PRIVACY and DATA PROTECTION APPENDIX (PDPA)

This Privacy and Data Protection Appendix (PDPA) forms part of the Contract Document and is entered into by the Baker Hughes legal entity identified as a party to the Contract Document ("BAKER HUGHES") on behalf of itself and on behalf of, and for the benefit of, any BAKER HUGHES Affiliate that is permitted to use the goods, services and/or deliverables provided by Supplier pursuant to the Contract Document but is not a direct party to the Contract Document. Any such BAKER HUGHES Affiliate shall be entitled to all of the rights and interests of BAKER HUGHES under this PDPA and may enforce this PDPA in its own name; and Supplier acting on its behalf and as agent for each Supplier affiliate.

This PDPA sets forth obligations with respect to the processing and security of BAKER HUGHES Information and Baker Hughes Information Systems in connection with the provision of goods, services and/or deliverables to BAKER HUGHES under the Contract Document. In the event BAKER HUGHES provides access to any BAKER HUGHES Information as defined herein or access to a BAKER HUGHES Information System as defined herein, Supplier must demonstrate compliance with this PDPA. BAKER HUGHES or BAKER HUGHES's agent shall have the right to conduct a cybersecurity assessment ("Assessment") of the applicable technical and organizational measures described herein.

In the event of inconsistency or conflict between this PDPA and the Contract Document with respect to a subject covered by this PDPA, the provision requiring the higher level of protection for any Personal Data or other BAKER HUGHES Information governed by this PDPA shall prevail. The requirements in this PDPA are in addition to any confidentiality obligations between BAKER HUGHES and the Supplier under the Contract Document. BAKER HUGHES or the applicable BAKER HUGHES Affiliate responsible for the protection of any of the Personal Data or other BAKER HUGHES Information governed by this PDPA may enforce the terms of this PDPA. References in this PDPA to BAKER HUGHES shall be deemed to include references to BAKER HUGHES Affiliates. This PDPA is also applicable when a Supplier affiliate is providing goods, services and/or deliverables under the Contract Document directly, in its own name, in which event Supplier's agreement to the terms of this PDPA is also given on behalf of such Supplier affiliate; and Supplier warrants that it has the power and authority to do so. As used herein, "Supplier" shall mean Supplier and each such Supplier affiliate, collectively.

If the Supplier and BAKER HUGHES are parties to a frame agreement, such as a Master Services Agreement, Master Hosted Services Agreement or other frame agreement governing the purchase of goods, services and/or deliverables by BAKER HUGHES and/or BAKER HUGHES Affiliates, then this PDPA (i) shall be deemed an appendix to, and shall form a part of, such frame agreement, and (ii) shall apply to each purchase order, task order, order form, statement of work or other Contract Document entered into between BAKER HUGHES and Supplier, or their respective affiliates, pursuant to such frame agreement. For the purposes of a purchase order, task order, order form, statement of work or other Contract Document entered into by a BAKER HUGHES Affiliate or a Supplier affiliate pursuant to such frame agreement, the terms "BAKER HUGHES" and "Supplier" in this PDPA shall be deemed to mean the applicable BAKER HUGHES Affiliate and/or Supplier affiliate named as a party in such Contract Document.

Supplier and each Supplier affiliate shall comply with all applicable Data Protection Laws in the Processing of BAKER HUGHES Information.

SECTION I – DEFINITIONS

The following definitions and rules of interpretation apply in this PDPA.

Any words following the terms "including", "include", "e.g.,", "for example" or any similar expression are for illustration purposes only.

(i) **"Adequacy Decision"** means a decision issued under Article 45 of the GDPR.

(ii) ***BAKER HUGHES Affiliate(s)*** means any entity (including joint ventures, corporations, limited liability companies, partnerships, limited partnerships, business trusts or other entities, subsidiaries, businesses, operating divisions, units or Profit &Loss units of them) that directly, or indirectly through one or more intermediaries, controls, is controlled by or under common control with BAKER HUGHES, whether now existing, or subsequently created or acquired.

(iii) ***BAKER HUGHES Information*** *is* any BAKER HUGHES information defined as "confidential" in the Contract Document and Baker Hughes Confidential Information and BAKER HUGHES Highly Confidential Information as defined herein.

(iv) ***BAKER HUGHES Confidential Information*** is information created, collected, or modified by BAKER HUGHES that would pose a risk of causing harm to BAKER HUGHES if disclosed or used improperly, and is provided and identified as such to the Supplier under the Contract Document. BAKER HUGHES Confidential Information also includes Baker Hughes Personal Data, Controlled Data, and Sensitive Personal Data as defined herein and Processed in connection with performance of the Contract Document.

(v) ***BAKER HUGHES Highly Confidential Information*** is BAKER HUGHES Confidential Information that BAKER HUGHES identifies as "highly confidential" in the Contract Document, or that BAKER HUGHES identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

(vi) ***BAKER HUGHES Information System(s)*** means any systems and/or computers managed by BAKER HUGHES, which includes laptops and network devices.

(vii) ***Contract Document*** means the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of goods, services and/or deliverables by Supplier to BAKER HUGHES.

(viii) ***Controlled Data*** is technical or government information with distribution and/or handling requirements proscribed by law, including but not limited to controlled unclassified information and license required export-controlled data, which is provided by BAKER HUGHES to the Third Party in connection with performance of the Contract Document.

(ix) ***Data Protection Laws*** means the European Data Protection Laws, UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

(x) ***EU/EEA Restricted Transfer*** means a transfer of Personal Data by BAKER HUGHES to the Supplier (or any onward transfer), in each case, where such transfer would be prohibited by European Data Protection Laws in the absence of the protection for the transferred Personal Data provided by the EU Standard Contractual Clauses.

(xi) ***European Data Protection Laws*** means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR"); and laws implementing or supplementing the GDPR.

(xii) **"*EU Standard Contractual Clauses"*** means the standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.

(xiii) ***Mobile Devices*** means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

(xiv) ***Personal Data*** or ***Personal Information*** mean any information related to an identified or identifiable natural person (Data Subject), as defined under applicable law Processed in connection with the Contract Document. Legal entities are Data Subjects where required by law.

(xv) ***"Personal Data Breach"*** has the meaning described in Data Protection Laws.

