SCHEDULE “X”

CYBERSECURITY TERMS AND CONDITIONS

1. SAUDI ARAMCO THIRD PARTY CYBERSECURITY STANDARD
   1. CONTRACTOR shall comply with the most current version of Saudi Aramco Cybersecurity Standards (SACS), Third Party Cybersecurity Standard (SACS-002), which is available at the E-Service Portals at Saudi Aramco website: <http://www.aramco.com>.
   2. Capitalized terms used in this Schedule “X” and not otherwise defined in this Contract shall have the respective meanings given in the SACS-002 Third Party Cybersecurity Standard.
2. CONTRACTOR CYBERSECURITY OBLIGATIONS
   1. In addition to the requirements of Paragraph 1.1, CONTRACTOR shall meet the requirements in this Paragraph in accordance with the specifications of the SACS-002 Third Party Cybersecurity Standard.
   2. CONTRACTOR shall:
      1. Access and use SAUDI ARAMCO Assets and Critical Facilities only as authorized by SAUDI ARAMCO and as required to conduct the WORK.
      2. Use SAUDI ARAMCO issued credentials (login ID, password) to access systems only as required to conduct the WORK. CONTRACTOR shall not use such credentials to access Assets or Critical Facilities other than those to which SAUDI ARAMCO has specifically authorized access.
      3. Take precautions to ensure that user IDs, passwords and authentication codes are stored securely.
      4. Be responsible for the security, integrity and appropriate authorized use of CONTRACTOR’s information systems, including those that interact at any time with a SAUDI ARAMCO system or are used to conduct business for SAUDI ARAMCO.
      5. Implement any additional cybersecurity controls and secure communication technologies recommended by SAUDI ARAMCO to ensure the security of its systems.
   3. If CONTRACTOR discovers a Cybersecurity Incident or encounters Suspicious Activities that relate to SAUDI ARAMCO Assets or CONTRACTOR systems that interact at any time with SAUDI ARAMCO Assets, CONTRACTOR shall notify SAUDI ARAMCO within one (1) or two (2) hours of discovering the Cybersecurity Incident and shall follow the Cybersecurity Incident Response Instructions set forth in Appendix A to the SACS-002 Third Party Cybersecurity Standard.
   4. After the resolution of any Cybersecurity Incident, CONTRACTOR shall submit to the Company Representative a detailed Cybersecurity Incident assessment detailing the impact and remediation efforts related to SAUDI ARAMCO Assets affected by the Cybersecurity Incident.
   5. CONTRACTOR shall conduct annual Compliance Assessment as per SACS-002 Third Party Cybersecurity Standard and shall submit the Compliance Assessment results and supporting documentation to SAUDI ARAMCO’s Information Security Department through [tpcompliance@aramco.com](mailto:TPCOMPLIANCE@ARAMCO.COM).
   6. SAUDI ARAMCO reserves the right to conduct a Cybersecurity Assessment not more than once per calendar year or more frequently upon the occurrence of any of the following:
      1. Suspicious Activities;
      2. A Cybersecurity Incident in respect of a CONTRACTOR Assets; and
      3. A Cybersecurity Incident in respect of a SAUDI ARAMCO Assets.
   7. SAUDI ARAMCO reserves the right, exercisable at its sole discretion, to revoke the access of CONTRACTOR or any of its individual personnel or agents to any SAUDI ARAMCO Assets and disable the connections of CONTRACTOR’s systems to SAUDI ARAMCO’s systems. Such action shall be in addition to and not in substitution of any right available to SAUDI ARAMCO under this Contract or at law and shall not relieve CONTRACTOR of any obligation to perform under this Contract

END OF SCHEDULE “X”