SUPPLY AGREEMENT

GENERAL TERMS AND CONDITIONS

1. GOODS AND/OR SERVICES

If Supplier is only supplying Services, the terms of this Contract applicable to Goods do not apply. If Supplier is only supplying Goods, the terms of this Contract applicable to Services do not apply.

2. DEFINITIONS AND INTERPRETATION

2.1. Terms not defined in these General Terms and Conditions have the meanings set out in the Order and/or the Specific Terms and Conditions. In addition:

"Applicable Laws": all applicable laws, by-laws, enactments, regulations, regulatory policies, ordinances, licences or orders of any court, tribunal or governmental, statutory, regulatory, judicial, administrative or supervisory authority, body or board, which are in force during the term of this Contract;

"**Authorisations**": all the licences, permissions, authorisations, consents and permits that the Supplier needs to comply with to carry out its obligations under this Contract;

"**Contract**": the Order, the Specific Terms and Conditions, these General Terms and Conditions, and any Schedules, Annexes and Appendices;

"**Deliverables**": all documents, reports, presentations, products, materials and data developed by Supplier or its agents, subcontractors, consultants, employees or affiliates in relation to the Services in any form, including any specific deliverables listed in the Order, Specific Terms and Conditions and/or Schedule 1;

"**Delivery Schedule**": the schedule for delivery of the Goods and/or Services, as set out in the Order and/or the Specific Terms and Conditions and/or Schedule 1;

"**Goods**": the goods to be provided by Supplier pursuant to this Contract, as described in the Order and/or the Specific Terms and Conditions and/or Schedule 1;

"**Insolvent**": such party being unable to pay its debts as they fall due and/or that the value of its assets is less than the amount of its liabilities taking into account its contingent and prospective liabilities, or such party being an individual, company or partnership voluntary arrangement, has a receiver, administrator or manager appointed over the whole or any part of its business or assets; or if an order shall be made or resolution passed for its winding up (except for the purpose of a bona fide amalgamation or reconstruction), or is subject to bankruptcy or dissolution, or if it shall otherwise propose or enter into any composition or arrangement with any or all classes of its creditors, or if it ceases or threatens to cease to carry on business or if it claims the benefit of any statutory moratorium;

"**Intellectual Property Rights**": patents, rights to inventions, copyright and related rights, moral rights, trade marks and service marks, business names and domain names, rights in get-up, goodwill and the right to sue for passing off, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets) and all other intellectual property rights, whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world;

"**Location**": the location(s) to which Goods will be delivered and/or at which Services will be provided, as specified in the Order and/or the Specific Terms and Conditions and/or Schedule 1;

"Mandatory Policies": SMRT's mandatory policies and codes of practice in force during the term of this Contract, including policies concerning health and safety, ethics, employment practices, privacy and data protection, cybersecurity and anti-bribery and corruption, and the policies set out in Schedule 2;

"**Order**": the purchase order(s) for Goods and/or Services issued by SMRT to the Supplier;

"**PDPA**" means Singapore's Personal Data Protection Act 2012 as amended and modified from time to time;

"**Personal Data**" shall have the same meaning ascribed to it in the PDPA;

"**Price**": the price payable by SMRT for Goods and/or Services, as set out in the Order and/or the Specific Terms and Conditions and/or Schedule 1;

"**Professional Practice**": practices, methods and procedures which would be adopted by a supplier exercising in the general conduct of its undertaking that degree of skill, diligence, prudence and foresight which would ordinarily and reasonably be expected from a supplier engaged in the business of providing services which are the same as or similar to the Services under the same or similar circumstances and conditions;

"**Services**": the services to be provided by Supplier pursuant to the Order and/or the Specific Terms and Conditions and/or Schedule 1, and such other services as are reasonably necessary for the performance, or enjoyment of the benefit, of such services;

"**Start Date**": the date on which this Contract commences, as specified in the Order and/or the Specific Terms and Conditions; and

"**Term**": the term of this Contract, as specified in the Order and/or the Specific Terms and Conditions.

2.2. In this Contract, (a) a reference to a statute or statutory provision is a reference to such statute or provision or subordinate legislation as amended or re-enacted; (b) the use of "including", "include", or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms; and (c) a reference to writing or written excludes emails unless otherwise specified.

2.3. If there is any conflict or inconsistency between the relevant parts of this Contract, the order of precedence shall be (unless expressly stated otherwise) as follows: first, the Order; then the Specific Terms and Conditions, then the General Terms and Conditions, then the Schedules, Annexes and Appendices (excluding the Supplier terms and conditions (if any)); and then the Supplier terms and conditions (if any) insofar as agreed in writing between Parties to form part of this Contract.

3. SUPPLY OF GOODS

3.1. Supplier warrants, represents and undertakes that it shall ensure that the Goods: (a) correspond with their description and any applicable specifications; (b) are of satisfactory quality and free from defects in material (including any raw materials contained in them), fabrication and workmanship and remain so for twelve (12) months after delivery; (c) comply with all Applicable Laws; and (d) are fit for any purpose held out by Supplier or made known to Supplier by SMRT prior to delivery.

3.2. Supplier warrants, represents and undertakes that at all times, it has and maintains the Authorisations and complies with Applicable Laws and the Mandatory Policies.

3.3. Supplier shall deliver the Goods: (a) according to the Delivery Schedule; (b) at the relevant Location; and (c) during SMRT's normal business hours, or as otherwise instructed by SMRT in writing. Supplier shall ensure that the Goods are properly packed and secured so as to enable them to reach their destination in good condition. Delivery is complete upon completion of unloading at the relevant Location.

