**Information Management/Information Technology (IM/IT) Agreement**

**for IT Access and Security**

**THIS AGREEMENT IS MADE ON \_\_\_ SEPTEMBER 2018 BETWEEN:**

BRUNEI SHELL PETROLEUM COMPANY SENDIRIAN BERHAD, whose registered office is at Jalan Utara, Panaga, Seria, KB2933, Brunei Darussalam (“COMPANY”), and

[\*\*CONTRACTOR],

whose registered office is at [\*\*, (\*\*) \*\*, \*\*] (“CONTRACTOR”),

**RECITALS**

1. COMPANY and CONTRACTOR have entered into one or more agreements whereby CONTRACTOR PERSONNEL may need access to COMPANY IT INFRASTRUCTURE; and
2. COMPANY and CONTRACTOR wish to establish the terms and conditions of access.

THE PARTIES AGREE AS FOLLOWS

# DEFINITIONS

Capitalised words and expressions have the following meanings when interpreting the AGREEMENT:

|  |  |
| --- | --- |
| **AFFILIATE** | in reference to a PERSON, any other PERSON that: (a) directly or indirectly controls or is controlled by the first PERSON; or (b) is directly or indirectly controlled by a PERSON that also directly or indirectly controls the first PERSON. A PERSON controls another PERSON if that first PERSON has the power to direct or cause the direction of the management of the other PERSON, whether directly or indirectly, through one or more intermediaries or otherwise, and whether by ownership of shares or other equity interests, the holding of voting rights or contractual rights, by being the general partner of a limited partnership, or otherwise.  |
| **AFFILIATE OF SHELL** | Any Affiliate of SHELL and shall for the purpose of this AGREEMENT include BSJV with the exception of Brunei LNG Sdn Bhd. |
| **AGREEMENT** | this IT Access and Security Agreement |
| **APPLICABLE LAWS** | where applicable to a PERSON, property, or circumstance, and as amended from time to time: (a) statutes (including regulations enacted under those statutes); (b) national, regional, provincial, state, municipal, or local laws; (c) judgments and orders of courts of competent jurisdiction; (d) rules, codes, directives, directions, regulations, and orders issued by government agencies, authorities, and other regulatory bodies; and (e) regulatory approvals, permits, licences, approvals, and authorisations.  |
| **AUTHORIZED USER** | the CONTRACTOR PERSONNEL who have access to the COMPANY IT FACILITIES or the COMPANY IT EQUIPMENT. |
| **BRUNEI SHELL JOINT VENTURES (“BSJV”)** | Brunei Shell Petroleum Company Sdn Bhd, Brunei Shell Marketing Sdn Bhd and Brunei LNG Sdn Bhd, which for the purpose of this AGREEMENT are considered AFFILIATES. |
| **COMPANY DATA** | (a) any information, including internal information, and data obtained, or accessible, via or in connection with the COMPANY IT EQUIPMENT or COMPANY IT FACILITIES and (b) the results, conclusions and findings of any evaluation by or on behalf of CONTRACTOR of any information mentioned under (a). |
| **COMPANY GROUP** | COMPANY and: (a) its co-venturers and joint ventures; and (b) any AFFILIATE of COMPANY, its joint ventures, or its co-venturers. |
| **COMPANY IT EQUIPMENT** | those items of IT equipment, IT machinery IT components, IT instruments and IT accessories, together with any documentation made accessible, or provided, by, or on behalf of, COMPANY, or AFFILIATES of COMPANY. |
| **COMPANY IT FACILITIES** | those applications, software, services, databases, network connections, communications together with any documentation and any other facilities made accessible, or provided, by, or on behalf of, COMPANY or AFFILIATES of COMPANY. |
| **COMPANY IT INFRASTRUCTURE** | the COMPANY IT EQUIPMENT, the COMPANY IT FACILITIES or the COMPANY DATA. |
| **CONFIDENTIAL INFORMATION** | all technical, commercial, or other information or materials, and all documents and other tangible items that record information, whether on paper, in machine readable format, by sound or video, or otherwise, relating to a PERSON’s business, including WORK PRODUCT and SCOPE provided to that PERSON, business plans, property, way of doing business, business results or prospects, the terms and negotiations of the AGREEMENT, proprietary software, IP RIGHTS, and business records. |
| **CONTRACT** | the contract under which the CONTRACTOR is undertaking activities for COMPANY, necessitating access to COMPANY IT INFRASTRUCTURE. |
