**Process Control Domain IT Security Agreement for Enterprise Industrial Automation Information Technology and Security for Integration and Maintenance Services**

**THIS AGREEMENT IS MADE ON [\*\*insert date] BETWEEN:**

[\*\*COMPANY],

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

and

[\*\*CONTRACTOR],

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

**RECITALS**

1. COMPANY and CONTRACTOR have entered into one or more CONTRACTS whereby CONTRACTOR GROUP may need access to COMPANY PCD INFRASTRUCTURE and/or CONTRACTOR will perform certain PCD SERVICES;
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:

|  |  |
| --- | --- |
| **ACCEPTANCE** | will have the meaning ascribed thereto in the CONTRACT. |
| **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 Process Control Domain 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 PCD INFRASTRUCTURE. |
| **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. |
| **COMPLETION**  | will have the meaning ascribed thereto in the CONTRACT. |
| **CONTRACT** | the contract under which the CONTRACTOR is providing certain goods and/or services for COMPANY as described therein, necessitating access to COMPANY PCD INFRASTRUCTURE and/or the provision of certain PCD SERVICES. |
| **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 PCD EQUIPMENT** | PCD equipment owned or contracted by CONTRACTOR GROUP for use 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. |
| **COMPANY DATA** | (a) any information, including CONFIDENTIAL INFORMATION, and data obtained, or accessible, via or in connection with the COMPANY PCD EQUIPMENT or COMPANY PCD 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 PCD EQUIPMENT** | those items of PCD equipment, PCD machinery, PCD components, PCD instruments and PCD accessories, together with any documentation made accessible, or provided, by, or on behalf of, COMPANY, or AFFILIATES of COMPANY. |
| **COMPANY PCD 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 PCD INFRASTRUCTURE** | the COMPANY PCD EQUIPMENT, the COMPANY PCD FACILITIES or the COMPANY DATA. |
| **CONFIDENTIAL INFORMATION** | will have the meaning ascribed thereto in the CONTRACT. |
|  |  |
| **INDEMNIFY** | will have the meaning ascribed thereto in the CONTRACT. |
| **INTEGRATION SERVICES** | CONTRACTOR providing services for the implementation of automation solutions in accordance with the PCD SECURITY STANDARD and the terms and conditions of this Agreement.  |
| **LIABILITIES** | will have the meaning ascribed thereto in the CONTRACT. |
| **MAINTENANCE SERVICES** | CONTRACTOR providing services to maintain and service PCD in accordance with the PCD SECURITY STANDARD and the terms and conditions of this Agreement. Maintenance activities are separate from activities used to operate the PCD and fall into two categories 1. those that apply specifically to maintaining the security of the PCD
2. and those that apply to maintaining other aspects of the PCD, such as device and equipment maintenance, with the purpose to ensure that PCD security is maintained and at minimum not degraded as a result of these activities
 |
| **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** | any event that could (a) disrupt the expected standard operation, (b) cause denial of operation or (c) inappropriate access to or use of any PCD service, facility, data or system but did not.  |
| **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. |
| **PROCESS CONTROL DOMAIN (PCD)** | devices that are dedicated to control, monitor or safeguard the equipment and operation of a specific WORKSITE. These include, amongst others, computers, workstations, servers, network devices, logic-solvers, controllers, intelligent electrical devices and instruments as well as any devices used to directly support the functions provided by this system (e.g. backup, active directory).  |
| **PCD SECURITY STANDARDS** | The stricter of the industrial automation and control systems security specifications, standards and practices that are internationally recognized as being sufficient to safeguard PCD INFRASTRUCTURE, such as the NIST Framework for Improving Critical Infrastructure Cybersecurity or IEC 62443 – Security for Industrial Automation and Control Systems and COMPANY’s standards as listed in APPENDIX 1 of this AGREEMENT, as amended from time to time, which specifies requirements and gives recommendations for PCD security of control and automation systems during the access by CONTRACTOR GROUP of the COMPANY PCD INFRASTRUCTER and the performance of the PCD SERVICES by CONTRACTOR. |
| **PCD SERVICES** | the INTEGRATION SERVICES and/or the MAINTENANCE SERVICES |
| **SECURITY INCIDENT** | any event that (a) disrupts the expected standard operation, (b) causes denial of operation or (c) inappropriate access to or use of any PCD service, facility, data or system caused by system failure or human error. |
| **WORKSITE** | will have the meaning ascribed thereto in the CONTRACT. |

#

# PCD SECURITY REQUIREMENTS

## In all instances in which CONTRACTOR GROUP has access to, or uses, COMPANY PCD INFRASTRUCTURE or CONTRACTOR performs PCD SERVICES such will be done in accordance with the terms and conditions of this AGREEMENT. CONTRACTOR will procure compliance thereof from the relevant members of CONTRACTOR GROUP and will INDEMNIFY COMPANY GROUP for any LIABILITIES arising out of CONTRACTOR GROUP’s non-compliance with such PCD SECURITY STANDARDS or this AGREEMENT.