3.4. SMRT has the right to inspect, test and approve or reject the Goods at any time (prior to, on or after delivery). Title and risk in the Goods shall pass to SMRT on completion of delivery. If SMRT considers that the Goods do not comply or are unlikely to comply with the requirements of this Contract, SMRT shall inform Supplier and Supplier shall immediately take such remedial action as is necessary to ensure compliance. SMRT shall have the right to conduct further inspections and tests after Supplier has carried out its remedial actions.

3.5. Notwithstanding SMRT's payment for the Goods, such payment shall not constitute evidence of SMRT's acceptance of the Goods and Supplier shall not be relieved from its responsibility to replace any defective or damaged Goods in accordance with clause 7 (***SMRT Remedies***).

4. SUPPLY OF SERVICES

4.1. Supplier warrants, represents and undertakes that it shall supply the Services from the Start Date for the Term: (a) with reasonable skill and care; and (b) in accordance with: (i) the Mandatory Policies; (ii) good industry practice; (iii) SMRT's instructions from time to time; (iv) Applicable Laws; and (v) the Delivery Schedule.

4.2. Supplier warrants, represents and undertakes that it shall ensure that at all times it has and maintains the Authorisations that it needs to carry out its obligations under this Contract.

4.3. SMRT has the right to inspect, test and approve or reject the Deliverables at any time (prior to, on or after delivery). Title and risk in the Deliverables shall pass to SMRT on completion of delivery. If SMRT considers that the Deliverables do not comply or are unlikely to comply with the requirements of this Contract, SMRT shall inform Supplier and Supplier shall immediately take such remedial action as is necessary to ensure compliance. SMRT shall have the right to conduct further inspections and tests after Supplier has carried out its remedial actions

4.4. Notwithstanding SMRT's payment for the Deliverables, such payment shall not constitute evidence of SMRT's acceptance of the Deliverables and Supplier shall not be relieved from its responsibility to replace any defective or damaged Deliverables in accordance with clause 7 (***SMRT Remedies***).

5. STATUS OF PERSONNEL

Supplier warrants, represents and undertakes that it shall ensure that all of its personnel (including its subcontractors) are legally entitled to work in Singapore according to Applicable Laws. Supplier is solely responsible for its personnel, who will at all times remain employees of Supplier.

6. VARIATION, AMENDMENT AND CANCELLATION

6.1. SMRT may vary or amend all or part of any order for Goods and/or Services by giving Supplier prior notice. Subject to receipt by SMRT of reasonable evidence, SMRT shall pay Supplier fair and reasonable compensation for any work already completed on the Goods and/or Services in accordance with this Contract (including any out-of-pocket expenses incurred or committed by Supplier at the time of termination).

6.2. SMRT may, at any time, cancel any order for Goods and/or Services by giving Supplier thirty (30) days

written notice. SMRT shall, in such circumstances, pay Supplier for any work already completed on the Goods and/or Services in accordance with the relevant Order.

6.3. For the avoidance of doubt, compensation under this clause 6 (***Variation, Amendment and Cancellation***) shall exclude loss of anticipated profits or any consequential loss. The total amount payable shall under no circumstances exceed the pro-rata Price calculated in relation to the actual Goods and/or Services delivered in accordance with this Contract, prior to the receipt by Supplier of written notice of variation, amendment or cancellation.

6A. INFORMATION TECHNOLOGY

6A.1. This clause only applies if Supplier is providing software in connection with the performance and/or delivery of the Goods and/or Services ("**Supplier System**").

6A.2 Supplier shall ensure that any Supplier System complies with the terms of this Contract, Applicable Laws and Professional Practice.

6A.3 Supplier shall:

6A.3.1. support and maintain the Supplier System throughout the Term in accordance with this Contract and Professional Practice;

6A.3.2. ensure that the Supplier System is fit for any specific purpose for which Supplier knew or ought reasonably to have known such Supplier System would be used by SMRT (including the way in which such Supplier System is intended to interface with any of SMRT's pre-existing hardware or equipment with which such Supplier System is intended to interface);

6A.3.3. ensure that the Supplier System complies with the Mandatory Policies, including any IT and/or data security requirements specified in the Mandatory Policies;

6A.3.4. maintain such level of availability of the Supplier System as is required to deliver its contractual obligations but, in any event, no less than 99.99% availability (excluding for these purposes scheduled downtime in accordance with Professional Practice), as measured on a monthly basis;

6A.3.5. report to SMRT as to the operation of the Supplier System (including promptly notifying SMRT of any events that could impact the operation of the Supplier System in a manner that could impact the delivery of the Goods and/or Services); and

6A.3.6. take such steps as are necessary in accordance with Professional Practice to prevent the introduction of viruses, or other harmful, or malicious code into the Supplier System or otherwise into SMRT's IT systems.

6A.4 Where required by SMRT, Supplier shall provide reasonable training and documentation to SMRT's personnel as to the operation of Supplier System as is necessary to facilitate the provision and receipt of the Goods and/or Services.

7. SMRT REMEDIES

7.1. If SMRT reasonably determines that there has been a failure by Supplier to supply the Goods and/or Services in accordance with this Contract (including any non-compliance with the Supplier's undertakings set out in clauses 3 (***Supply of Goods***) and/or 4 (***Supply of Services***)) then, whether or not it has accepted the Goods and/or Deliverables, SMRT may exercise any one or more of the following remedies at its sole discretion:

7.1.1. to terminate this Contract with immediate effect without compensation to the Supplier;

7.1.2. to accept or reject the applicable Goods and/or Deliverables (in whole or in part) and, where relevant, return the applicable Goods and/or Deliverables to Supplier at Supplier's own risk and expense;

7.1.3. to require Supplier to replace the rejected Goods and/or Deliverables and/or re-perform the relevant Services;

7.1.4. to refuse to accept any subsequent delivery of the Goods and/or Services and/or Deliverables which Supplier attempts to make;

7.1.5. to recover from Supplier any costs incurred by SMRT in obtaining substitute Goods and/or Deliverables and/or Services from a third party; and

7.1.6. to claim, where applicable, liquidated damages as set out in the Specific Terms and Conditions, or damages for any other costs, loss or expenses incurred by SMRT which are in any way attributable to Supplier's failure to carry out its obligations in accordance with this Contract.

