detection.

7) Seller adheres to the following minimum standard password requirements when using Seller systems to access applications that contain Buyer Data:

   a. Accounts are locked after maximum of 5 failed login attempts or within 10 minutes of inactivity.

   b. Passwords automatically expire at 90 days for general users and 45 days for administrators.

   c. Passwords must be at least one (1) day old before they can be changed.

   d. Passwords must be different from the previous five (5) passwords used.

   e. Upon initial logins, users are forced to change passwords.

   f. Complex password are mandated (min 8 characters and combination of Upper and lower case letter, numerals and special characters). Administrator accounts must follow minimum 12 character password.

8) Seller PC's and servers are automatically locked with a password protected screen saver after a defined period of inactivity.

9) Applications used to provide services to Buyer contain logs that document access to the application data.

10) Buyer Data is encrypted at rest on Seller's systems.

Section 5 – Data Transmission Controls

1) Seller requires that all Buyer Data transferred over public networks be encrypted.

2) Seller only transfers Buyer Data to authorized third parties approved by Buyer. The approval is documented in writing and maintained by the Seller.

Section 6 – Data Entry Controls

1) Seller systems that are used to access applications containing Buyer Data have the capability to generate activity and event logs in order to determine when access to an application is made and by whom.

2) Seller policies and standards define log retention schedules.

Section 7 – Order Controls

Seller employs the following measures to Buyer Data is processed according to Buyer' instructions:

1) Buyer' processing instructions are documented in the contractual agreement between the parties.

2) Seller uses controls and processes to ensure compliance with contractual terms including data processing instructions.

3) All Seller personnel and subcontractors are contractually bound to respect the confidentiality of all confidential information, including Buyer Data.

Section 8 – Availability Controls

Seller employs the following measures to ensure Buyer Data is protected against random destruction or loss:

1) For systems and applications in Seller control, Seller maintains disaster recovery and business continuity plans that are regularly revised and updated to meet our expanding activities and services. These plans are designed to reduce or eliminate the loss potential to Services.

2) Physical protection against damages from natural and manmade disaster is implemented at all locations storing Buyer Data.

3) The information processing systems and facilities are adequately protected from power failures and other disruptions by using permanence of power supplies such as multiple feeds, uninterruptible power supply (ups), backup generator and other supporting utilities.

4) Equipment is maintained in accordance with the Sellers recommended service intervals and

specifications are in place.

5) Seller mandates media handling and secure destruction standards for the safe and permanent destruction of Buyer Data that is no longer required.

6) Seller workstations and servers are protected with antivirus software. Systems are enabled with real time protection and periodical scans and are regularly updated with anti-virus signatures. All systems are centrally monitored and managed for virus activity. Reports are generated regularly identifying any assets which are infected, have outdated signatures or do not have antivirus installed/activated and remedial actions taken.

7) Network traffic, Passwords, API interactions and data flow between various tiers of the infrastructure are encrypted as per business needs and Buyer requirements.

8) Seller has implemented controls to detect, prevent and recover against malware infections.

9) Seller owned PC's have active up-to-date personal firewall rule set definitions. Seller centrally manages the personal firewall software installed on PC's for reporting and to distribute rule set definitions for intrusion detection and prevention.

Section 9 – Separate Processing

Seller employs the following measures to ensure separate processing of Buyer Data is maintained:

1) Buyer data sets that are required for Seller to provide services are supplied to Seller by Buyer. Before such data is supplied, the Buyer provides instructions for the processing of the data set and Seller follows the instructions to ensure the data is used for the purpose prescribed by Buyer or its clients.

2) When updating Seller systems and applications used to provide services to clients, Seller physically separates the test and development from the production systems and applications.

Section 10 - Security Incident and Privacy Incident Response Plans

1) Seller follows a Data Protection Incident Response Process that details the handling of intentional or inadvertent information security events affecting the integrity, confidentiality, authentication, non-repudiation, and availability of information, and the information technology infrastructure of Seller that contain Buyer Data.

2) Seller’s process requires them to notify Buyer immediately and no more than 24 hours after discovery of a suspected with reasonable certainty or actual breach of Buyer Data.

3) All Incidents are resolved in a time-bound manner and following their closure the lessons learned are documented and reviewed for ongoing quality and improvement purposes.

Section 11 – Other

1) In addition, Seller shall:

   a. direct and procure Seller personnel not to attempt to break security systems or to obtain access to any programs or data beyond the scope of the access rights granted and not to conduct any activity using issued login-ids, passwords, keys or other access credentials (“Access

Credentials") contrary to applicable laws and regulations, including without limitation those relating to export and import laws, and the terms of use embedded into the systems and network; and

b. if access has been granted to named individuals through the issuance of Access Credentials, restrict access to such individuals, direct them not to share or transfer Access Credentials with anyone, and immediately notify Buyer if an individual authorized to access the systems and network is no longer an employee or no longer requires access to the systems and networks.

2) Ensure that any device connecting to a Buyer internal network must have an appropriate firewall for business and anti-virus software solution installed and running. Without limiting any of its other rights, Buyer reserves the right to restrict, monitor and/or terminate access to its systems and network at any time.

3) Utilize industry recognized encryption, pseudonymization, or use other equivalent measures as reasonable and in accordance with industry best practice to protect the security of, all Personal Data that it receives from, or collects on behalf of, Buyer, during Processing in delivery of the Services.

4) Regularly perform internal and external evaluations and test and monitor the effectiveness of it technical and organizational measures and shall promptly adjust and/or update those measures as reasonably warranted by the results of such evaluation, testing, and monitoring.

5) At any point during the term of Agreement, upon request, provide Buyer with a copy of Seller's applicable security standards and policies. Seller shall, upon request, permit inspection by the auditors of Buyer or its client of Seller applicable security procedures and guidelines.