| **CONTRACTOR GROUP** | CONTRACTOR and: (a) its subcontractors, (b) any AFFILIATE of CONTRACTOR or its subcontractors; and (c) any director, officer, employee, other PERSON or AGENCY PERSONNEL employed by or acting for and on behalf of CONTRACTOR, its subcontractors, or the AFFILIATES of CONTRACTOR and its subcontractors. |
| **CONTRACTOR IT EQUIPMENT** | IT equipment owned by CONTRACTOR, IT equipment within CONTRACTOR’s control and other IT equipment used by, or on behalf of, CONTRACTOR in connection with the CONTRACT or this AGREEMENT. |
| **CONTRACTOR PERSONNEL** | any individual provided by CONTRACTOR GROUP, whether directly or indirectly, and assigned to work in connection with the performance of SCOPE, whether or not an employee of CONTRACTOR GROUP. |
| **CSI** | any competitively sensitive information (including but not limited to commercial, technical, production or strategic information) that provides insight into a company’s current or future market conduct or strategy or that could influence the market conduct of a (potential) competitor. |
| **IP RIGHTS** | all patents, copyright, database rights, design rights, rights in CONFIDENTIAL INFORMATION, including know-how and trade secrets, inventions, moral rights, trademarks and service marks (all whether registered or not and including all applications for any of them and all equivalent rights in all parts of the world), whenever and however arising for their full term, and including any divisions, re-issues, re-examinations, continuations, continuations-in-part, and renewals. |
| **MATERIAL** | any software, model, standard, manual, practice, associated documentation, or operating procedures provided under, or in connection with, the CONTRACT or this AGREEMENT. |
| **MEANS OF IDENTIFICATION AND AUTHENTICATION** | the means provided by, or on behalf of, COMPANY to CONTRACTOR or AUTHORIZED USERS used to identify and authenticate such AUTHORIZED USERS, such as, but not limited to, a user-id and password or a smart card and pin. |
| **NEAR MISS** | an identified occurrence of a system, service or network state indicating a possible breach of information risk management policy or failure of safeguards, or a previously unknown situation that may be relevant to confidentiality, integrity, availability or regulatory compliance. |
| **PERSON** | (a) a natural person; or (b) a legal person, including any individual, partnership, limited partnership, firm, trust, body corporate, government, governmental body, agency, or instrumentality, or unincorporated venture. |
| **PERSONAL DATA** | any information relating to an identified or identifiable individual, unless otherwise defined under APPLICABLE LAWS related to the protection of individuals, the processing of such information, and security requirements for and the free movement of such information. |
| **SECURITY INCIDENT** | a successful or unsuccessful attempt to access, use, steal, disclose, conceal, modify or destroy information and interference with or misuse of information process infrastructure, applications and data. |
| **SECURITY STANDARD** | information security specifications, standards and practices that are internationally recognized as being sufficient to safeguard IT equipment and information, such as the ISO 27001/2 or COBIT standard, as amended from time to time, which will – at a minimum – include: (i) adequate measures to secure IT equipment;(ii) using adequate access controls;(iii) systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;(iv) design and implement a coherent and comprehensive suite of information security controls or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and(v) adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.The full and complete implementation of COMPANY’s standards on information risk management is deemed to be compliant with the SECURITY STANDARD. |
| **WORKSITE** | places where activities in connection with CONTRACT are to be performed, including manufacturing, fabrication, or storage facilities, installations, vessels, offices, or workshops. |

#

# IT SERVICES & IRM REQUIREMENTS

## IT Controls & Requirements

In all instances in which CONTRACTOR or CONTRACTOR PERSONNEL has access to, or uses, COMPANY IT EQUIPMENT or COMPANY IT FACILITIES, CONTRACTOR and COMPANY will abide by the terms of this AGREEMENT.