# PCD SECURITY STANDARD

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

## CONTRACTOR will promptly notify COMPANY in writing of any material changes to the way CONTRACTOR has implemented the PCD SECURITY STANDARD as soon as reasonably practicable.

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

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

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

# PCD ACCESS AND SERVICES

In the event of required access to COMPANY PCD INFRASTRUCTURE and in the performance of PCD SERVICES, CONTRACTOR must to comply with the following requirements at its own cost and expense unless explicitly agreed otherwise in writing in this Agreement:

## **ASSET INVENTORY**

### CONTRACTOR will provide accurate logical and physical infrastructure drawings and documentation of COMPANY PCD FACILITIES or COMPANY PCD EQUIPMENT provided in accordance with the CONTRACT or this AGREEMENT, including its network devices, internal interfaces, and external interfaces. CONTRACTOR must after every change update and provide the updated documentation and drawings to ensure such is an accurate representation of COMPANY PCD FACILITIES or COMPANY PCD EQUIPMENT.

### CONTRACTOR must after every change update and provide the as-built and installed COMPANY PCD EQUIPMENT connection and configuration documents.

## **RISK ASSESSMENT**

## CONTRACTOR will conduct a security risk assessment of COMPANY PCD INFRASTRUCTURE or contribute to (participate in) a security risk assessment conducted by COMPANY.

## **PCD MODIFICATIONS & MANAGEMENT OF CHANGE**

## CONTRACTOR requires COMPANY’s prior written approval before making any changes; modifications or updates to COMPANY PCD INFRASTRUCTURE.

## **SECURE ARCHITECTURE**

###  CONTRACTOR will ensure that the physical network segmentation architecture used in COMPANY PCD FACILITIES, including its use of network security devices or equivalent mechanisms, in accordance with the design approved by COMPANY.

###  CONTRACTOR will ensure that time distribution/synchronization for the COMPANY PCD FACILITIES is performed from a secure and accurate source that uses a protocol that is accepted by the COMPANY.

### CONTRACTOR will ensure that architecture documentation describing wireless systems will accurately describe the following:

#### Data exchange between a Level 1 (Safety Instrumented System and/or Basic Process Control) network and wireless instrumentation,

#### Data exchange between a Level 2 (Supervisory Control) network and a Level 3 (Operations Management) network through a secure wireless link,

#### Security mechanisms that prevent an intruder from gaining access to COMPANY PCD EQUIPMENT using the wireless system,

#### Security mechanisms that restrict access within COMPANY PCD FACILITIES by personnel with handheld wireless devices, and

#### Where required, security mechanisms that provide protection for remote management of wireless systems.

## **VULNERABILITY MANAGEMENT**

### CONTRACTOR must provide documentation that:

#### verifies that COMPANY PCD EQUIPMENT identified by COMPANY (e.g. as result of a security assessment, threat analysis, and/or security testing) has adequate security appropriate to such equipment’s level of risk;

#### describes how to harden the security of COMPANY PCD EQUIPMENT, including whitelisting capabilities;

#### describes how to mitigate security weaknesses inherent in the design and/or implementation of communication protocols used in the COMPANY PCD EQUIPMENT that were known prior to COMPANY PCD EQUIPMENT integration or maintenance activities.

#### describes a strategy for all security patches and updates required for COMPANY PCD EQUIPMENT which CONTRACTOR pursuant to the CONTRACT provided, advised on or maintained including, amongst others:

##### a detailed description of each patch which must be available to COMPANY within an agreed time frame after the release of a patch by its manufacturer.

##### the approval status/lifecycle state of each patch and update; i.e., approved, not approved, not applicable, in test,

##### a warning if the application of an approved patch requires or causes a re-start of the system,

##### the reason for those patches and updates that are not approved or not applicable,

##### a plan for the remediation for those patches and updates that are applicable but not approved.

### CONTRACTOR must recommend security analysis tools (e.g. network scanning tools) for use on COMPANY PCD EQUIPMENT and will (i) provide instructions on how to use them, (ii) identify any known adverse effects such tools may have on COMPANY PCD EQUIPMENT’s performance, (iii) provide recommendations how to prevent such adverse effects

### CONTRACTOR must represent and warrant that its security hardening guidelines and procedures are followed during COMPANY PCD EQUIMENT related activities.