7.2. SMRT's rights and remedies under this Contract are in addition to its rights and remedies implied by law.

8. PRICE AND PAYMENT

8.1. Subject to the receipt by SMRT of a valid invoice, SMRT shall pay any undisputed portion of the applicable Price for Goods and/or Services delivered in accordance with this Contract.

8.2. No extra charges shall be payable unless agreed in writing and signed by an authorised representative of SMRT. For the avoidance of doubt, the Price is inclusive of all costs and expenses of Supplier.

8.3. SMRT shall make payment less amounts it is required to withhold pursuant to Applicable Laws in relation to taxation.

8.4. SMRT may at any time, without limiting any of its other rights or remedies, set off any liability of Supplier to SMRT against any liability of SMRT to Supplier.

8.5. Any forecasts provided by SMRT are indicative and are non-binding unless expressly stated in writing to be binding.

9. INDEMNITY

9.1. Supplier shall indemnify and hold harmless SMRT, SMRT's affiliates, and their respective officers, directors, employees, subcontractors, customers, agents, successors and assigns ("**SMRT Indemnified Parties**") from and against all liabilities, costs, expenses, damages and losses and all other reasonable professional costs and expenses) suffered or incurred by an SMRT Indemnified Party as a result of or in connection with any claim made against an SMRT Indemnified Party:

9.1.1. for Supplier's breach of any warranties, representations or undertakings under this Contract;

9.1.2. for Supplier's breach of any confidentiality and/or personal data obligations under this Contract;

9.1.3. for actual or alleged infringement of a third party's rights arising out of or in connection with the supply or use of the Goods and/or Services;

9.1.4. for death, personal injury or damage to property arising out of or in connection with defects in Goods and/or Services; and

9.1.5. arising out of or in connection with the supply of the Goods and/or Services, to the extent that such claim arises out of the material breach or delay, gross negligence, wilful misconduct, or fraud in performance of this Contract by Supplier, its employees, agents and/or contractors.

10. LIMITATION OF LIABILITY

10.1. To the extent permitted by Applicable Laws, SMRT shall not be liable to Supplier for any: (a) special, indirect, incidental or consequential loss or damage of any nature whatsoever; or (b) loss of profits, loss of business, loss of contracts, loss of revenue, loss of anticipated savings or loss of goodwill, in connection with this Contract, whether in contract, tort, breach of statutory duty or otherwise.

10.2. To the extent permitted by Applicable Laws, the maximum aggregate liability of either Party to the other Party arising under or in connection with this Contract, whether in contract, tort (including negligence), breach of statutory duty or otherwise, shall not exceed an amount equal to the Price of this Contract.

10.3. Supplier shall hold insurance cover to an appropriate value to cover the liability assumed by it under this Contract. On request, Supplier will promptly provide SMRT with evidence of such insurances.

11. INTELLECTUAL PROPERTY

11.1. All Intellectual Property Rights owned by either Party prior to the date of this Contract or developed or created by either Party other than in the course of performing its obligations under this Contract ("**Background IPR**") will remain vested in each Party and shall not be assigned or (subject to clause 11.2) licensed under this Contract.

11.2. To the extent that any of the Goods and/or any of the Deliverables incorporate or embody Background IPR, Supplier hereby grants to SMRT a perpetual, irrevocable, royalty-free, non-transferable (save as permitted by this Contract), non-exclusive licence to use Supplier's Background IPR to facilitate and/or enable the use by SMRT of the Goods and/or the Deliverables, and unless otherwise agreed between Parties in writing, SMRT hereby grants to Supplier, for the duration and purpose of this Contract, a royalty-free, non-exclusive license to use SMRT's Background IPR to facilitate and/or enable the use by Supplier of the Goods and/or Deliverables.

11.3. Subject to clause 11.1, all Intellectual Property Rights in and to the Goods and the Deliverables ("**Foreground IPR**") will immediately vest in SMRT. Supplier hereby assigns with full title guarantee (by way of present assignment of present and future rights) such Foreground IPR to SMRT. Supplier shall use all reasonable endeavours to obtain waivers of all moral rights (and any similar rights in other jurisdictions) in and to the Goods and/or Deliverables (as applicable).

12. TERM AND TERMINATION

12.1. This Contract starts on the Start Date and shall expire at the end of the Term, subject to earlier termination in accordance with this Contract.

12.2. Without limiting its other rights or remedies, either party (the "**Non-Defaulting Party**") may terminate this Contract with immediate effect by giving written notice to the other party (the "**Defaulting Party**") if: (a) the Defaulting Party commits a material breach of this Contract and (if such a breach is remediable) fails to remedy it within thirty (30) days of receiving notice from the Non-Defaulting Party; or (b) if the Defaulting Party is Insolvent; or (c) if the Defaulting Party or any person employed by it is deemed by the Non-Defaulting Party to be guilty of an offence under the Prevention of Corruption Act 1960.

12.3. SMRT shall be entitled to terminate this Contract in its entirety for convenience without any liability by providing not less than thirty (30) days' prior written notice to Supplier.