## Personal Data

### If CONTRACTOR processes PERSONAL DATA on behalf of COMPANY, CONTRACTOR agrees to comply, and ensure that other members of CONTRACTOR GROUP comply, with the relevant APPLICABLE LAWS. Any member of CONTRACTOR GROUP processing PERSONAL DATA must enter into a standard form data processing agreement as advised by COMPANY.

### CONTRACTOR will not provide COMPANY with any PERSONAL DATA of any individual except where such provision is necessary and CONTRACTOR has obtained any consent or permission as may be required by APPLICABLE LAW. CONTRACTOR will take all necessary steps to ensure that COMPANY may share PERSONAL DATA with its AFFILIATES and contractors in countries with differing legal requirements for data protection. Otherwise, CONTRACTOR will render the data anonymous so that it cannot be identified as being that of a particular individual.

# IT SECURITY STANDARD

## CONTRACTOR will, as a minimum, comply with, and fully implement, the SECURITY STANDARD.

## CONTRACTOR will promptly notify COMPANY in writing of any material changes to (i) the way CONTRACTOR has implemented the SECURITY STANDARD, (ii) its information security strategy, (iii) its IT policies, (iv) its operational IT standards or (v) its IT procedures as soon as reasonably practicable.

## CONTRACTOR will maintain clear guidelines and policies for action associated with any (alleged) breach of the SECURITY STANDARD or other IT security policies and will operate an effective IT security education program for their staff on a continuous basis, which should be based on internationally accepted standards.

## CONTRACTOR will ensure that (i) all CONTRACTOR IT EQUIPMENT that is disposed of, will be securely overwritten prior to such disposal and (ii) all data and licensed software has been completely removed.

## CONTRACTOR will continually monitor compliance with the SECURITY STANDARD, in accordance with internationally accepted standards.

# CONTRACTOR'S OBLIGATIONs

## CONTRACTOR will, and will ensure the CONTRACTOR PERSONNEL will, access the COMPANY IT INFRASTRUCTURE solely with CONTRACTOR IT EQUIPMENT or COMPANY IT EQUIPMENT.

## CONTRACTOR will not attempt to

### access any other systems or facilities;

### modify or add to the COMPANY IT FACILITIES or COMPANY IT EQUIPMENT;

### in any way to disable or reconfigure any log files or facilities on COMPANY IT EQUIPMENT or COMPANY IT FACILITIES; or

### install or cause to be installed into or on COMPANY IT EQUIPMENT or COMPANY IT FACILITIES any hardware, software, electronic, or other security mechanism or other disablement, deactivation, de-installation, damage or deletion mechanism which will hinder use of any of the COMPANY IT INFRASTRUCTURE.

## CONTRACTOR will not use the access to the COMPANY IT INFRASTRUCTURE for any other purpose other than performance of the CONTRACT and in accordance with the terms of this AGREEMENT.

## CONTRACTOR IT EQUIPMENT used to connect to COMPANY IT EQUIPMENT or COMPANY IT FACILITIES, or process and store COMPANY DATA must be managed in compliance with the SECURITY STANDARD. CONTRACTOR will take the integrity and security of COMPANY IT INFRASTRUCTURE into account when considering, and making, changes to CONTRACTOR IT EQUIPMENT.

## COMPANY can impose additional security standards and controls on CONTRACTOR IT EQUIPMENT used to (i) connect to COMPANY IT EQUIPMENT or COMPANY IT FACILITIES, or (ii) process and store COMPANY DATA by so notifying the CONTRACTOR. CONTRACTOR will implement such additional security standards and controls within 14 days of notification.

## CONTRACTOR will, and will ensure that CONTRACTOR PERSONNEL will, take reasonable security measures to prevent (i) unauthorized physical access to CONTRACTOR IT EQUIPMENT or COMPANY IT EQUIPMENT under its control and (ii) unauthorized access to COMPANY DATA under its control.