(xvi) ***Process(es/ing) or Processed*** means to perform any operation or set of operations upon BAKER HUGHES Information, whether or not by automatic means, including, but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing or destroying.

(xvii) **Restricted Transfer(s)** means either *EU/EEA Restricted Transfer, UK Restricted Transfer and/or* Switzerland Restricted Transfer or any other data transfer restriction under Data Protection Laws.

(xviii) ***Security Incident*** means any actual or suspected event or breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to BAKER HUGHES Information or when Baker Hughes Information is used for a purpose not permitted under the Contract Document or this PDPA, or where a BAKER HUGHES Information System or BAKER HUGHES Information is accessed by any person other than Supplier Personnel pursuant to the Contract Document or this PDPA.

(xix) ***Sensitive Personal Data*** is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance and Portability Act of 1996; personal bank account and payment card information and other financial account information; national identifiers; and special categories of data under applicable law (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, home life and sexual orientation).

(xx) ***Supplier*** is the entity or affiliate entity providing goods, services and/or deliverables to BAKER HUGHES pursuant to the Contract Document. Supplier may also be referred to as Third Party.

(xxi) ***Supplier Information System(s)*** means any Supplier system(s) and/or computer(s) used to Process, store, transmit and/or access BAKER HUGHES Information pursuant to the Contract Document, which includes laptops and network devices.

(xxii) ***Supplier Personnel*** means all persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates and third parties (for example, suppliers, contractors, sub-contractors, and agents), as well as anyone directly or indirectly employed, engaged or retained by any of them.

(xxiii) "**Switzerland Restricted Transfer**" means an international transfer of Personal Data from Switzerland which: (i) is made between the Parties to, or within a Party to, this PDPA; and (ii) would at the time of the international transfer, be prohibited by applicable Data Protection Laws in Switzerland in the absence of the protection for the transferred Personal Data provided by the relevant EU Standard Contractual Clauses (as amended for pursuant to this PDPA).

(xxiv) **"Transfer"** means the transfer or disclosure or any other type of access to Personal Data to a person, organization or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.

(xxv) **"Transfer Mechanism(s)"** means the EU Binding Corporate Rules, the EU Standard Contractual Clauses, the UK IDTA, or any other transfer mechanism permitted or required to undertake a Transfer under Data Protection Laws.

(xxvi) ***Trusted Third Party Network Connection*** is a physically isolated segment of the Third-Party network connected to BAKER HUGHES internal network in a manner identical to a standard BAKER HUGHES office.

(xxvii) "***UK Data Protection Laws*** means all laws relating to data protection, the Processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

(xxviii) "**UK GDPR"** means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

(xxix) "**UK IDTA**" means the International Data Transfer UK Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018.

(xxx) **UK Restricted Transfer** means a transfer of Personal Data by BAKER HUGHES to the Supplier (or any onward transfer), in each case, where such transfer would be prohibited by UK Data Protection Laws in the absence of the protection for the transferred Personal Data provided by the UK IDTA.

"Lower case terms" used but not defined in this PDPA, such as "controller", "processor" and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies.

Section II applies to all Suppliers that Process any BAKER HUGHES Information or have access to BAKER HUGHES Information Systems.

SECTION II – COLLECTING, STORING, PROCESSING, OR SHARING BAKER HUGHES INFORMATION AND/OR HAVING ACCESS TO BAKER HUGHES INFORMATION SYSTEM(S)

Part A: TECHNICAL and ORGANIZATIONAL SECURITY MEASURES

Supplier shall comply with the following measures as applicable to the service, products and/or deliverables provided by the Supplier under the Contract Document:

Whenever a Supplier has access to BAKER HUGHES Information and/or BAKER HUGHES Information System(s), the Supplier is subject to the measures detailed in the Contract Document or other information security supplementary document which is incorporated by reference into the Contract Document, this PDPA, and BAKER HUGHES third-party security requirements and risk assessments completed by the Supplier (collectively, "Third Party Security Requirements") unless it is mutually agreed in the Contract Document that no such terms need to apply due to the specific nature of the relevant Processing or access to Baker Hughes Information or Information Systems.
Taking into account the state of the art and the nature, scope, context and purposes of Processing as well as applicable Data Protection Laws Supplier shall implement and maintain appropriate technical and organizational security measures and controls designed to protect BAKER HUGHES Information and/or BAKER HUGHES Information System(s) from Personal Data Breaches and/or Security Incidents, and to ensure ongoing confidentiality, integrity, availability of BAKER HUGHES Information and Information Systems. Specifically, supplier shall implement and maintain the following measures:

1. GENERAL ORGANIZATIONAL MEASURES

- **Governance Personnel and Accountability.** Supplier shall appoint a designated individual responsible for the development, implementation, maintenance, and oversight of the Supplier's security and data privacy programs to ensure accountability for compliance with industry and regulatory requirements.

- **Measures for internal IT and IT security and privacy governance and policy management.** At all locations where BAKER HUGHES Information is Processed, accessed, or stored (each a "Supplier Facility"), Supplier will maintain, monitor, and enforce a comprehensive written information security program which shall include industry standard written data protection policies and procedures sufficient to establish and facilitate Supplier's security program, copies of which may be requested by BAKER HUGHES. In addition, Supplier agrees as follows:
  - Supplier's security program shall control the implementation, modification, and testing of information security throughout Supplier's organization.

- Supplier shall appoint one or more employees in its organization with responsibility for oversight of and the management of security events and Security Incidents.
- Supplier shall meet with BAKER HUGHES upon BAKER HUGHES's request to review any changes in Supplier's security program or to review information about the information security environment.
- Supplier shall assign responsibility for controlling any third-party processing of BAKER HUGHES Information.
- Supplier shall follow security principles of "segregation of duties" and "least privilege" with respect to personnel and third-party access to BAKER HUGHES Information or BAKER HUGHES Information Systems and shall limit access to BAKER HUGHES Information and BAKER HUGHES Information Systems to personnel performing services under the Contract Document requiring access to the same , and solely to the extent necessary to perform the services to BAKER HUGHES under the Contract Document.

