

## PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

To the extent that the work under this Agreement requires the Seller to receive or have access to PII as defined below, this Clause applies.

### (a) DEFINITIONS

- i. **"Clause"** means this portion of the subcontract.
- ii. **"Data"** in this Clause means PII and De-Identified Data to which Company provides Seller access to provide the Services, and any information derived therefrom.
- iii. **"De-Identified Data"** means information from which any personally identifiable information about or relating to any Individual has been removed or coded and where there is a very low risk of identifying a particular Individual in the Data.
- iv. **"Individual"** in this Clause means any natural person represented in the Data.
- v. **"Law" or "Laws"** in this Clause means any law, statute, rule, regulation, order, judgment, notice, opinion, guidance or ordinance of any governmental authority, legislative, judicial, quasi-judicial, regulatory body, local government, or any agencies or departments, supervising authorities, and any industry self-regulatory bodies thereof, in each case, as these may be repealed, re-enacted, amended, overruled or replaced from time to time.
- vi. **"Personally Identifiable Information" or "PII"** means information about a specific individual that either directly identifies the individual or can otherwise be associated to the individual. PII includes, but is not limited to, an individual's first name or first initial and last name in combination with any one or more of the following Data elements including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts, etc.
- vii. **"Security Incident"** means any unauthorized access, use, disclosure, modification, or destruction of Data or interference with system operations in an information system containing Data. "Security Incident" includes the re-identification of an Individual in De-Identified Data.

### (b) PERMITTED USE AND DISCLOSURE

- i. The Seller may use or disclose PII solely for the purpose of providing Services in accordance with this Agreement. The Seller may not use PII for its own purposes.
- ii. The Seller agrees to allow access to PII only to those employees who need the PII to perform the Services under this Agreement. The Seller shall ensure that its employees will not discuss, divulge, or disclose any such PII to any person or entity except those persons within the Seller's organization directly concerned with the performance of the Services.
- iii. The Seller agrees not to disclose PII to third-parties unless specifically authorized by the company in writing.

### (c) SECURITY REQUIREMENTS

- i. Seller will implement and maintain appropriate safeguards to prevent any use or disclosure of Data for purposes other than those permitted by this Agreement, including administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of any electronic Data that Seller creates, receives, maintains, and transmits on behalf of Company. These safeguards must meet or exceed the security

## **PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)**

controls set forth in the current National Institute of Standards and Technology (NIST) Special Publication SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" or equivalent privacy and security controls. Upon request of Company, Seller will provide evidence to Company that these safeguards are in place and are properly managed. Any changes to the security safeguards shall be subject to Company approval. All electronic copies of PII must be protected with NIST FIPS 140-2 compliant encryption while in transit.

### **(d) SECURITY INCIDENTS**

- i. Seller will report all Security Incidents to Company within one (1) hour of learning of the event.
- ii. Seller will cooperate in any investigation related to a Security Incident and will take immediate steps to mitigate harm to Individuals and Company arising from such Security Incident and reasonable mitigation efforts as requested by Company.
- iii. Where a Security Incident was caused by Seller or Seller's personnel, agents or subcontractors, the Seller will reimburse Company for any reasonable expenses Company incurs in investigating the Security Incident (including but not limited to forensic analysis), in reporting any Security Incident as required by applicable Laws (including but not limited to governmental authorities and individuals whose Data is affected in the Security Incident), and in mitigating harm to those Individuals.

### **(e) COMPLIANCE WITH LAW AND THIS CLAUSE**

- i. The Seller shall administer a monitoring process to ensure compliance with the provisions of this clause, promptly report any breaches to the Company's technical representative, and implement immediate, appropriate corrective actions to contain and prevent recurrence.
- ii. The Seller agrees to protect and handle all PII in accordance with applicable Federal, State, and other regulatory requirements for the collection, use, and protection of personally identifiable information.

### **(f) TERMINATION**

- i. The Company may terminate this Agreement for default if Seller or an employee of the Seller fails to comply with the provisions of this clause. The Company may also exercise any other rights and remedies provided by law or this Agreement.
- ii. Upon termination or expiration of this Agreement, the Seller shall destroy Data and certify such destruction in writing to Company within 60 business days of termination or expiration of the Agreement.

### **(g) INSPECTIONS AND AUDITS**

- i. Company and its auditors (including external auditors) as designated from time to time, once annually (or at an additional time if good cause exists) shall have the right to: (i) conduct an audit during business hours and upon reasonable advance notice with respect to Seller use and disclosure of Data to confirm compliance with the terms of this

## PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Agreement; and (ii) examine controls and security practices and procedures with respect to Data as set forth in Section (c) (Security Requirements).

### (h) INDEMNIFICATION

- i. Seller will defend, hold harmless and indemnify Company and its employees, agents, officers, directors, corporate affiliates and contractors ("Company Indemnitees") from and against any claims, losses, damages, liabilities, costs, expenses, penalties or obligations (including attorneys' fees), which a Company Indemnitee may incur as a result of: (i) Seller's gross negligence or willful misconduct; (ii) a Security Incident caused by Seller or Seller's personnel, agents or subcontractors; or (iii) any unauthorized use or disclosure of Data by Seller or Seller's personnel, agents or subcontractors.

### (i) INSURANCE REQUIREMENT

- i. At all times during the Term of this Agreement and for one (1) year thereafter, Seller, at Seller's sole cost and expense, shall procure and maintain insurance in amounts and form customary in the industry for comparable businesses and sufficient for the business conducted under this Agreement, provided that they include Commercial General Liability in an amount not less than USD \$2,000,000 annual aggregate limit, Professional Liability/E&O in amounts not less than \$2,000,000 annual aggregate limit, and Cyber Liability in any amount not less than USD 2,000,000 annual aggregate limit. Insurance carriers must have an A.M. Best Rate or better of A-/VIII.

### (j) MISCELLANEOUS

- i. The Seller agrees to execute any additional agreements or modifications to this agreement necessary to protect the Data from disclosure or in order to comply with Company's contractual obligations, law, regulation, or its Prime Contract with the U.S. Department of Energy.
- ii. The Seller shall include this clause in all appropriate subcontracts. However, such provision in the subcontracts shall not relieve Seller of its obligation to assure compliance with the provisions of this clause.
- iii. Seller obtains no rights in the Data and expressly disclaims all right of ownership thereto. Seller agrees, and shall ensure, that the PII will at all times remain within the United States.