## CONTRACTOR will (i) clearly identify all CONTRACTOR IT EQUIPMENT and (ii) establish and maintain an inventory of CONTRACTOR IT EQUIPMENT.

# ACCESS FOR AUTHORIZED USERS

## CONTRACTOR will not allow access to COMPANY IT INFRASTRUCTURE to others than the AUTHORIZED USERS and concurs that AUTHORIZED USERS email addresses may be added to the COMPANY global address list.

## CONTRACTOR may nominate only CONTRACTOR PERSONNEL as AUTHORIZED USERS. CONTRACTOR may nominate additional AUTHORIZED USERS by submitting their name and location of use to COMPANY. COMPANY may accept or reject a nomination for an additional AUTHORIZED USER at its sole discretion.

## CONTRACTOR will make sure that there is a user registration and de-registration procedure in place, covering at least (i) granting and revoking access to CONTRACTOR IT EQUIPMENT and COMPANY IT INFRASTRUCTURE, (ii) an annual review process of AUTHORIZED USER's access rights, and (iii) a process on terminating all access rights of employees, contractors, and THIRD PARTIES immediately upon termination of their relationship with CONTRACTOR.

## Upon completion of any required training and instructions the AUTHORIZED USERS will be issued a MEANS OF IDENTIFICATION AND AUTHENTICATION. CONTRACTOR will maintain an up-to-date list of the AUTHORIZED USERS who have been given a MEANS OF IDENTIFICATION AND AUTHENTICATION and will notify COMPANY as soon as possible of any AUTHORIZED USERS who's access can be terminated.

## AUTHORIZED USERS will be given access to those parts of the COMPANY IT EQUIPMENT and COMPANY IT FACILITIES as is reasonably required for the execution of the AGREEMENT.

## Prior to the issue of a MEANS OF IDENTIFICATION AND AUTHENTICATION, CONTRACTOR will provide the AUTHORIZED USERS with all instructions as requested by COMPANY.

## In the event that the MEANS OF IDENTIFICATION AND AUTHENTICATION is issued in the form of a smart card or a user-id and password, CONTRACTOR will instruct AUTHORIZED USERS to:

### not disclose or give their smart card, user-id or password to any other person (including any other AUTHORIZED USER) nor write down their user-id or password;

### not store their user-id or password in any data file, unless such file is encrypted;

### refrain from any action that could allow any person to gain access to their smart card, user-id or password;

### make every reasonable effort to prevent any situation that would allow any person to obtain access to their smart card, user-id or password; and

### adhere to any other instructions that may be provided by COMPANY.

## The CONTRACTOR's and AUTHORIZED USER's access to and use of the COMPANY IT infrastructure and Materials is at the CONTRACTOR's own risk. The CONTRACTOR fully indemnifies and holds COMPANY, and any AFFILIATE of COMPANY, harmless against all claims by any AUTHORIZED USERS, relating to the COMPANY IT INFRASTRUCTURE.

## All COMPANY DATA will be treated as COMPANY’s CONFIDENTIAL INFORMATION, not subject to exceptions otherwise provided in the CONTRACT. CONTRACTOR will comply with all requirements in the CONTRACT prior to any disclosure required by APPLICABLE LAW or otherwise.

# TERMS OF USE

CONTRACTOR PERSONNEL may be required to accept certain terms of use before they can access certain COMPANY IT INFRASTRUCTURE. CONTRACTOR will instruct CONTRACTOR PERSONNEL to adhere to the terms of this AGREEMENT and any such terms of use. in the event of conflict between any such terms of use and this AGREEMENT, the terms of this AGREEMENT will prevail.

# MAINTENANCE AND SUPPORT

## COMPANY IT EQUIPMENT and COMPANY IT FACILITIES are maintained by, and may be located at COMPANY GROUP facilities, or those of a third party contracted to provide services to COMPANY GROUP. COMPANY may provide mandatory updates or patches, but otherwise provides no maintenance or support, unless expressly, and in writing, agreed otherwise.

## COMPANY extends no warranty concerning the results or effects of the use of the COMPANY IT INFRASTRUCTURE and does not warrant that the access to the COMPANY IT INFRASTRUCTURE will be uninterrupted, secure or error free.