- **Measures for ensuring data minimization.** Supplier shall implement appropriate measures and controls to ensure BAKER HUGHES Information is Processed only for the purposes of providing the services under the Contract Document and will limit its Processing to the minimum data needed for the specific purpose specified in the Contract Document. To the extent applicable to the services provided under the Contract Document, Supplier shall ensure that BAKER HUGHES Information is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed. Supplier shall utilize data-masking or tokenization techniques ("Data Masking") to obfuscate Personal Data for all purposes where un-obfuscated Personal Data is not explicitly required. Consistent with these requirements, Supplier must utilize Data Masking or tokenization techniques in circumstances including, but not limited to, the following:

  - Data Masking in Non-Production Environments. Personal Data should not be used in Non-Production Environments, but in the event Personal Data is required for such use, Supplier will utilize Data Masking to obfuscate Personal Data when any BAKER HUGHES Information is stored in Non-Production Environments. Non-Production environments are defined as any environment that is not designated for live production use, including, but not limited to, development, test and quality assurance environments and data backups. To the extent Supplier seeks an exception from the requirements of this subsection, Supplier must obtain written consent from BAKER HUGHES. If BAKER HUGHES agrees in writing to provide an exception, then such exception shall apply only to the discrete instance for which it was granted.
  - Display Masking. Supplier will utilize Data Masking to obfuscate Personal Data in Production Environments including any paper output (e.g., reports, printouts, and copies) when displayed to anyone other than authorized personnel who require such access for the performance of the Services.

- **Measures for ensuring data quality.** To the extent applicable to the services provided under the Contract Document, Supplier shall maintain appropriate policies, procedures, and technical controls to ensure quality of BAKER HUGHES Information can be maintained as agreed in the Contract Document or otherwise instructed by BAKER HUGHES in relation to the services provided under the Contract Document.

- **Measures for ensuring limited data retention.** Supplier shall implement appropriate measures to ensure that it does not retain BAKER HUGHES Information for longer than Supplier is permitted to retain such information under the Contract Document or this PDPA. Supplier shall return or destroy all BAKER HUGHES Information in accordance with this PDPA and the Contract Document.

  Supplier shall implement policies, procedures, and technical controls regarding the disposal of BAKER HUGHES Information, and tangible property containing BAKER HUGHES Information, taking into account available technology so that BAKER HUGHES Information cannot be practicably read or reconstructed. Supplier's disposal policy shall require that such information is reviewed on a routine basis to ensure Supplier's compliance with its obligations under the Contract Document or this PDPA. As part of its information security and privacy program, Supplier shall, and shall ensure that its agents, contractors and permitted sub-contractors, take appropriate measures to properly dispose of or destroy BAKER HUGHES Information, whether such information is in paper, electronic or other form in accordance with the Contract Document or this PDPA.

  Additionally, Supplier shall implement and maintain policies and procedures that govern the receipt and removal of hardware and electronic media that contain BAKER HUGHES Information into and out of the Supplier's Facility, and the movement of these items within a Supplier Facility, including policies and procedures to address the final disposition of BAKER HUGHES Information and/or the hardware or electronic media on which it is stored, and procedures for

removal of BAKER HUGHES Information from electronic media before the media are made available for re-use. These measures shall, at a minimum, meet NIST standards and guidelines for media sanitization.

2. HUMAN RESOURCE SECURITY MANAGEMENT

- **Measures for Information Security and Data Privacy Training and Awareness.** Supplier shall implement and maintain policies and programs ensuring that its employees, agents, contractors, and permitted sub-contractors that have access to BAKER HUGHES Information or BAKER HUGHES Information Systems receive regular security, privacy and data classification awareness and training. Supplier training and awareness program shall contain training on how to implement and comply with its enterprise IT cybersecurity and privacy programs and how to protect BAKER HUGHES Information. Cybersecurity training, including new threats and vulnerabilities, shall be required for all Supplier developer and system administration staff supporting Supplier's systems Processing BAKER HUGHES Information and/or having access to BAKER HUGHES Information Systems. All development staff should be trained on secure coding principles and best practices.
- **Employee Screening.** Supplier shall implement appropriate measures to ensure that its employees that have access to BAKER HUGHES Information and/or BAKER HUGHES Information Systems are appropriately screened, or in the case of agents, contractors and permitted sub-contractors reasonable due diligence is performed by Supplier before they are provided access to BAKER HUGHES Information or BAKER HUGHES Information Systems.
- **Confidentiality Obligations.** Supplier shall implement appropriate measure to ensure that its employees, agents, contractors and permitted sub-contractors that have access to BAKER HUGHES Information and/or BAKER HUGHES Information Systems are bound by the terms of a written confidentiality or non-disclosure agreement that commits such parties to adhere to security requirements no less protective than those set forth in the Contract Document and this PDPA. Such confidentiality or non-disclosure agreement shall in no way limit Supplier's liability for the disclosure, use, or misuse of any BAKER HUGHES Information by any such employees, agents, contractors and permitted sub-contractors.

3. TECHNICAL MEASURES

- **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Supplier's Processing systems and services.** Supplier shall establish, maintain, monitor, and enforce (and update as necessary) comprehensive policies, procedures, and technical controls with respect to each Supplier Facility and any related system, device, network and application that contain BAKER HUGHES Information and/or connect to BAKER HUGHES Information Systems to ensure its confidentiality, integrity, and availability and to protect it from disclosure, improper alteration, and/or destruction, including but not limited to maintaining the following measures:
  - **Network and communications security** to ensure that communications and operations management include both physical and logical security controls.
  - **Identity and access controls** to ensure that only authorized users have approved access from approved devices at approved times. Apply the principle of least privilege (e.g., role-based access controls) as the basis of access authorization for Supplier systems used in Processing BAKER HUGHES Information. Measures shall include processes to grant and revoke access rights based on business need; strong authentication procedures for production environments that require a username, password, and multifactor authentication; processes to segregate access based on defined and documented duties to reduce opportunities for unauthorized or unintentional modification or misuse of systems or assets; and the use of firewall and intrusion detection systems to log access events for review by authorized Supplier personnel and to encrypt and decrypt personal data where appropriate. User access rights must be reviewed periodically to ensure that users have access to Supplier's systems and BAKER HUGHES Information and/or BAKER HUGHES Information Systems only to the extent necessary to perform job functions and that access rights are immediately removed on the termination of personnel or when access is not required for job functions.
  - **Malware protection** with up-to-date industry standard anti-virus and anti-malware controls.
  - **IT asset management system** to maintain a master inventory of all assets used in the delivery of the services under the Contract Document, with identified owners or responsible parties for each asset.
  - **Patch Management systems** to ensure that all servers, workstations, laptops, network devices, and appliances adhere to a hardening standard commensurate with industry expectations and must be updated per an approved patch management process; and ensure that all software, firmware, and hardware is patched in accordance with vendor recommendations.

