Contractor IT Security and Privacy Addendum

This Contractor IT Security and Privacy Addendum sets forth supplemental terms and conditions to the Agreement between you and Esri. For reference, Contractor as referenced herein may be known as Consultant, Supplier, or Vendor in the Agreement.

A. Security Overview. For any Task Order or Statement of Work in which Contractor is providing Service(s), Contractor will provide a secure environment for any and all hardware and software (including servers, network, and data components) to be provided or used by Contractor as part of its performance under this Agreement. Contractor represents that the security measure it takes in performance of its obligations under this Agreement are, and will at all times: (i) have implemented the "moderate" impact controls of National Institute of Standards and Technology (NIST) 800-53 security requirements; (ii) the security requirements, obligations, specifications, and event reporting procedures set forth in this Addendum of the Agreement; or (iii) any security requirements, obligations, specifications, and/or event reporting procedures set forth in the applicable Task Order or Statement of Work. Failure of Contractor to comply with the security requirements hereunder shall constitute a breach of the Agreement.

Contractor specifically represents and warrants that it has established and during the term of this Agreement will at all times enforce an Information Security Program including the requirements included in this addendum.

Esri reserves the right to modify the obligations set forth in this Addendum or add new obligations, and any such modified or new security requirement, specification, or event reporting procedures shall become effective thirty (30) calendar days after written notice thereof from Esri.

B. Definitions. The words, terms, or phases set forth in this Addendum will have the meanings provided below:

1. **"Security Controls"** means any specific hardware, software, or administrative mechanisms necessary to enforce NIST 800-53, in accordance with the terms of this Agreement as methods for addressing security risks to information technology systems and relevant physical locations or implementing related policies. Security Controls specify technologies, methodologies, implementation procedures, and other detailed factors or other processes to be used to implement Security Policy elements relevant to specific groups, individuals, or technologies.
2. **"Sensitive Information"** means the following information (whether written or oral, in hard copy or other form), whether or not prepared by Esri or any of its Representatives, that is sensitive and proprietary to Esri and, in the case of licensed material, to its licensor: (i) all information regarding Esri's past, present, or prospective customers or employees, the manner in which Esri conducts its business, the extent to which Service(s) are offered to or used by customers, the costs to provide such Service(s), the types and levels of staffing utilized by Esri, or Esri's operational or financial plans and/or expectations; (ii) all information regarding the technology, listings, or protocols embodied in computer systems and programs owned by or licensed to Esri; (iii) all trade secrets and intellectual property rights owned by or licensed to Esri; and (iv) any other information held by or concerning Esri that is not readily available to the public.
3. **"Security Policies"** means statements of direction for securing company information pertaining to security and mandating compliance with applicable laws and regulations.
4. **"Security Procedures"** means step-by-step actions taken to achieve and maintain compliance with NIST 800-53.

C. Information Security Program. Contractor specifically represents and warrants that it has established and during the term of this Agreement will at all times maintain an Information Security Program which includes:

1. Security Policies, Security Procedures, and Security Controls and provided to Esri via written documentation;

2. An accurately completed risk assessment questionnaire provided by Esri to Contractor upon execution of this Agreement and periodically throughout the term of the Agreement with a minimum of at least once annually thereafter;
3. A security incident management program;
4. A security awareness program;
5. A security change management program to promote stability and reliability of Contractor's security environment during the security change process; and
6. Business continuity and recovery plans, including regular testing.

D. Privacy. Contractor specifically represents and warrants that it has established and during the term of this Agreement will at all times maintain a privacy program that protects the privacy of personnel information as prescribed by the applicable privacy laws and regulations.

E. Security Architecture. Contractor specifically represents and warrants that it has established and during the term of this Agreement will at all times maintain:

1. A security architecture that reasonably ensures implemented and effective NIST 800-53 security controls;
2. A system of effective firewall(s) and intrusion detection technologies necessary to protect Esri data;
3. Appropriate network security design elements that provide for segregation of data;
4. Procedures to encrypt information in transmission and storage;
5. Procedures to ensure regular testing of Contractor's security systems and processes;
6. Database and application layer design processes that ensure website applications are designed to protect Esri data that is collected, processed, and transmitted through such systems.