# MONITORING, LOGGING, SHARING OF THREAT INFORMATION

## COMPANY reserves the right to log and monitor the use of any COMPANY IT INFRASTRUCTURE for security reasons at any time without notice. Such monitoring may include inspection of the COMPANY IT INFRASTRUCTURE.

## CONTRACTOR will share with COMPANY, as soon as reasonably practicable, any threat, vulnerability, and incident information that could potentially be of interest to COMPANY.

# SECURITY INCIDENT MANAGEMENT PROCEDURES

## CONTRACTOR will, and will procure that CONTRACTOR PERSONNEL will, report to COMPANY in a readily-accessible format and without delay all (i) SECURITY INCIDENTS, (ii) suspected SECURITY INCIDENTS, (iii) NEAR MISSES, (iv) suspected NEAR MISSES, (v) anomalies, (vi) contact by law enforcement, (vii) contact by regulatory or security authorities, and (viii) civil injunctions or search orders, all in as far as they impact, or might impact, COMPANY IT INFRASTRUCTURE.

## CONTRACTOR will, and will procure that CONTRACTOR PERSONNEL will, cooperate with investigations deemed necessary by COMPANY in the event of a known or suspected SECURITY INCIDENT. In the event of a known or suspected SECURITY INCIDENT, CONTRACTOR will reasonably collaborate with COMPANY in the root cause analysis and the forensic investigation.

## CONTRACTOR will, and will procure that CONTRACTOR PERSONNEL will, ensure that in the event of a SECURITY INCIDENT the overall business impact for COMPANY will be minimized and all COMPANY DATA will be isolated and protected in such a way as to minimise loss or damage to COMPANY IT INFRASTRUCTURE.

# SOFTWARE

## COMPANY may, from time to time, make available MATERIALS for use on COMPANY IT EQUIPMENT or CONTRACTOR IT EQUIPMENT used by AUTHORIZED USERS.

## CONTRACTOR will, and will procure that the AUTHORIZED USERS will, use such MATERIALS for the performance of the CONTRACT and in accordance with the terms of this AGREEMENT only and will not distribute, copy, reproduce, translate, adapt, modify or reverse engineer it. CONTRACTOR is aware that such MATERIALS may contain security features, such as features that prevent access to it or COMPANY IT INFRASTRUCTURE, or features that automatically or through other means remove it and its contents. COMPANY will not be liable for any losses, claims, damages, fees, fines, penalties or expenses resulting from, or connected to, the security features of such MATERIALS.

# AUDIT RIGHTS

## COMPANY may request CONTRACTOR to provide a yearly assurance letter specifying CONTRACTOR's compliance with the controls contained in this AGREEMENT, in a format advised by COMPANY.

## CONTRACTOR will permit COMPANY, or its authorized representatives, at all reasonable times, to audit the CONTRACTOR's and CONTRACTOR PERSONNEL's

### compliance with this AGREEMENT, including (i) compliance with the SECURITY STANDARD, and (ii) compliance with IT controls contained, or referred to, in the CONTRACT or work orders or similar documents issued thereunder; and

### use of the COMPANY IT INFRASTRUCTURE.

## CONTRACTOR will provide COMPANY, or its authorized representative, all cooperation and access, including access to CONTRACTOR PERSONNEL, together with all information, records, correspondence or other papers and data carriers in possession of CONTRACTOR or CONTRACTOR PERSONNEL that are necessary for COMPANY, or its authorized representatives, to carry out such audit.

## At least 8 weeks prior to commencing an audit, COMPANY will inform CONTRACTOR of the scope of such audit.

## COMPANY or its duly authorized representatives has the right to reproduce and retain copies of the aforementioned material. CONTRACTOR has the right, at its own expense, to appoint a CONTRACTOR representative to participate in the audit.

## COMPANY will also be allowed to perform an audit under the same conditions provided in this article on compliance with all or parts of this AGREEMENT.