12.4. Termination of this Contract, in whole or in part, shall not affect any of the Parties' rights and remedies that have accrued as at termination, including the right to claim damages in respect of any breach of this Contract which existed at or before the date of termination. Any other clauses of this Contract that expressly or by implication are intended to come into or continue in force on or after termination shall remain in full force and effect.

13. INSPECTION & AUDIT

Supplier shall:

13.1. maintain all books, accounts, records and quality control information relating to its performance of this Contract or otherwise required by Applicable Laws ("**Records**") and shall ensure that these are at all times comprehensive and accurate;

13.2. retain and properly store the Records during the Term and for at least five years after termination or expiry; and

13.3. at all times during the Term and for at least five years after termination or expiry, allow SMRT and/or its representatives to enter any Supplier premises upon no less than 14 days' prior written notice to access, inspect, audit and copy the Records for the sole purpose of assessing Supplier's compliance with the requirements of this Contract. Any audit must be conducted during Supplier's ordinary business hours. SMRT shall use all reasonable endeavours to minimise disruption to Supplier's business in connection with any such audit.

14. CONFIDENTIALITY AND PERSONAL DATA

14.1. Save for disclosure to (a) employees, officers, representatives or advisers who need to know such information for the purposes of exercising the 'Party's rights or carrying out its obligations under or in connection with this Contract, or (b) a court of competent jurisdiction or any governmental or regulatory authority (as may be required by law), each Party undertakes that it shall retain in confidence and not use or disclose any confidential information concerning the business, affairs, customers, clients or suppliers of the other Party without the prior written consent of the other Party.

14.2. Schedule 3 (***Transfer of SMRT Data***) shall apply in respect of any Personal Data that is disclosed by SMRT to the Supplier ("**SMRT Data**") and received by the Supplier via or from Singapore under this Contract.

14.3. Regarding the supply of the Goods and/or Services, this Contract constitutes the entire agreement of the Parties and supersedes all prior agreements, understandings and negotiations.

14A. CYBERSECURITY

14A.1. Schedule 4 shall apply in respect of any Goods and/or Services for any computer or computer system. "Computer" and "computer system" shall have the meanings ascribed to them in Schedule 4.

15. GENERAL

15.1. No modification of the terms of this Contract is valid unless in writing and signed by both Parties.

15.2. SMRT may, at any time, novate, assign, transfer or sub-license the whole or any part of its rights under this Contract by giving written notice to the Supplier. Supplier may not novate, assign, transfer or sub-license the whole or any part of its rights nor subcontract any or all of its obligations under this Contract without prior written approval from SMRT, such approval shall not be unreasonably withheld.

15.3. Notices shall be in writing and shall be delivered by hand or by post to the address in this Contract.

15.4. This Contract (and any and all disputes in connection with this Contract) shall be governed by and interpreted in accordance with the laws of Singapore. Any and all disputes arising out of or in connection with this Contract will be finally settled by the Singapore courts.

SCHEDULE 1

A. Goods and/or Services

[Goods:

- Description of Goods: [FULL DESCRIPTION]
- Specification of Goods: [TECHNICAL, DESIGN, PERFORMANCE, BUSINESS OR ANY REGULATORY REQUIREMENTS]
- [Any other KPIs]

[Services:

- Description of Services: [FULL SERVICES SPECIFICATION]
- Key Deliverables: [SPECIFIC DELIVERABLES]
- [Any other KPIs]

B. Price

[Goods:

- Price applicable to Goods: [FULL DESCRIPTION OF UNIT PRICE AND TOTAL PRICE]
- Calculation of amount payable for the Goods: [CALCULATION, INCLUDING ANY PERFORMANCE RELATED PAY]
- Payment due: [DATE]]

[Services:

- Price applicable to Services: [FULL DESCRIPTION OF UNIT PRICE AND TOTAL PRICE]
- Calculation of amount payable for the Services: [CALCULATION, INCLUDING ANY PERFORMANCE RELATED PAY / RATE CARD]
- Payment due: [DATE]]

C. [Tender Specifications, Response and Clarifications] [*if applicable]*

D. [Supplier Terms & Conditions] [*if applicable*]

SCHEDULE 2

MANDATORY POLICIES

1. Safety and Security Policy

A. **Supplier items**. Supplier shall be solely responsible for providing all required equipment including, where necessary, personal protective equipment in accordance with SMRT standards.

B. **Working days and hours**. Supplier shall comply with Applicable Laws, including Ministry of Manpower regulations, concerning the working hours of Supplier Personnel and SMRT shall approve the proposed working days and hours in advance of the Start Date.

C. **Supplier Supervisors**. If required by SMRT, all Supplier Supervisors must successfully complete the SMRT Safety Orientation Course, the costs of which shall be borne solely by Supplier.

D. **Security**. Supplier shall ensure that Supplier Personnel observe and comply with all SMRT policies, practices and procedures relating to security (including but not limited to cybersecurity).

Suppliers who are required to use, operate and manage Critical Information Infrastructure (as defined in the Cybersecurity Act 2018) under Contract shall ensure that each of the Supplier's personnel completes an e-learning course on Cybersecurity (or any other courses instructed by SMRT), the costs of which shall be borne solely by the Supplier.

Supplier shall, upon request, provide SMRT with particulars of all Supplier Personnel, including but not limited to name, address, identity card or work permit numbers, citizenship, date of birth and/or education level.

If the Location is deemed by SMRT as restricted or sensitive or if the Term for the performance of the Services exceeds thirty (30) days, Supplier must submit the information required to SMRT for security screening.

