UNISYS

DATA SECURITY ADDENDUM ("DSA") to the Purchase Order agreed between the Buyer and the Seller (the "Agreement")

This DSA shall, effective as of the date executed below, 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 or Data Privacy Addendum ("DPA"), as appropriate.

Definitions

Security incidents - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

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

Third-party risk assessments - Risk assessments performed by Seller on its third-parties

Third-party - Service providers external to an organization

"Buyer Data" shall mean any Buyer 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 Services under the Agreement.

Buyer third-party auditors - Third-party auditors hired by Buyer to conduct an audit of Seller on the behalf of Buyer.

VPN (Virtual Private Network) - A data network that enables two or more parties (e.g. a teleworker and an organization) to communicate securely across a public network by creating an encrypted private connection between them.

Seller represents and warrants that it has implemented and will maintain 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. At a minimum, these shall include each of the following:

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. Seller's third-party risk assessments prior to engaging their services and at least annually thereafter, 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, and for the protection of Buyer Data.

3) Industry standards: Seller, at its own expense,
   - attains and maintains the latest version of ISO 27001 certification
   - at least annually, undertakes SSAE18 SOC 1 Type II and SOC 2 Type II audits.

ISO 27001 certification and SSAE18 audits cover Seller's people, processes, technology and facilities related to the provision of services. Seller agrees to make available copies of the most recent ISO certificate(s) and SSAE18 audit report(s) to Buyer 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) Confidentiality Agreement: Seller requires all personnel to agree to a Confidentiality Agreement as a condition of employment and to follow policies and procedures on the protection of personal data and confidential information.

3) Security and Privacy Training: Seller personnel receive training, upon hire and 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 or processing 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.

4) Documents that contain Buyer Data are kept in locked cabinets when not in use.

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 ID and password.

2) VPN is used for remote access to Buyer Data in on-premises data processing applications and to on-premises data processing systems. Multi-factor authentication is used for remote access to Buyer Data in cloud-based data processing applications and to cloud-based data processing systems.

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

4) 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.

5) 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.

6) Seller triggers automatic revocation of access rights within 24 hours when a user leaves the company or changes roles.

7) 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.

8) Seller adheres to the following minimum standard password requirements when using Seller systems and applications to access, store and process Buyer Data:

a. Accounts are locked after maximum of 5 failed login attempts

b. Inactive sessions are terminated automatically within 10 minutes of inactivity and require re-authentication.

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

d. Passwords must be different from the previous ten (10) passwords used.

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

f. Complex password is mandated (min 8 characters and three of four character types: one upper case, one lower case, one number, and one special non-alphanumeric character). Administrator accounts must follow minimum 12 character password.

9) Seller PCs and servers are automatically locked with a password protected screen saver after 10 mins of inactivity.

10) Applications and systems used to provide services to Buyer contain logs that document access to Buyer data.

11) Buyer Data is encrypted at rest on Seller's systems and applications. Encryption algorithms and minimum key lengths are consistent with the most recent NIST guidelines and/or Center for Internet Security (CIS) Benchmarks.

Section 5 – Data Transmission Controls

1) Network traffic, Passwords, API interactions and all data flow between various tiers of the infrastructure are encrypted. Encryption algorithms and minimum key lengths are consistent with the most recent NIST guidelines and/or Center for Internet Security (CIS) Benchmarks.

2) Seller requires that wireless network communications used for Buyer data are encrypted using the WPA2 (or above), with EAP-TLS.

3) 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 and applications containing Buyer Data have the capability to generate activity and event logs in order to determine when access to systems, applications and Buyer data is made and by whom.

2) Seller policies and standards define log retention schedules.

3) Logs contain sufficient information about the event. For example, the type of event, when the event occurred, where the

event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject/device associated with the event.