## Unless COMPANY reasonably suspects non-compliance, COMPANY cannot perform an audit on matters that have been audited by COMPANY in the previous twelve months. For the avoidance of doubt, COMPANY can perform multiple audits a year, or simultaneously, as long as the scope of those audits is different.

## In the event an audit or CONTRACTOR's compliance monitoring reveals any deficiencies, weaknesses or areas of non-compliance, CONTRACTOR will, without prejudice to COMPANY’s other rights or remedies, promptly take such steps as may be required to remedy those deficiencies, weaknesses, areas of non-compliance as soon as is practicable under the circumstances and in any case within 6 months from the date the audit results are communicated in writing to CONTRACTOR. The costs related to the remedial actions are the sole responsibility of the CONTRACTOR.

## CONTRACTOR will keep COMPANY informed of the status of any remedial action, including the estimated timetable for completing the remedial actions, and will provide written confirmation to COMPANY as soon as any remedial action has been completed.

# INFORMATION SHARING

## Most Confidential

CONTRACTOR will not access or store COMPANY DATA classified as, or reasonably understood to be, 'Most Confidential', unless explicitly authorized by COMPANY in writing in advance. CONTRACTOR will notify COMPANY immediately if it receives, or has access to such COMPANY DATA, will return or destroy such COMPANY DATA immediately, and CONTRACTOR will not be entitled to use or disclose such COMPANY DATA for any reason.

## Anti-Trust & CSI

CONTRACTOR will not access COMPANY DATA which is CSI without COMPANY's explicit prior written consent, which consent will only be provided if, and to the extent, access to such CSI is deemed strictly necessary for the execution of the CONTRACT. CONTRACTOR will notify COMPANY immediately if it receives, or has access to, COMPANY DATA which is CSI without receiving prior written consent. CONTRACTOR will return or destroy such COMPANY DATA immediately and CONTRACTOR will not be entitled to use or disclose such COMPANY DATA for any reason. For the avoidance of doubt, in all circumstances the disclosure of any CSI is and remains subject to legal restrictions.

## Technical and Non-Technical Security Measures

CONTRACTOR will take all appropriate technical measures and assure it and CONTRACTOR PERSONNEL take all reasonable security measures to (i) protect the integrity of, (ii) prevent unintentional disclosure of, and (iii) prevent unauthorized access to COMPANY DATA.

## Limitation on use of COMPANY DATA and MATERIALS

CONTRACTOR will neither use nor disclose any COMPANY DATA or MATERIALS to CONTRACTOR PERSONNEL or THIRD PARTIES with the aim to (i) procure any types of materials or services similar to the services or the materials provided by COMPANY or AFFILIATES of COMPANY or (ii) provide any types of materials or services similar to the services or the materials provided by COMPANY or AFFILIATES of COMPANY to a THIRD PARTY, other than expressly agreed under the CONTRACT.

## Segregation of COMPANY DATA

CONTRACTOR will, and will ensure that CONTRACTOR PERSONNEL will, take reasonable efforts to logically segregate COMPANY DATA from the data of CONTRACTOR or third parties.

## Qualification of COMPANY DATA

CONTRACTOR acknowledges and agrees that any COMPANY DATA or MATERIALS received by it or CONTRACTOR PERSONNEL is on an "as is" basis. COMPANY makes no representations, extends no warranties of any kind, either express or implied, accepts no liability EVEN IF NEGLIGENT, and assumes no responsibilities whatsoever with respect to fitness for a particular purpose, merchantability, non-infringement, suitability, accuracy or completeness of the COMPANY DATA or any MATERIALS provided by COMPANY, all to the fullest extent permitted by APPLICABLE LAW.

## Minimum Requirements

CONTRACTOR acknowledges that any IT requirements imposed on it are minimum requirements and CONTRACTOR should independently verify whether additional requirements or controls are necessary. CONTRACTOR further acknowledges that any advice, training or other information received are provided "as is" and any use or implementation of such advice, training or information is solely for the account and risk of CONTRACTOR, who should independently verify whether additional advice, training or information is necessary.