Supplier shall ensure that all Supplier Personnel are legally entitled to work in Singapore and shall therefore be solely responsible for arranging, at its sole cost, any appropriate work pass. All passes must be returned to SMRT on the resignation, termination or expiry of the appointment of any Supplier Personnel.

Supplier shall comply with the SMRT security standing order and access control procedures.

Appropriate security passes must be worn by Supplier Personnel at all times.

E. **Safety**. Supplier shall ensure that Supplier Personnel observe and comply with all SMRT manuals (including but not limited to SMRT Work Safety Manual), policies, practices and procedures relating to safety. This obligation includes taking safety precautions to eliminate or reduce danger to Supplier Personnel, SMRT staff and the general public, whilst minimising obstruction and inconvenience.

SMRT reserves the right to issue a "Stop Work Order" should any critical safety lapse or breach be identified. Supplier must then implement appropriate corrective measures and seek SMRT approval before any Supplier Personnel recommences any work. Supplier shall not seek compensation for any increase in the costs of performing the Services following the issuance of any "Stop Work Order".

Supplier shall be fully responsible for their Method Statement (or Safe Work Procedure / Instruction) and Risk Assessment; and ensure their contents comply with the Workplace Safety & Health Act and applicable regulations. SMRT shall not be held liable for any shortcomings in these documents.

F. **Clearing and cleaning on completion of the Services**. At the end of each day during the Term, Supplier must ensure that Supplier Personnel removes all rubbish and that no materials are left behind which could violate the regulatory requirements by the National Environment Agency (NEA) or give cause to complaints from members of the public.

G. **Public safety**. Supplier shall look after the interest of traffic and public safety and safety of Supplier Personnel at all times.

H. **Non-compliance with Workplace Safety and Health Act and applicable regulations**. If Supplier is found by SMRT to be in breach of any Applicable Laws, SMRT has the right to terminate this Contract, without prejudice to its other rights.

I. **Qualification of Supplier.** Supplier shall ensure that it is certified to either bizSAFE Level 3 or higher by the Workplace Safety and Health Council, or to equivalent recognized international standards (for example, ISO 45001).

2. Data and Privacy Policy

Updated from time to time and found at https://www.smrt.com.sg/smrt-data-protection-policy/

3. Suppliers' Commitment on Sustainability, Transparency, Accountability and Integrity in Business

Supplier shall:

a. Affirm its commitment to ethical and sustainable procurement;
b. Be on the guard against slavery within the global supply chain;
c. Have zero tolerance for corruption and bribery; and
d. Ensure that their actions do not harm the environment.

SCHEDULE 3

TRANSFER OF SMRT DATA

1. The Supplier acknowledges and agrees that in relation to any SMRT Data received via or from Singapore, such SMRT Data may only be transferred to, and collected, used and disclosed by the Supplier within the territories identified below ("**Territory**"):

   [INSERT COUNTRIES]

2. The Supplier shall provide a standard of protection in relation to such SMRT Data that is comparable to the protection applicable thereto under the PDPA and any requirements set out in any advisory or other guidelines issued from time to time by the Personal Data Protection Commission of Singapore, including without limitation:

   2.1. **Purpose**: The Supplier shall not use or disclose SMRT Data for any purpose other than as specified in this Contract.

   2.2. **Use and disclosure**: The Supplier shall only use and disclose SMRT Data in a manner and to the extent permitted in this Contract and observe all limitations as to such use or disclosure as SMRT may notify the Supplier from time to time.

   2.3. **Accuracy**: The Supplier shall make a reasonable effort to ensure that SMRT Data is accurate and complete, if SMRT Data is likely to be (i) used by the Supplier to make a decision that affects the Individual to whom SMRT Data relates; or (ii) (if permitted under this Contract) disclosed by the Supplier to another organisation.

   2.4. **Protection**: The Supplier shall protect SMRT Data in its possession or under its control by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and (ii) the loss of any storage medium or device on which SMRT Data is stored.

   2.5. **Retention**: The Supplier shall cease to retain its documents containing SMRT Data or remove the means by which SMRT Data can be associated with particular Individuals, as soon as it is reasonable to assume that (i) the specified purposes are no longer being served by retention of SMRT Data; and (ii) retention is no longer necessary for legal or business purposes.

   2.6. **Access**: The Supplier shall ensure that upon request by an individual, the Supplier shall, as soon as reasonably possible, provide the individual with (i) the personal data about the individual that is in the possession or under the control of the Supplier; and (ii) information about the ways in which that personal data has been or may have been used or disclosed by the Supplier within a year before the date of the individual's request. Where the Supplier refuses such a request, the Supplier shall preserve a complete and accurate copy of the Personal Data concerned for the period required under the PDPA.

   2.7. **Correction:** Unless the Supplier is satisfied on reasonable grounds that a correction should not be made, the Supplier shall, upon receiving a request from an individual to correct an error or omission in the personal data about the individual that is in the possession or under the control of the Supplier, (i) correct the personal data as soon as practicable; and (ii) send the corrected personal data to every other organisation to which the personal data was disclosed by the Supplier within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

   2.8. **Policies/Accountability:** The Supplier shall ensure that its employees, agents and sub-contractors who may receive or have access to any SMRT Data are aware of the obligations specified in this Schedule 3, any policies prescribed by SMRT in relation to SMRT Data and SMRT's privacy policies and agree to abide by the same.