### CONTRACTOR is responsible to close any gaps in COMPANY PCD EQUIPMENT’s security hardening, including gaps in COMPANY’s PCD SECURITY STANDARDS, that affect or may affect such COMPANY PCD EQUIPMENT, whether such gaps in security where discovered in COMPANY PCD EQUIPEMENT pursuant to this AGREEMENT or which are publicly known vulnerabilities affecting equipment like COMPANY PCD EQUIPMENT or that should have been known by CONTRACTOR to have such affect.

### CONTRACTOR's security hardening guidelines and procedures must represent and warrant that only necessary, authorised, and documented digital certificates for certificate authorities (CAs) are installed.

### CONTRACTOR will make available to COMPANY, through an interface commonly accepted by the industrial and security communities, a patch list that identifies:

#### approved security patches applicable to COMPANY PCD EQUIPMENT software which CONTRACTOR pursuant to the CONTRACT provided, advised on or maintained including (e.g. control system and component software, operating system software, and 3rd party software applications),

#### which of the applicable security patches have been approved for use in COMPANY PCD EQUIPMENT,

#### the version numbers of the software to which the approved patches apply,

#### this list shall be made available to COMPANY within an agreed timeframe after the release of a patch by the manufacturer.

### CONTRACTOR will require the prior written approval from COMPANY for installing each security patch.

###  CONTRACTOR will ensure that if COMPANY requests CONTRACTOR to install security software patches (including firmware upgrades), CONTRACTOR installs as soon as possible when requested by COMPANY.

### CONTRACTOR must ensure that the security hardening level of COMPANY PCD EQUIPMENT is retained after each patch installation, e.g. by reinstalling software or changing system configuration settings.

## **PORTABLE MEDIA & DEVICE**

## CONTRACTOR must represent and warrant that portable media, including installation media and portable computers, used in or connected to COMPANY PCD EQUIPMENT by CONTRACTOR is free of known malware prior to use in COMPANY PCD INFRASTRUCTURE.

## **MALWARE PROTECTION**

## CONTRACTOR must provide COMPANY with documented instructions for the proper installation, configuration and update of malware protection mechanisms that are tested and verified for COMPANY PCD EQUIPMENT.

### CONTRACTOR must represent and warrant that:

#### malware protection engines and versions have the prior written agreement from COMPANY before installation,

#### malware protection mechanisms have been correctly installed/updated and properly configured in accordance with COMPANY's approved standards and procedures,

#### malware definition files are installed within the time period instructed by COMPANY,

#### malware configurations are maintained and kept up to date.

### CONTRACTOR must represent and warrant that malware, other than zero-day malware, can be detected and properly handled by the installed malware protection mechanisms.

### CONTRACTOR will provide to COMPANY documentation that describes:

#### how malware definition files for COMPANY PCD EQUIPMENT are evaluated and approved,

#### reporting the status of malware definition files to COMPANY within 7 days after release of the files by the manufacturer, unless otherwise agreed in writing by CONTRACTOR and COMPANY. This status includes the applicability (e.g. component and version) and approval state (e.g. approved, installed, disapproved, etc.) for each malware definition file.

### CONTRACTOR will have the capability to ensure that all devices, including workstations, supplied to COMPANY PCD FACILITY by CONTRACTOR are free of malware prior to use by COMPANY.

## **SYSTEM BACKUPS**

### CONTRACTOR will provide documentation for recommended backup procedures for COMPANY PCD EQUIPMENT that include, but is not limited to the following:

#### Instructions on how to make a full backup of COMPANY PCD EQUIPMENT, and partial backups if applicable, using at least one of the following methods

### proprietary backup architecture on removable media,

### single system backup architecture on removable media,

### distributed back-up architecture in which each backup system backs up a subset of the CONTRACTOR's Automation Solutions at COMPANY PCD FACILITY, or

### centralized back-up architecture using one backup system for all of the CONTRACTOR's Automation Solutions at COMPANY PCD FACILITY.

####  Provisions to back-up the following types of data

### operation system files and cryptographic data (e.g. keying material),

### applications (including middleware, such as tunnelling software),

### configuration data, database files,

### log files, electronic log book,

### unconventional file types including, but not limited to network equipment settings, control system controller settings (tuning parameters, set points, alarm levels),

### field instrumentation parameters,

### directory information, and

### other files identified by CONTRACTOR that are required to create a complete backup of COMPANY PCD EQUIPMENT,

#### Recommendations for offsite storage of backup media,

#### Provisions to ensure changes to COMPANY PCD EQUIPMENT that could affect the integrity of a backup are not made while a backup is in progress.

### CONTRACTOR will have the capability to provide documented instructions to COMPANY for restoring COMPANY PCD EQUIMENT or its components to normal operation.

### CONTRACTOR will have the capability to provide documentation to COMPANY that describes how to control and securely manage removable backup media.