## IP RIGHTS, Warranties and Indemnities

### Nothing in the AGREEMENT or this APPENDIX will be construed as a transfer to CONTRACTOR or the AUTHORIZED USERS of the IP RIGHTS related to or that vest in the COMPANY IT INFRASTRUCTURE, COMPANY DATA or the MATERIALS.

### CONTRACTOR represents and warrants that:

#### it either owns or is entitled to licence any and all IP RIGHTS in any software and services that CONTRACTOR provides to COMPANY under the CONTRACT;

#### it will not use any available open source software of any third parties; and

#### that any software and services that CONTRACTOR provides to COMPANY under the AGREEMENT will function in accordance with the agreed functional specifications.

### CONTRACTOR will at its own expense defend, hold harmless and indemnify COMPANY from and against all claims, proceedings, judgements, liabilities, losses, damages, costs (including legal costs), fines penalties, assessments and expenses arising out of (i) any allegation or claim that the software or the services or the possession or use of the software or the services provided by CONTRACTOR under the AGREEMENT infringes any IP RIGHTS of any third party; and (ii) any breach by CONTRACTOR of this sub-article.

# RECORDS MANAGEMENT

## CONTRACTOR will at all times maintain and keep, complete and accurate records of, and adequate supporting documents and a complete audit trail for, all of the following:

### audits as mentioned in this APPENDIX);

### user activity,

### SECURITY INCIDENTs;

### NEAR MISSES; and

### such other information as COMPANY may reasonably specify from time to time.

## CONTRACTOR will maintain and keep the aforementioned items for the duration of this AGREEMENT and thereafter for the longer of:

### the period required by any APPLICABLE LAW; or

### seven years.

# TRADE CONTROLS

## International Travel or Data Transmission

### CONTRACTOR acknowledges that (i) COMPANY IT INFRASTRUCTURE may be located or supported in countries other than where CONTRACTOR is located and (ii) that provided connectivity may be across international borders and therefore subject to limitations under this article or APPLICABLE LAW.

### CONTRACTOR will ensure (i) that it and CONTRACTOR PERSONNEL will comply with all APPLICABLE LAWS relating to international travel and international data transmission and (ii) that all CONTRACTOR PERSONNEL will check whether they are allowed to import COMPANY IT INFRASTRUCTURE into their destination country before travelling or sending it there.

## Encryption

### The services and MATERIALS may contain, or utilize, encryption functionality, which may be subject to use, import or export restrictions in a variety of countries. CONTRACTOR will ensure compliance with all APPLICABLE LAWS relating to encryption functionality contained in, or utilized by, the services or MATERIALS. COMPANY will provide CONTRACTOR, at its request, with relevant information as reasonable requested and specified by CONTRACTOR in order to determine any restrictions related to encryption.

### CONTRACTOR will not, and will ensure that CONTRACTOR PERSONNEL will not, provide any encryption keys to any authorities without first receiving written approval from COMPANY. If such is not possible, CONTRACTOR will inform COMPANY in writing of the provision of encryption keys as soon as possible.

# E-DISCOVERY

## When COMPANY IT INFRASTRUCTURE is located at a CONTRACTOR WORKSITE, or any other location within CONTRACTOR'S control, CONTRACTOR will, within a reasonable time and upon request, provide COMPANY access to such COMPANY IT INFRASTRUCTURE.

## When COMPANY IT FACILITIES or COMPANY DATA is located on CONTRACTOR IT EQUIPMENT, CONTRACTOR will, upon written request and reasonable notice, provide COMPANY or its representative the opportunity to produce a forensic copy of such COMPANY IT FACILITIES or COMPANY DATA, as soon as possible after such request. If required by APPLICABLE LAWS, and only to the extent the requirements of the APPLICABLE LAWS cannot be fulfilled by remote interrogation or remote access, CONTRACTOR will provide COMPANY or its representative access and control over the physical CONTRACTOR IT EQUIPMENT on which COMPANY IT FACILITIES or COMPANY DATA is located. CONTRACTOR may, at its own cost, supervise any such physical access. CONTRACTOR will not, and will ensure that CONTRACTOR PERSONNEL will not, delete any COMPANY DATA contained on the relevant CONTRACTOR IT EQUIPMENT as from the moment the written notice has been received by the CONTRACTOR.