3. The Supplier hereby agrees and undertakes that:

   3.1. notwithstanding anything else in this Contract, in respect of all SMRT Data, the Supplier shall keep all SMRT Data confidential, and not make further disclosures of SMRT Data (whether to an entity of the SMRT or otherwise) except

(i) in accordance with this Contract; or (ii) in accordance with a valid court order, to the extent legally required in response to a request from a law enforcement agency or in order to comply with applicable laws, in which case the Supplier shall immediately notify SMRT when it becomes aware that a disclosure of SMRT Data may be required in order to comply with applicable law;

3.2. the Supplier shall comply with all laws and regulations, as may be applicable to the SMRT Data and any requirements arising under any such relevant laws as SMRT may be required to comply with, or may become obliged under any such law to require the Supplier's compliance with, as SMRT may from time to time notify the Supplier in writing;

3.3. the Supplier shall, in respect of any SMRT Data collected, used, disclosed, accessed and/or processed by the Supplier in connection with this Contract, comply with any requests, directions or guidelines which SMRT may provide to the Supplier from time to time, including but not limited to SMRT's Privacy Statement, which is accessible at https://www.smrt.com.sg/smrt-data-protection-policy/ and which may be updated from time to time;

3.4. the Supplier shall provide SMRT with such assistance as they may reasonably require in meeting their own obligations under the PDPA;

3.5. in respect of all IT, software and hardware systems owned, leased, licensed, used and/or provided by the Supplier in connection with this Contract, the Supplier shall comply with any and all security requirements, directives, guidelines and/or standards that may be prescribed by SMRT in its sole and absolute discretion from time to time; and

3.6. the security and confidentiality obligations in this Contract and/or this Schedule 3 shall apply for so long as the Supplier retains any SMRT Data, and notwithstanding any termination of this Contract.

4. The Supplier agrees and undertakes to SMRT that, to the maximum extent not prohibited by applicable law, the Supplier shall at its own expense immediately notify SMRT (and in any event no later than 24 hours following the occurrence of any of the following events) of:

4.1. any complaint by, or request received from: (i) any Individual in relation to his/her Personal Data; or (ii) any relevant authority (including without limitation any authority or agency which has jurisdiction over SMRT) ("**Relevant Authority**") in relation to Personal Data, including without limitation any access, correction, data portability or similar requests;

4.2. any notification and/or commencement of any investigation by any Relevant Authority in relation to any Data Incident. "**Data Incident**" means any incident or circumstances which may, has/have resulted in, and/or which may reasonably give rise to any suspicion, in respect of Personal Data in each case whether transmitted, collected, used, disclosed, stored and/or otherwise processed, of: (i) destruction; (ii) loss; (iii) alteration; (iv) unauthorised collection, use, disclosure, access, processing, copying, modification or disposal; and/or (v) the loss of any storage medium or device on which such Personal Data is stored;

4.3. any circumstances which may suggest or indicate the occurrence of any Data Incident, including without limitation any Data Incident which is: (i) likely to result in significant harm or impact to individuals to whom the information relates; (ii) of a significant scale; and/or (iii) involving Personal Data of 500 or more individuals;

4.4. any claim (including without limitation any action, application, demand, proceeding, threat or any other analogous claims) (each a "**Claim**"), allegation, undertaking process, expedited decision, or litigation in connection with any Data Incident; and/or

4.5. the Supplier becoming aware of, learns of or suspects: (i) any collection, use or disclosure of any Personal Data collected in connection with this Contract otherwise than as permitted under this Contract or any misuse of any such Personal Data; (ii) any security breach in connection with this Contract that could compromise the security or integrity of such Personal Data or otherwise adversely affect SMRT or expose it to any Claim; and/or (iii) any Personal Data collected in connection with this Contract may have been or is at risk of having been disclosed to or obtained by any unauthorised person.

5. For the purposes of this Schedule 3, a Data Incident shall be deemed to result in significant harm to an Individual if the Data Incident relates to any Personal Data or classes of Personal Data relating to any Individual so specified in the

Personal Data Protection (Notification of Data Breaches) Regulations 2021 of Singapore

6. In the event that the Supplier notifies SMRT of any event referred to in Clauses 4.1 – 4.5 above (each a "**Relevant Event**"), the Supplier shall in each case:

   6.1. provide SMRT all information and assistance: (i) as SMRT may request in relation thereto, including without limitation for SMRT to verify the nature and veracity of the Relevant Event; (ii) as may be required under applicable law (e.g. PDPA); and (iii) in relation as the case may be to the investigation and remedy of any breach of security and any Claim or litigation with respect to this unauthorised access, use or disclosure of Personal Data;

   6.2. comply with SMRT's directions and all reporting and notification requirements under applicable law in connection therewith;

   6.3. adhere to and implement the steps set out in any incident response plan as may be amended or otherwise prescribed by SMRT from time to time;

   6.4. not, without SMRT's prior written consent, make any report(s) to any Relevant Authority in connection with the Relevant Event (unless required under applicable law in which case the Supplier shall notify SMRT without undue delay of any such requirement). Without prejudice to the generality of the foregoing, the Supplier shall provide to SMRT a copy of any report(s) submitted to the Relevant Authority by the Supplier; and

   6.5. upon notice by SMRT, provide SMRT and SMRT's employees, representatives, agents and officers unrestricted access to audit, inspect and obtain information relating to the Supplier's: (i) systems (including without limitation information systems and/or security management systems) and/or data; and (ii) books, records and documentation (including without limitation information stored in computerised form), to the extent such systems, books, records, and/or documentation (as the case may be) relate to the Relevant Event, and permit SMRT and SMRT's employees, representatives, agents and officers to make copies thereof. The Supplier shall provide full cooperation and reasonable assistance to SMRT for the completion of any such access, audit and/or inspection.