### CONTRACTOR will provide documentation to COMPANY that describes how to verify successful system backup.

### CONTRACTOR must, at COMPLETION or ACCEPTANCE (as the case may be), verify that:

#### it is possible to perform a complete back-up of COMPANY PCD EQUIPMENT, and

#### it is possible to restore a fully functioning COMPANY PCD EQUIPMENT from this back-up.

### CONTRACTOR must perform a backup of COMPANY PCD EQUIPMENT in accordance with COMPANY'S backup schedules and data restore and disaster recovery objectives.

### CONTRACTOR must ensure, prior to the start of such backup, that COMPANY PCD EQUIPMENT is able to continue normal operation during a backup.

### CONTRACTOR must documentation to COMPANY that describes how to generate and maintain audit logs of all backup and restore activities.

### CONTRACTOR must document a recommended disaster recovery plan that includes, but is not limited to the following:

#### Description of various disaster scenarios and their impact on COMPANY PCD INFRASTRUCTURE,

#### Step-by-step instructions for restoring, restarting, failed components and integrating them into COMPANY PCD INFRASTRUCTURE,

#### Minimum architecture requirement for restoring COMPANY PCD EQUIPMENT.

# CONTRACTOR'S OBLIGATIONs

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

## CONTRACTOR will not attempt to

### access any other systems or facilities;

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

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

### install or cause to be installed into or on COMPANY PCD EQUIPMENT or COMPANY PCD 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 PCD INFRASTRUCTURE.

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

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

## COMPANY can impose additional security standards and controls on CONTRACTOR PCD EQUIPMENT used to (i) connect to COMPANY PCD EQUIPMENT or COMPANY PCD 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 PCD EQUIPMENT or COMPANY PCD EQUIPMENT under its control and (ii) unauthorized access to COMPANY DATA under its control.

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

# ACCESS FOR AUTHORIZED USERS

## CONTRACTOR will not allow access to COMPANY PCD INFRASTRUCTURE to others than the AUTHORIZED USERS.

## 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 PCD EQUIPMENT and COMPANY PCD 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 whose access can be terminated.

## AUTHORIZED USERS will be given access to those parts of the COMPANY PCD INFRASTRUCTURE 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 user-id and password, CONTRACTOR will instruct AUTHORIZED USERS to:

### not disclose or give their 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 user-id or password;

### make every reasonable effort to prevent any situation that would allow any person to obtain access to their 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 PCD INFRASTRUCTURE is at the CONTRACTOR's own risk. The CONTRACTOR fully INDEMNIFIES COMPANY GROUP against all LIABILITIES by any AUTHORIZED USERS, relating to the COMPANY PCD 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.

## CONTRACTOR will immediately notify the COMPANY of changes in CONTRACTOR PERSONNEL who have access to COMPANY PCD FACILITIES or COMPANY PCD EQUIPMENT.

# 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 PCD EQUIPMENT and COMPANY PCD 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 PCD INFRASTRUCTURE and does not warrant that the access to the COMPANY PCD 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 PCD INFRASTRUCTURE for security reasons at any time without notice. Such monitoring may include inspection of the COMPANY PCD 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 PCD 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 PCD INFRASTRUCTURE.

# SOFTWARE

## COMPANY may, from time to time, make available MATERIALS for use on COMPANY PCD EQUIPMENT or CONTRACTOR PCD 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 PCD 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 PCD SECURITY STANDARD, and (ii) compliance with PCD controls contained, or referred to, in the CONTRACT or work orders or similar documents issued thereunder; and

### use of the COMPANY PCD 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

## Access and Storing COMPANY DATA

CONTRACTOR will not access or store COMPANY DATA, 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.

## 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 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 PCD 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 PCD 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 PCD 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 PCD INFRASTRUCTURE.

## When COMPANY PCD FACILITIES or COMPANY DATA is located on CONTRACTOR PCD EQUIPMENT, CONTRACTOR will, upon written request and reasonable notice, provide COMPANY or its representative the opportunity to produce a forensic copy of such COMPANY PCD 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 PCD EQUIPMENT on which COMPANY PCD 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 PCD 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 PCD INFRASTRUCTURE for one or more AUTHORIZED USERS.

## Upon termination of access, CONTRACTOR will immediately ensure that all relevant COMPANY PCD 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 [\*\*insert full COMPANY name]**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name:Position: | **For and on behalf of [\*\*insert full CONTRACTOR name]**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name:Position: |

**APPENDIX 1**

**COMPANY PCD SECURITY STANDARDS**

### Integration Services – BSP Process Control Domain Security Specification Standard and the BSP Industrial Automation Control System Architecture Design Standard

### Maintenance Services – IRM 3.318 – Risk Profile Process Control Domain and Process Control Domain Integrity Recommended Practices