## CONTRACTOR will be liable for all fees, fines, and penalties, expenses and/or liabilities incurred by COMPANY or AFFILIATES of COMPANY resulting, or related to, a breach of this article. Any such fees, fines, and penalties, expenses and/or liabilities are deemed direct damages.

# TERMINATION

## COMPANY may, at any time, restrict, suspend or terminate the access to COMPANY IT INFRASTRUCTURE for one or more AUTHORIZED USERS.

## Upon termination of access, CONTRACTOR will immediately ensure that all relevant COMPANY IT INFRASTRUCTURE or MATERIALS provided, including all copies and documentation, relating thereto are returned to COMPANY or, if so directed by COMPANY, destroyed as soon as possible.

# NOTICES

All notices or other communications under the AGREEMENT must be in English and in writing, and: (i) delivered by hand; (ii) sent by prepaid courier; (iii) sent by registered post; or (iv) sent by email with confirmation receipt requested. Notices will be addressed to the individuals provided to receive notices under the CONTRACT. Notices and communications are effective when actually delivered at the address specified in the CONTRACT.

# GOVERNING LAW AND DISPUTE RESOLUTION

## Governing Law

This CONTRACT, and any dispute or claim arising out of or in connection with this CONTRACT or its subject matter or formation, including any non-contractual disputes or claims, will be exclusively governed by and construed in accordance with the laws of England and Wales, excluding conflict of law rules and choice of law principles that provide otherwise. The United Nations Convention on the International Sale of Goods will not apply to this CONTRACT.

## Dispute Resolution

### Any dispute or claim arising out of or in connection with the CONTRACT or its subject matter or formation, whether in tort, contract, under statute, or otherwise, including any question regarding its existence, validity, interpretation, breach, or termination, and including any non-contractual claim, will be finally and exclusively resolved by arbitration at Singapore International Arbitration Centre (“SIAC”) under its then current arbitration rules (the “RULES”). The arbitral tribunal, to be appointed in accordance with the RULES, will consist of one arbitrator. However, if either party asserts the amount in controversy exceeds USD $5 million, then the tribunal will consist of three arbitrators. The seat of the arbitration will be Singapore. The language of the arbitration will be English.

### The International Bar Association (“IBA”) Rules on the Taking of Evidence in International Arbitration will apply to the arbitration. Each party waives, to the fullest extent permitted by law any right under the laws of any jurisdiction: (i) to apply to any court or other judicial authority to determine any preliminary point of law; and (ii) to appeal or otherwise challenge the award, other than on the same grounds on which recognition and enforcement of an award may be refused under Article V of the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958 (“The New York Convention”).

### Nothing in this Article will be construed as preventing any party from seeking conservatory or similar interim relief from any court with competent jurisdiction. Any award rendered by the arbitral tribunal will be made in writing and will be final and binding on the parties. The parties will carry out the award without delay. Judgment upon any award or order may be entered in any court having jurisdiction. All aspects of the arbitration will be considered confidential.

# ADDITIONAL LEGAL PROVISIONS

COMPANY is entitled to specific performance of the AGREEMENT. A provision of the AGREEMENT is not waived unless made in writing by an authorised representative of the waiving party. The waiver of a right or the partial exercise of a remedy does not limit a party’s entitlement to exercise such right or remedy in the future. Members of CONTRACTOR GROUP or COMPANY GROUP not a party to the AGREEMENT, but conferred rights in it, are entitled to enforce those rights, but their consent will not be required to amend or terminate the AGREEMENT, even if it affects those rights. Otherwise, the parties do not intend that any term of this AGREEMENT should be enforceable by any PERSON who is not a party. The AGREEMENT may be signed in any number of counterparts, all of which constitute a single instrument.

**Signatories**

|  |  |
| --- | --- |
| **For and on behalf of BRUNEI SHELL PETROLEUM COMPANY SENDIRIAN BERHAD**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name:Position: | **For and on behalf of [\*\*insert full CONTRACTOR name]**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name:Position: |