- **Measures for ensuring the ability to restore the availability and access to Baker Hughes Information and BAKER HUGHES Information Systems in a timely manner in the event of a physical or technical incident.** Supplier shall establish and maintain appropriate policies, procedures, and technical controls for responding to an emergency,

Security Incident or other events (for example, fire, vandalism, system failure, and/or natural disaster) that can cause interruption of Supplier's or BAKER HUGHES's operations directly related to the Services and/or Supplier's performance of the services under the Contract Document, including but not limited to:

- Documented business continuity and disaster recovery plans that include procedures to restore data and the functionality of affected systems, including procedures to rebuild systems, update software, install patches, and change configurations, as needed. Supplier shall maintain appropriate backups of BAKER HUGHES Information as part of its business continuity and disaster recovery plans.
- Documented policies and procedures for the backup and recovery of data maintained in cloud-based environments, including periodic backups of production services, files, and databases, and the storage of backups in a separate data center.
- Periodic testing of Supplier's business continuity and disaster recovery plans.
- Documented procedures to analyse the root cause of Security Incidents and other security events and to implement changes to existing controls, where appropriate, to better respond to future threats.

- **Measures for regularly testing, assessing, evaluating the effectiveness of technical and organizational measures, certification and assurance in order to ensure the security.** At Supplier's sole cost and expense, Supplier shall perform regular testing and monitoring of the effectiveness of Supplier's security program, including through SOC 2 Type II audits of Supplier's solution performed by an independent external third-party auditor, and through periodic vulnerability scans and risk assessments designed to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of each Supplier Facility and any related system, device, network and application that contain BAKER HUGHES Information and/or connect to BAKER HUGHES Information Systems, and to ensure that these risks are addressed. BAKER HUGHES may, with Supplier's full cooperation, conduct written assessments of Supplier to determine the continued adequacy of their safeguards to control the internal and external risks to the security of BAKER HUGHES Information and BAKER HUGHES Information Systems.

- **Measures for the protection of data during transmission and storage.** Supplier shall establish and maintain policies, procedures, and technical controls to guard against unauthorized access to BAKER HUGHES Information in storage and during transmission, including but not limited to:
  - Restrict and maintain security control to prevent unauthorized access to BAKER HUGHES information or BAKER HUGHES Information Systems, except by personnel who have a business "need to access" to perform a particular function.
  - Ensure BAKER HUGHES Information is encrypted in transit and at rest in hosted environments. The terms "encrypt" or "encrypted" as used in this PDPA shall mean the transformation of data, in accordance with the applicable law and industry best practices, through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.
  - Use commercially reasonable, industry standard encryption key management system to securely manage the lifecycle of encryption keys, including storing and transmitting encryption keys separately from the data.
  - Use of full-device hard drive encryption to protection the confidentiality and integrity of information maintained on approved mobile devices.

- **Measures for ensuring events logging.** Supplier shall maintain policies, procedures, and technical controls that record and examine activity in Supplier's system, device, network, and application that contain BAKER HUGHES Information and/or connect to BAKER HUGHES Information Systems that contain or use electronic information, including maintaining appropriate logs and reports concerning these security requirements and compliance therewith.

4. PHYSICAL AND ENVIRONMENTAL SECURITY MANAGEMENT

- **Measures for ensuring physical security of locations at which BAKER HUGHES Information is Processed.** Supplier shall implement, at a minimum, policies, procedures, physical and technical controls, and industry standard security measures, as they may evolve and improve from time to time, sufficient to protect Supplier Facilities, including by defining security perimeters with appropriate security barriers and ingress and egress controls, to protect against unauthorized access, damage, and interference with respect to such Supplier Facilities. Supplier shall establish and maintain clear lines of responsibility and operating procedures for each such Supplier Facility, including the

segregation of duties, where appropriate, to lower the risk of negligent or intentional system and/or information misuse. Such procedures shall include at a minimum the following:

- A badge-based access control system to control physical access and movement into and throughout Supplier's facilities; and
- Processes and procedures to monitor Supplier Facility access and promptly remove facility access rights from terminated personnel.

Part B: Security and Privacy Incidents

1. Supplier shall notify BAKER HUGHES without undue delay after becoming aware of any Security Incident experienced by Supplier (which includes any Personal Data Breach). Supplier shall report Security Incidents to BAKER HUGHES's Cyber Incident Response Team via phone at toll-free: 1 (800) 819-9630 or international: +1 (713) 489-6711 or via the web portal at: https://www.bakerhughes.com/contact-us. Supplier shall cooperate with BAKER HUGHES in its investigation of an incident. Supplier shall provide BAKER HUGHES with sufficient information to allow BAKER HUGHES to meet any obligations to assess and report the incident under the Data Protection Laws which may be provided in stages as it becomes available to Supplier and shall include the following a detailed description of the Security Incident, the type of data that was the subject of the Security Incident, the identity of each affected person, details of any sub-processors involved, the categories and numbers of data subjects concerned, and the categories and numbers of BAKER HUGHES Personal Data records concerned, the name and contact details of Supplier's Chief Information Security and data protection officers or other relevant contact from whom more information may be obtained; the likely consequences of the Personal Data Breach; and the measures taken or proposed to be taken to address the Personal Data Breach and any other information BAKER HUGHES reasonably requests, as soon as such information can be collected or otherwise becomes available.
2. Unless prohibited by law, Supplier shall provide BAKER HUGHES reasonable notice of, and the opportunity to comment on and approve, the content of any notice related to a Security Incident prior to publication or communication to any third party, except BAKER HUGHES shall not have the right to reject content in a security notice that must be included to comply with applicable law.
3. Should BAKER HUGHES elect to send a security notice regarding a Security Incident, Supplier shall provide reasonable and timely information relating to the content and distribution of that security notice as permitted by applicable law or regulation pursuant to the security notice.
4. Other than approved security notices, or to law enforcement or as otherwise required by law, Supplier may not make any public statements concerning BAKER HUGHES's involvement with a Security Incident to any third-party without explicit prior written authorization of BAKER HUGHES's Legal Department.