Section 7 – Order Controls

Seller employs the following measures to ensure that 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 people, processes, technology and facilities related to the provision of services, Seller maintains disaster recovery and business continuity plans that are regularly reviewed and updated to meet our expanding activities and services. These plans are designed to reduce or eliminate the loss potential to Services, and meet the recovery time objective, recovery point objective and minimum business continuity objective agreed between Buyer and Seller. Seller, at its own expense, test the data backups restoration, disaster recovery and business continuity plans, at least annually. Seller, upon request, will provide the test results to Buyer. Seller, at its own expense, shall promptly take the necessary measures to remedy any deficiency identified from the test and ensure remediation of deficiencies within the agreed timelines.

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 manufacturer’s recommended service intervals and specifications.

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 systems are protected with antivirus software, and encryption controls such as Bitlocker. Systems are enabled with real time protection and periodical scans, and are regularly updated with latest 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) Seller has implemented controls to detect, prevent and recover against malware and ransomware.

8) Seller owned PCs have active up-to-date personal firewall and intrusion prevention software. Seller centrally manages the personal firewall and intrusion prevention software installed on PCs for reporting and to distribute software updates, rule set definitions, and signature updates. Policy rules are reviewed and updated as new threats are identified.

9) Seller maintains, and routinely tests, a secure configuration of applications and systems at all times.

10) Seller has a firewall and intrusion detection system (IDS) or intrusion protection system (IPS) monitoring all data flows. Firewall and IDS / IPS are kept current with the latest software updates and signature updates. Policy rules are reviewed and updated as new threats are identified.

11) Seller has implemented web application firewalls, or an equivalent solution for protecting its externally facing web applications that are used to store and process Buyer data.

12) For in-house application and software development, Seller has established a secure development methodology and coding standards based on industry frameworks such as OWASP Top 10, SANS or NIST.

13) For in-house application and software development, Seller mandates a secure code review using manual and / or automated means before production use and when there is a major change. Vulnerabilities are remediated before use of the application and software in production environment.

14) Periodic vulnerability scans (at least quarterly) are performed by qualified personnel on Seller applications, systems and network used to access, process and store Buyer data. Vulnerabilities discovered are addressed in a timely manner. A copy of the report and re-test results confirming the closure of the vulnerabilities are provided to Buyer, upon request.

15) Periodic penetration tests (at least annually) are performed by qualified external firms on Seller applications, systems and network used to access, process and store Buyer data. Vulnerabilities discovered are addressed in a timely manner. A copy of the report and re-test results confirming the closure of the vulnerabilities are provided to Buyer, upon request.

16) Security patches are installed in a timely manner based on the criticality of patches.

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, Buyer provides instructions for the processing of the data set and Seller follows the instructions to ensure the data is used only for the purpose prescribed by Buyer or its clients.

2) Seller physically or logically separates the test and development environment from the production systems and applications used to provide services to Buyer.

3) Production data is not copied into a non-production environment unless production equivalent controls are provided.

4) Seller separates Buyer Data either physically or logically from Seller's internal data and other clients' data.

Section 10 - Security Incident and Privacy Incident Response Plans

1) Seller follows a Data Protection and Security 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, provided to Buyer, and reviewed for ongoing quality and improvement purposes.

4) Seller provides the security incident report to Buyer within 3 working days after closing the incident

Section 11 – Other

1) In addition, Seller shall:

   a. direct 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 owned by Seller or Seller personnel 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 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 its 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 and business continuity policies, standards, plans, processes and procedures.

6) Seller shall, upon request, permit Buyer, Buyer third-party auditors, and Buyer clients, to audit Seller’s security controls relevant to the provision of services. Seller, at its own expense, shall promptly take the necessary measures to remedy any deficiency identified from the audit and ensure remediation of deficiencies within the agreed timelines.

7) Seller shall, upon request, respond to assessment questionnaires within the specified timeline provided by Buyer. Seller, at its own expense, shall promptly take the necessary measures to remedy any deficiency identified from the assessment and ensure remediation of deficiencies within the agreed timelines.

8) If Seller uses a third-party and contractors for the provision of services, Seller ensures such third-parties and contractors are compliant with the measures specified in this Addendum.