F. System Management. Contractor specifically represents and warrants that it has established and during the term of this Agreement will at all times maintain:

1. Mechanisms to keep security patches current;
2. Monitoring systems and procedures to detect attempted and actual attacks on or intrusions into Esri data;
3. Procedures to monitor, analyze, and respond to security alerts;
4. Use and regular update of commercial state-of-the-art antivirus software; and
5. Procedures to regularly verify the integrity of installed software.

G. Access Control. Contractor specifically represents and warrants that it has established and during the term of this Agreement will at all times enforce:

1. Appropriate mechanisms for user authentication and authorization in accordance with a "need to know" policy;
2. Controls to enforce rigorous access restrictions for remote users, contractors and service providers;
3. Timely and accurate administration of user account and authentication management;
4. Mechanisms to encrypt or hash all passwords;
5. Procedures to immediately revoke accesses of inactive accounts or terminated/transferred users;
6. Procedures maintaining segregation of duties;
7. Procedures to ensure assignment of unique IDs to each person with computer access; and
8. Procedures to ensure Contractor-supplied defaults for passwords and security parameters are changed and appropriately managed.

H. Physical Access. Contractor specifically represents and warrants that it has established and during the term of this Agreement will at all times enforce:

1. Physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and protected in appropriate data centers;
2. Appropriate facility entry controls are in place to limit physical access to Esri Data and Esri's computer system and/or network that store or process data;

3. Procedures to ensure access to facilities is monitored and restricted on a "need to know" basis;
4. Measures to protect against destruction, loss, or damage of Esri data and Esri dependent computer system and/or network due to potential environmental hazards, such as fire and water damage or technological failures; and
5. Controls to physically secure all Esri sensitive information and to properly destroy such information when it is no longer needed.

I. Employee Background Check. Where permitted by law, Contractor agrees to perform and ensure successful completion/clearance of background checks: (i) upon hire for each Contractor employee, and (ii) for all new Contractor contract employees that are assigned to perform work at Esri's premises and/or who have access to Esri Information ("**Applicable Personnel**") as further described herein.

This background check will, to the extent permitted by applicable law, at minimum include an investigation for, and review of (i) any state/territory and federal/national convictions, (ii) any convictions involving identity theft, access device fraud, credit card fraud, or financial crimes and (iii) any deferred adjudications with respect to any of the above (collectively "**Convictions**"). In addition, Contractor agrees to verify that (i) all Applicable Personnel are eligible to work in the United States or the country in which they are contracted to work, and (ii) that no Applicable Personnel is included in the current Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons list ("**OFAC List**") or other similar blocked persons list of a country in which the contracted work will take place. If it is discovered by Contractor that Applicable Personnel has a Conviction, evidence of illegal drug use, or is ineligible to work as noted herein, then Contractor shall, immediately upon receipt of said information, remove such Applicable Personnel from assignment on Esri premises and shall prohibit such Applicable Personnel from entering Esri's premises or facilities, or accessing Esri Information. Contractor shall notify Esri in writing within two business days of gaining such knowledge. Contractor shall be responsible for obtaining any necessary consent for the background checks and tests from such individuals and to provide proof that Contractor has conducted same. Contractor agrees, to the extent permitted by law, to keep all such reports for a period of at least three years past the last date the individual was assigned to Esri. Upon request, Contractor shall submit a certification letter to Esri via a mutually agreeable format, certifying Contractor's compliance with the foregoing requirements

J. Accountability. Contractor specifically represents and warrants that audit/transaction logs are collected from systems and applications that store, process or transport Esri data.

K. Security Breach. Contractor will notify Esri within 72 hours of discovery of a security incident, breach, or unauthorized use or disclosure of Esri information. Contractor will coordinate with Esri to determine additional specific actions that will be required of Contractor for mitigation of the Breach, which may include notification to affected parties, and provide timely updates of all remediation activities. All associated costs shall be borne by Contractor.

Within seven (7) days of the closure of the incident, Contractor will provide Esri with a written report describing the incident, actions taken and plans for future actions to prevent a similar incident.

L. Audit. Contractor acknowledges and agrees that Esri may audit Contractor to confirm that Contractor has satisfied the obligations of this Addendum. Contractor shall act in a commercially reasonable manner to correct any deficiencies mutually identified and to bring itself promptly into compliance with its obligations under this Addendum.