Part C: BAKER HUGHES Audit Rights

BAKER HUGHES reserves the right to conduct an audit upon 30 days advance notice, of Supplier's compliance with the requirements in this PDPA, including but not limited to: (i) review of the Supplier's applicable policies, processes, and procedures, (ii) review of the results of Supplier's most recent vulnerability assessment and accompanying remediation plans, and (iii) on-site assessments during regular business hours of Supplier's physical security arrangements and Supplier Information Systems. BAKER HUGHES reserves the right to conduct an application vulnerability assessment if Supplier's vulnerability assessments do not meet or exceed BAKER HUGHES application security requirements. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes BAKER HUGHES Confidential Information.

Subject to the confidentiality provisions of the Contract Document, BAKER HUGHES or its representative may review, audit, monitor, intercept, access, and disclose any information provided by Supplier that is Processed or stored on BAKER HUGHES Information Systems or on BAKER HUGHES Mobile Devices accessing the BAKER HUGHES network.

Part D: Supplier Personnel

Supplier is responsible for compliance with this PDPA by all Supplier Personnel. Prior to providing access to any BAKER HUGHES Information to any Supplier Personnel, Supplier must obligate them to comply with applicable requirements of the Contract Document and this PDPA. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel. Supplier may not appoint any third party engaged in providing services and/or deliverables under the Contract Document without the prior written consent of BAKER HUGHES. Where such consent has been given, any change of such third party requires BAKER HUGHES's prior written approval.

The SECTION III only applies whenever a Supplier and/or its Supplier Personnel Process Personal Data either as Data Processor (Part A) and/or as Data Controller (Part B) in connection with the Contract Document.

SECTION III – PERSONAL DATA PROCESSING

Part A: PERSONAL DATA PROCESSORS

1. **Processing**. Supplier will, and will ensure that all of its Supplier Personnel will:
   (a) Only Process Personal Data on, and in compliance with, BAKER HUGHES's written instructions which may be set out in a Contract Document or otherwise issued from time to time, unless Processing is required by UK, EU or EU Member State law or any other applicable Data Protection Laws to which the Supplier is subject, in which case Supplier shall inform BAKER HUGHES of that legal requirement before such Processing, unless that law prohibits such information on important grounds of public interest. For clarity, Supplier will not collect, retain, use, or disclose Personal Data for any purpose other than as necessary for the specific purpose of Processing BAKER HUGHES Personal Data, including collecting, retaining, using, or disclosing Personal Data for a commercial purpose other than providing and enhancing products and services. Without limiting the foregoing, Supplier will not sell BAKER HUGHES Information or Personal Data. Where Supplier believes that any BAKER HUGHES instruction violates the terms of the Contract Document or applicable law, unless prohibited from doing so by applicable law, Supplier must inform BAKER HUGHES without undue delay before performing such instruction.

   (b) Process all Personal Data fairly and lawfully and in accordance with all laws applicable to Supplier's activities concerning Personal Data governed by this PDPA.

   (c) Where BAKER HUGHES has provided prior written approval for direct collection (including where expressly provided in the Contract Document), comply with applicable Data Protection Laws and regulations, including provisions concerning notice, consent, access and correction/deletion; any notices to be provided and any consent language to be used when collecting such information directly from a Data Subject are subject to BAKER HUGHES's prior and written approval.

   (d) When applicable, assist BAKER HUGHES with ensuring compliance with Articles 32 to 36 of the GDPR and/or UK GDPR or any other applicable Data Protection Law.

2. **Inquiries.** Unless prohibited by law, Supplier shall notify BAKER HUGHES promptly of any subpoena or other legal requirement prior to disclosure, so that BAKER HUGHES may seek a protective order or take other appropriate steps to protect its information. If disclosure must be made, limiting any disclosure only to the specific confidential information that is legally required to be disclosed and, unless prohibited by law, act only upon BAKER HUGHES's instruction concerning any request by a third party for disclosure of Personal Data or for information concerning Supplier's Processing of Personal Data.

3. **Confidentiality & Information Security**. Supplier shall comply with Section II above if Supplier Processes Personal Data in connection with the Contract Document. Supplier shall limit disclosure of or access to Personal Data to its Supplier Personnel who have legitimate business need-to-know relating to this Contract Document, and who have received proper training and instruction as to the requirements of the Contract Document (such as confidentiality requirements) and this PDPA and who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. **Return of Personal Data and Termination**. Supplier shall, within thirty (30) days of termination of the Contract Document, or if requested during the term of the Contract Document, cease all Processing of Personal Data and return to BAKER HUGHES all copies of Personal Data. In lieu of returning copies, BAKER HUGHES may, at its sole discretion, require Supplier to destroy all copies of Personal Data, using agreed upon methods to ensure such Personal Data is not recoverable, and certify to such destruction. Supplier may continue to retain Personal Data beyond the period prescribed in this section above where required by law, or in accordance with the Contract Document and/or applicable regulatory or industry standards, provided that (i) Supplier notifies BAKER HUGHES prior to the Contract Document's termination or expiration of the obligation, including the specific reasons for such retention; (ii) Supplier has a documented retention period and secure deletion procedure for such copies, with back-up copies retained only to the end of their legally required retention period; (iii) following such period, all copies and back-up copies are deleted in such a manner that they are not recoverable; (iv) Supplier performs no Processing of Personal Data other than that necessitated by retaining or deleting the relevant copies; and (v) Supplier continues to comply with all the requirements of this PDPA in relation to any such retained Personal Data until the same is securely deleted. Termination or expiration of the Contract Document for any reason shall not relieve the Supplier from obligations to continue to protect Personal Data in accordance with the terms of the Contract Document, this PDPA and applicable law.

5. **Supplier Personal Data.** BAKER HUGHES may require Supplier to provide certain Personal Data such as the name, address, telephone number, and e-mail address of Supplier's representatives to facilitate the performance of the Contract Document,

and BAKER HUGHES and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of the Contract Document, including but not limited to Supplier payment administration. BAKER HUGHES will be the Controller of this data for legal purposes and agrees to use reasonable technical and organizational measures to ensure that such information is Processed in conformity with applicable Data Protection Laws. Supplier may obtain a copy of the Supplier personal information by written request or submit updates and corrections by written notice to BAKER HUGHES. BAKER HUGHES will comply at all times with the privacy notice posted on its website.