7. The Supplier may only export SMRT Data outside the Territory upon the written consent of SMRT and not otherwise. Where SMRT has provided such written consent, then unless otherwise agreed in writing, and without prejudice to the generality of the foregoing obligations, the Supplier shall ensure and procure that the overseas recipient of such SMRT Data shall provide a standard of protection in relation to SMRT Data that is comparable to the protection applicable thereto under the PDPA and any requirements set out in any advisory or other guidelines issued from time to time by the Personal Data Protection Commission, including, without limitation, the obligations set out in this Schedule 3.

8. The Supplier shall fully defend, indemnify and hold harmless SMRT and its related corporations or associated companies as well as their respective employees, representatives, agents and officers (collectively, **'Indemnitees'**) from and against any claim, action, demand or complaint, as well as all liabilities, judgments, penalties, compounds, losses, costs, damages and expenses which Indemnitees may suffer in connection with any breach of this Schedule 3, and any failure to comply with any data protection or privacy laws in any relevant jurisdictions, and whether arising on account of the actions of the Supplier, its employees, representatives or agents or otherwise howsoever. This Schedule 3 shall survive the termination or expiry of this Contract, howsoever caused.

9. For the purposes of this Schedule 3, any capitalised terms used in this Schedule 3 which are not defined herein but are defined in the PDPA shall bear the same meaning as set forth in the PDPA.

SCHEDULE 4

CYBERSECURITY

This Schedule 4 sets out the additional terms and conditions that apply to the Supplier for the supply of the Goods and/or Services as referenced in the applicable Order and/or Schedule 1 of this Contract, and shall have effect and be construed as an integral part of, and shall be deemed to be incorporated into this Contract.

1. DEFINITIONS AND INTERPRETATION

1.1. In this Schedule 4, the following words and expressions shall have the following meanings unless the context otherwise requires:

"**Applicable Standards**"	has the meaning ascribed to it in Annex 1 to this Schedule;
"**CMA**"	means the Computer Misuse Act 1993 of Singapore, including any subsidiary legislation, regulations and any codes of practice, standards of performance, advisories, guidelines, frameworks, or written directions issued thereunder, in each case as amended, consolidated, re-enacted or replaced from time to time;
"**computer**"	has the meaning ascribed to it in the Cybersecurity Act;
"**computer system**"	has the meaning ascribed to it in the Cybersecurity Act;
"**critical information infrastructure**" or "**CII**"	has the meaning ascribed to it in the Cybersecurity Act / means any provider-owned critical information infrastructure and third-party-owned critical information infrastructure;
"**cybersecurity**"	has the meaning ascribed to it in the Cybersecurity Act;
"**Cybersecurity Act**"	means the Cybersecurity Act 2018 of Singapore, including any subsidiary legislation, regulations and any codes of practice, standards of performance, advisories, guidelines, frameworks, or written directions issued thereunder, in each case as amended, consolidated, re-enacted or replaced from time to time;
"**Cybersecurity Event**"	means an observable occurrence of an activity in or through a computer or computer system, that may affect the cybersecurity of that or another computer or computer system, and includes a cybersecurity incident, cybersecurity threat or cybersecurity vulnerability;
"**Cybersecurity Incident**"	has the meaning ascribed to it in the Cybersecurity Act, and includes without limitation, in connection with the Goods and/or Services, and any Interconnected System therewith, the following:

(a) any unauthorised hacking to gain unauthorised access to or control thereof;

(b) any installation or execution of unauthorised software or computer code, of a malicious nature thereof;

(c) any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the Goods

and/or Services (or any Interconnected System therewith) and an authorised user of Goods and/or Services (or any Interconnected System therewith), as the case may be; and/or

(d) any denial-of-service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the Goods and/or Services (or any Interconnected System therewith);

"**Cybersecurity risk**"	has the meaning ascribed to it in Section 6 of the Cybersecurity (Critical Information Infrastructure) Regulations of the Cybersecurity Act;
"**cybersecurity risk profile**"	in relation to the Goods and/or Services, means the profile that outlines the Goods', Services' and/or any Interconnected System's (as the case may be) known cybersecurity risks, policy constraints and regulatory obligations for the determination of level risk mitigating controls required;
"**cybersecurity threat**"	has the meaning ascribed to it in the Cybersecurity Act;
"**cybersecurity vulnerability**"	has the meaning ascribed to it in the Cybersecurity Act;
"**interception**"	in relation to a communication to or from the Goods and/or Services (or any Interconnected System therewith), includes access to, or recording of the communication and/or acquiring the substance, meaning or purport of that communication;
"**Interconnected System**"	(a) means any computer or computer system under the owner's control that is interconnected with or that communicates with a system;
"**provider-owned critical information infrastructure**"	has the meaning ascribed to it in the Cybersecurity Act;
"**Rectification**"	has the meaning ascribed to it in Clause 6.3 of Annex 2;
"**Rectification Plan**"	has the meaning ascribed to it in Clause 6.1 of Annex 2;
"**Relevant Authority**"	includes any authority which has jurisdiction over cybersecurity matters in relation to SMRT or any of its systems, the Goods and/or Services, and any Interconnected Systems therewith, including without limitation: (a) the Minister as referenced in the Cybersecurity Act; (b) the Land Transport Authority of Singapore; and (c) any authority (and its authorised officers, delegates, and/or agents) conferred powers to administer or otherwise exercise any power, duty or function under Applicable Standards, including without limitation: (i) the Ministry of Communication and Information of Singapore; (ii) the Cyber Security Agency of Singapore; (iii) the Commissioner of Cybersecurity, Deputy

	Commissioner of Cybersecurity, Assistant Commissioner, cybersecurity officer, incident response officer, and/or assistant licensing officer appointed under and pursuant to the Cybersecurity Act; and/or (iv) a police officer, and/or an authorised person conferred powers of investigation under Section 40 of the Criminal Procedure Code 2010 of Singapore or any other written law;
"**Relevant Cybersecurity Event**"	has the meaning ascribed to it in Clause 3.3 of this Schedule 4; and
"**third-party-owned critical information infrastructure**"	has the meaning ascribed to it in the Cybersecurity Act.