6. **Compliance assistance**. Upon request, Supplier shall provide BAKER HUGHES with all information necessary to demonstrate Supplier's compliance with applicable law including Data Protection Laws and this PDPA, and assist BAKER HUGHES in ensuring compliance with the data protection obligations taking into account the nature of Processing and the information available to the Supplier; in particular security of Processing, preparation of data protection impact assessments (where required), any required breach notification to data protection authorities and data subjects, obtaining approval for Processing from data protection authorities where required, and allow for and contribute to audits, including inspections, conducted by BAKER HUGHES or another auditor mandated by BAKER HUGHES in accordance with the provisions as laid down in Section II Part C in this PDPA.

   Supplier shall immediately inform BAKER HUGHES if, in its opinion, an instruction infringes any applicable law including GDPR or other Data Protection Laws.

7. **Record of Processing Activities.** If applicable, Supplier shall maintain a record of its Processing activities conducted for and on behalf of BAKER HUGHES. Such a record shall contain: (i) the categories of Processing carried out on behalf of BAKER HUGHES; (ii) details of EU/EEA Restricted Transfers or UK Restricted Transfers of Personal Data including the identification of the country or international organisation that the Personal Data is transferred to and record of the safeguards the Supplier has put in place to ensure that the transfer will be in accordance with Data Protection Laws. The Supplier shall make this record available to BAKER HUGHES within 48 hours of receiving such a request.

8. **Data Subject requests.** Supplier shall promptly:
   (a) notify BAKER HUGHES if it receives a request from a data subject under Data Protection Laws in respect of Personal Data (including full details and copies of the complaint, communication or request), as well as data correction, deletion, blocking and/or Processing and provide full co-operation, assistance, and support to BAKER HUGHES, consistent with the functionality of services or applications provided under the Contract Document, to comply with any data subject requests to exercise their rights under applicable Data Protection Laws. The Supplier shall not respond to the request itself, unless authorised to do so by BAKER HUGHES;

   (b) assist BAKER HUGHES by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of BAKER HUGHES' obligation to respond to requests for exercising the data subject's rights.

9. **Sub-processing**

   (a) Subject to Section II, Part D, the Supplier has BAKER HUGHES' general authorisation for the engagement of sub-processors from the list set out in the Contract Document or other contract exhibits executed between the parties, provided that the Supplier shall:
      i where Supplier engages another processor for carrying out specific Processing activities on behalf of BAKER HUGHES include in substance the same data protection obligation terms (not less stringent) binding the Supplier under this PDPA in the contract between the Supplier and that other processor (sub-processor) when Processing Personal data by way of a contract or other legal act under any applicable law including Data Protection Laws, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements any applicable law including Data Protection Laws. Where that other processor (sub-processor) fails to fulfil its data protection obligations, the Supplier (initial processor) shall remain fully liable to BAKER HUGHES for the performance of that other processor's obligations.
      ii provide, at BAKER HUGHES' request, a copy of the agreement between the Supplier and its processor;
      iii remain fully liable to BAKER HUGHES for any act or omission of the processor;
      iv the Supplier shall notify BAKER HUGHES of any failure by the processor to fulfil its obligations under that contract.

   (b) The Supplier shall specifically inform BAKER HUGHES in writing of any intended changes to list in the Contract Document through the addition or replacement of sub-processors at least 30 days in advance, thereby giving BAKER HUGHES sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Supplier shall provide BAKER HUGHES with the information necessary to enable BAKER HUGHES to exercise its right

to object. In the event that BAKER HUGHES reasonably objects, then Supplier shall suspend the appointment of the processor.

(c) The list of sub-processors set out in the Contract Document or as provided to BAKER HUGHES during the onboarding or assessment process shall be deemed to be incorporated herein unless BAKER HUGHES and/or BAKER HUGHES Affiliate has objected to some or all of them. In case of objections, only those sub-processors shall be deemed to be incorporated herein on which Baker HUGHES and/or BAKER HUGHES Affiliate and Supplier have agreed any other legally binding agreement with Supplier.

Part B: PERSONAL DATA CONTROLLERS

Controller obligations. Supplier shall:

(a) only Process Personal Data in order to perform its obligations under the Contract Document;

(b) provide information to affected data subjects required under Data Protection Laws to ensure sufficient transparency of its Processing of the Personal Data;

(c) ensure that any person acting under its authority in relation to the Personal Data, including a processor, is appointed in accordance with Data Protection Law and shall only Process personal data on Supplier's instructions;

(d) notify BAKER HUGHES's Cyber Incident Response Team at the contact details provided in SECTION II Part B, 1) as soon as reasonably practicable upon becoming aware of a Personal Data Breach affecting Personal Data, not refer to BAKER HUGHES in any notification of such breach to a supervisory authority or third party unless required to do so by law, and, where reasonably practicable, provide a copy of any proposed notification and consider in good faith any comments made by BAKER HUGHES before notifying the Personal Data Breach to any third parties;

(e) in the event of a Personal Data Breach, take appropriate measures to address the Personal Data Breach, including measures to mitigate its possible adverse effect and document all relevant facts relating to the Personal Data Breach, including its effects and any remedial actions taken, and keep a record of it;

(f) where the Personal Data is no longer required for the performing its obligations under the Contract Document, securely delete the Personal Data, including deleting all existing copies, unless applicable Data Protection Laws require its retention;

(g) to the extent that Supplier engages third parties in an arrangement that involves an EU/EEA Restricted Transfer, Switzerland Restricted Transfer or a UK Restricted Transfer, Supplier shall ensure that an adequate safeguard is in place between the Supplier and the third party to protect the transferred Personal Data in compliance with Data Protection Laws. Supplier shall make available evidence of such safeguard to BAKER HUGHES on reasonable request.

SECTION IV – ADDITIONAL REGULATORY REQUIREMENTS

In the event Supplier Processes BAKER HUGHES Information, including Personal Data, that is subject to additional regulatory requirements, Supplier agrees to provide assistance to BAKER HUGHES for BAKER HUGHES's compliance with such requirements. Such assistance may include, without limitation, execution of additional agreements with BAKER HUGHES and/or BAKER HUGHES Affiliate as required by applicable law, compliance with additional security requirements, ensuring adequate safeguards and appropriate transfer mechanism are in place for cross-border data transfers, completion of regulatory filings applicable to Supplier, and participation in regulatory audits.

Part A: INTERNATIONAL DATA TRANSFERS

Without prejudice to any applicable Data Protection Laws, no Transfer of Personal Data may take place to countries that have not received an Adequacy Decision or without having in place an adequate Transfer Mechanism.

1. **European-specific Terms.** To the extent BAKER HUGHES Transfers Personal Data from the European Economic Area, UK, or Switzerland, Supplier commits to enter into the European Data Transfer Agreement (EDTA) including the EU Standard Contractual Clauses, the UK IDTA and Switzerland specifics when needed or ensures that equivalent safeguards are in place. To the extent applicable, the executed EDTA forms part of the terms and conditions of the Contract Document and this PDPA and is entered between Supplier and all its Affiliates and BAKER HUGHES on behalf of its Affiliates. Where the Transfer to Supplier is covered by Supplier's BCR and/or the Data Privacy Framework (DPF) Program (EU-US, UK Extension to the EU-US, Swiss-US: https://www.dataprivacyframework.gov/s/)Supplier warrants that it shall (i) maintain it in good standing for the duration of the services provided under the Contract Document, (ii) promptly notify BAKER HUGHES of any subsequent material changes in such authorization/certification, and (iii) enter

into an appropriate onward transfer agreement with any such sub-processor, or by entering into SCCs, in each case providing the same or more protection than the terms in this PDPA.

2. **Restricted Transfers from Other Jurisdictions.** Transfers from other jurisdictions that have Transfer restrictions are subject to the terms of the Contract Document and this PDPA. The parties agree to work together in good faith to complete additional Transfer restrictions documentation (such as any country-specific standard contractual clauses/cross-border data transfer agreements and assessments required by applicable Data Protection Law) as necessary to address compliance with Transfer restriction requirements.

3. **Data Transfer Impact Assessment Questionnaires** Supplier agrees to provide additional information as it may be required by applicable Data Protection Law and execute the data transfer impact assessment and/or Security Assessment Questionnaire during its on-boarding process. Supplier agrees and acknowledges that the data transfer impact assessment questionnaire completed during its on-boarding process is deemed incorporated in this PDPA, the EDTA, or other applicable country-specific cross-border data transfer agreements executed between the parties.

4. **Onward International Transfers & Hosting Locations**. Supplier must receive approval from BAKER HUGHES prior to (i) moving Personal Data from the hosting jurisdictions identified in the Contract Document and/or other contract exhibits executed between the parties to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than such hosting jurisdictions identified in the Contract Document; or (iii) transferring Personal Data outside of the European Economic Area, Switzerland, the UK, or other Restricted Transfers; where BAKER HUGHES approves, such approval may be subject to conditions including the execution of additional agreements to facilitate compliance with applicable law (including the Supplier entering into Module 3 of the EU Standard Contractual Clauses).

Part B: CALIFORNIA-SPECIFIC TERMS

With reference to the California Consumer Privacy Act, Cal. Civ. Code §1798.100 et seq., as may be amended from time to time (including but not limited to those amendments enacted by the California Privacy Rights Act of 2020) and including any implementing regulations ("CCPA/CPRA"), the parties acknowledge and agree that Supplier is a "Service Provider" and may receive Personal Data of California residents pursuant to the business purpose of providing the services to BAKER HUGHES in accordance with the Contract Document. Supplier shall not: (i) sell the Personal Data; (ii) retain, use, or disclose the Personal Data for any purpose other than for the specific purpose of performing the Service, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Service; and (iii) retain, use, or disclose the Personal Data outside of the direct business relationship between BAKER HUGHES and Supplier; (iv) combine Personal Data with other Personal Data received from any other source or collected from Service Provider's own interactions with California residents. Suppliers certifies that it understands the restrictions in this Section IV Part B and will comply with them in accordance with the requirements of the CCPA/CPRA. The parties agree to work together in good faith to complete additional California Privacy schedules as necessary to address compliance with California Privacy Law requirements.

SECTION V – ADDITIONAL PROVISIONS

1. **Insurance**. In addition to any insurance required by the Contract Document, Supplier agrees to have Cybersecurity Insurance (Cyber Liability) with a minimum limit of ten million dollars ($10,000,000) for each and every claim and in the aggregate, covering liabilities for financial loss resulting or arising from acts, errors, or omissions, in rendering the goods or services, and data theft, damage, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential corporate information, transmission of a computer virus or other type of malicious code, and participation in a denial of service attack on a third party. Such insurance must address all of the foregoing without limitation if caused by Supplier, its affiliates or Supplier Personnel, or an independent contractor working on behalf of the Supplier in providing the goods or services.

2. **Indemnity**. In addition to any indemnity provided in the Contract Document, with respect to any Security Incident, Supplier agrees to defend, indemnify, and hold harmless BAKER HUGHES, BAKER HUGHES Affiliates and their respective directors, officers, employees, agents, representatives and successors ("BAKER HUGHES Indemnitees") from and against all loss, damage, cost and expense arising out of or related to a Security Incident, including but not limited to, (a) attorneys' fees and costs of computer forensics work required for Security Incident investigations, (b) notifications to affected individuals and other entities, (c) credit monitoring or identity theft services provided to affected individuals, (d) establishing and operating a call center to respond to inquiries of affected individuals, (e) any other Security Incident remediation efforts that are reasonable under the circumstances; (f) damage to, impairment of, disablement of, or loss of

use of any computer system, hardware, software, data, tangible property, or any other property, and (g) any fines, fees or assessments imposed on any BAKER HUGHES Indemnitees by a third party or governmental authority.

3. **Limitation of Liability** In addition to any exceptions to any limitations of liability in the Contract Document, such exceptions shall be amended to add the following: NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE CONTRACT DOCUMENT, ANY LIMITATION ON SUPPLIER'S LIABILITY WILL NOT APPLY TO (A) SUPPLIER'S INDEMNIFICATION OBLIGATIONS UNDER THIS PDPA, (B) SUPPLIER'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, (C) CLAIMS AND INCURRED COSTS RELATING TO SUPPLIER'S BREACH OF ITS OBLIGATIONS OF CONFIDENTIALITY HEREUNDER, (D) DAMAGE TO, IMPAIRMENT OF, DISABLEMENT OF, OR LOSS OF USE OF ANY COMPUTER SYSTEM, HARDWARE, SOFTWARE, TANGIBLE PROPERTY, OR ANY OTHER BAKER HUGHES AND/OR BAKER HUGHES AFFILIATE PROPERTY CAUSED BY AN ACT OR OMISSION OF SUPPLIER, OR (E) ANY FINES, FEES OR ASSESSMENTS IMPOSED ON BAKER HUGHES AND/OR BAKER HUGHES AFFILIATE BY A THIRD PARTY OR GOVERNMENTAL AUTHORITY AS A RESULT OF SUPPLIER'S ACTIONS OR INACTIONS WITH RESPECT TO SUPPLIER'S OBLIGATIONS UNDER THIS PDPA.

4. PCI**.** In the event that the Supplier will Process credit card or debit card data, the following shall apply:

a. If the Services or goods involve (in whole or in part) the storage, Processing or transmission of credit card data or primary account numbers, Supplier shall comply with the requisite Payment Card Industry Data Security Standard, Payment Application Data Security Standard, and Payment Brand Rules (collectively, "PCI Standards"). Supplier shall notify BAKER HUGHES and/or BAKER HUGHES Affiliate within five (5) business days of any adverse change in Supplier's PCI Standards compliance status. To the extent that the Services require Supplier to access credit card data or primary account numbers and/or BAKER HUGHES's or its affiliates' credit card environment(s), Supplier shall treat such data, numbers and environment(s) in a manner consistent with the terms of the PCI Standards Supplier shall not cause BAKER HUGHES and/or its Affiliates to be in non-compliance with any of the aforementioned policies, procedures, or laws described above in this Section. Supplier acknowledges that Supplier is responsible for the security of cardholder data that Supplier possesses or otherwise stores, Processes, or transmits on behalf of BAKER HUGHES and/or BAKER HUGHES Affiliate, or to the extent that Supplier could impact of the security of BAKER HUGHES's and/or BAKER HUGHES Affiliate cardholder data environment.

b. Security Incident Affecting Cardholder Data. In addition to Section II Part B above, in the event that a Security Incident affects Personal Data subject to the PCI Standards, Supplier shall, within forty-eight (48) hours of the Security Incident, conduct an internal investigation to determine whether unauthorized Processing of cardholder data may have occurred and shall report the results of such investigation to BAKER HUGHES and/or BAKER HUGHES Affiliate If such investigation is inconclusive, or upon request by BAKER HUGHES and/or BAKER HUGHES Affiliate or a card organization, Supplier, at Supplier's sole expense, will engage a forensic investigator Supplier, selected or approved by BAKER HUGHES and/or BAKER HUGHES Affiliate and/or the card organizations, no later than 48 hours following Supplier's notice of the Security Incident to BAKER HUGHES and/or BAKER HUGHES Affiliate , to investigate the Security Incident. Such forensic investigator shall conduct promptly an examination of Supplier's systems, procedures and records and issue a written report of its findings. For the avoidance of doubt, Supplier shall provide such access, information, and assistance as is necessary for the forensic investigator, BAKER HUGHES and/or BAKER HUGHES Affiliate and/or card organizations to complete the investigation of the Security Incident. Supplier will not alter or destroy any records related to the Security Incident. Under all circumstances, Supplier shall maintain complete and accurate documentation regarding the Processing of cardholder data and the circumstances surrounding a Security Incident. Supplier will provide to BAKER HUGHES and/or BAKER HUGHES Affiliate information related to Supplier's or any card organization's investigation related to any unauthorized Processing of cardholder data including but not limited to forensic reports and systems audits.

5. **Restriction on using BAKER HUGHES Information**

Without limitation of the foregoing, Supplier shall not create any de-identified information from the BAKER HUGHES Information, shall not use or disclose any of the BAKER HUGHES Information for benchmarking or other comparisons, and shall not create any derivative works using any or all of the BAKER HUGHES Information unless expressly agreed herein or in the Contract Document.

APPENDIX 1 – DESCRIPTION OF PERSONAL DATA PROCESSING

Subject matter and duration of the Processing of the Personal Data: The subject matter and duration of the Processing of the Personal Data are set out in the Contract Document.

The nature and purpose of the Processing of the Personal Data: The nature and purpose of the Processing of Personal Data are set out in the Contract Document.

Categories of Data Subjects

The categories of data subjects are set out in the Contract Document and/or specified during the Supplier on-boarding process and may include Job applicants; BAKER HUGHES workforce (Employees and former employees, Employee Dependents); Individual Contractors and temporary workers; Customer Representative; Supplier Representative; Channel Partner Representative; Visitors (web visitor, onsite visitors, event attendees); Shareholders; Other Stakeholders (e.g., Community Members, Research Participants)

Types of Personal Data may include the following types of Personal Data as set out in the Contract Document

The categories of Personal Data are set out in the Contract Document or specified during the Supplier on-boarding process and may include

- Audio, Visual, and other Sensory Information (e.g., audio, video recordings)
- Authentication Information (e.g., work issued ID, user ID)
- Background and Criminal Information (e.g., criminal history, background check results)
- Biometric Information (e.g., fingerprints, keystroke patterns)
- Communication and Collaboration Information (e.g., call-logs, emails, instant messaging)
- Contact Information (e.g., name, home address, email address, phone number)
- Personal Identification Information (e.g., age, date of birth, gender)
- Digital Identification Information (e.g., cookie information, mobile traffic data)
- Education & Skills (e.g., academic record, resumes, qualifications)
- Employment Information (e.g., salary, benefits, job title)
- Family Information (e.g., children's name and photo)
- Financial Information (e.g., bank account information, credit card number)
- Government-issued Identifiers (e.g., driver's license number, passport number, social security number)
- Health and Health Insurance Information (e.g., health and safety related information, sick leave certificates, vaccination related data)
- Individual Preferences and Characteristics (e.g., abilities, habits, behavior)
- Location data (e.g., geo location, location tracking)
- Special Personal Information Attributes (e.g., ethnicity, religion, sexual orientation, political affiliation and activities, trade union membership)
- Travel and Expense (e.g., expense details, travel history, travel booking details)

The obligations and rights of BAKER HUGHES

The obligations and rights of BAKER HUGHES are set out in the Contract Document and this PDPA.