1.2. The Annexes shall form part of this Schedule and have the same force and effect as if expressly set out in the body of this Schedule.

1.3. Where the provision number is stated without a description of any document, then it refers to the provision so numbered in the document where the reference appears.

1.4. Capitalised expressions used without definition in this Schedule shall have the meanings respectively ascribed to them in the main Contract and/or any other Schedules.

1.5. Unless otherwise expressly stated, the Supplier's obligations set out under this Schedule shall be cumulative, in addition, and without prejudice to the Supplier's other obligations under this Contract.

1.6. Unless otherwise expressly stated herein, the Supplier shall bear all costs and expenses, including legal and other consultant fees, arising in connection with performing or ensuring the due performance of each of its obligations under this Schedule, and/or with any other matters referenced therein.

2. SCOPE OF APPLICATION

2.1. The Goods and/or Services supplied by the Supplier under this Contract is hereby designated, as determined by SMRT in its sole discretion, as Category A/B/C for the purposes of this Contract. The Supplier shall ensure and procure that, in its provision and delivery of the Goods and/or Services, the terms and conditions of this Contract applicable to such categorisation of the Goods and/or Services shall be met.

2.2. SMRT may, in its sole discretion, revise the categorisation of the Goods and/or Services at any time by notifying the Supplier in writing. Such reclassification may occur, including but not limited to, where there are changes in the nature of the Goods and/or Services provided, modifications to operational or cybersecurity requirements, regulatory updates, changes in the Supplier's scope of work, and/or any other circumstances that, in SMRT's sole determination, warrant a reclassification.

3. SUPPLIER OBLIGATIONS

3.1. The Supplier hereby undertakes in connection with the supply and provision of the Goods and Services under this Contract, regardless of whether the Goods and/or Services have been designated as Category A, B or C:

(a) to ensure and procure that the Goods and/or Services supplied shall meet the requirements set out in the Applicable Standards;

(b) to ensure and procure the implementation of robust security and other protocols as well as performance, service-level and quality standards appropriate to the supply of the Goods and/or Services. Without prejudice to the generality of the foregoing, the Supplier shall establish and maintain safety and facility procedures, data security policies, procedures and such administrative, organisational, physical, procedural and technical

measures to reduce and mitigate the impact of any cybersecurity risks in connection with the supply of the Goods and/or Services, and any Interconnected Systems therewith, in accordance with the requirements as provided in this Contract and the Applicable Standards, and shall, upon SMRT's request, provide to SMRT a copy of the certification or documentation (where applicable) of each standard or accreditation that has been met by the Supplier and thereafter provide the same with respect to the renewal or re-certification of each such standard or accreditation (as the case may be) annually and upon SMRT's request any other information and/or documentation pertaining to the Supplier's security measures;

(c) to supply the Goods and/or Services with qualified personnel in a good workmanlike manner consistent with the Applicable Standards and prevailing best industry standards and practices, including without limitation standards relating to cybersecurity and data integrity, and ensure the use of all necessary equipment, computer capacity, software, and trained personnel with appropriate security clearances and qualifications, to properly supply the Goods and/or Services to the standards aforementioned;

(d) to ensure and procure that the Supplier's personnel, the Goods and/or Services provided by the Supplier (and/or the Supplier's personnel), and any Interconnected System therewith, shall not breach and/or cause SMRT and/or any SMRT's Affiliates (and/or their respective personnel) to be in breach of the Applicable Standards, and to ensure, including by taking all necessary steps, measures, and doing all acts and things necessary, that SMRT and/or any SMRT's Affiliates (and/or their respective personnel) meet and are in a position to meet any duty or obligation under the Applicable Standards in relation to its systems and any Interconnected Systems therewith;

(e) after diligently assessing the requirements of the Applicable Standards, to ensure that the cybersecurity features and measures adopted in respect of the Goods and/or Services, and any Interconnected System therewith, are adequate and appropriate for protection against a Cybersecurity Event and Cybersecurity Incident, and where any part of the Goods and/or Services, and any Interconnected System therewith, involves the transmission of data over a network, also ensuring, without limitation, protection against all unlawful cyber activity in relation to such data, and to ensure that the aforesaid features and measures meet a level of cybersecurity appropriate to the risks presented by the nature of the Goods and/or Services, any Interconnected System therewith, (as the case may be) to be protected; and

(f) to ensure and procure full compliance by its personnel of all physical, technical, administrative and other security and integrity procedures that SMRT may from time to time prescribe, including restricting access only to authorised personnel and activities as well as authorised process interfaces and devices. The Supplier shall also ensure that all such personnel are fully aware of such security and integrity procedures. The Supplier further agrees that SMRT may restrict access to its systems and/or any Interconnected Systems therewith (or parts thereof) and require that the Goods and/or Services shall be provided and/or performed on-site, where applicable, and under the supervision of an appropriate SMRT personnel.

3.2. In addition to the Supplier's obligations under the Applicable Standards, the Supplier shall, to the maximum extent not prohibited by Applicable Law, immediately notify SMRT in writing or through such other method as may be instructed or directed by SMRT:

(a) where the Supplier becomes aware of any event or circumstances which discloses a breach or potential breach:

(i) of any of its obligations under this Contract and/or any Applicable Standards; and/or

(ii) which is reportable (whether by SMRT or any other party) to any Relevant Authority pursuant to any Applicable Standards;

(b) of any notification and/or commencement of any investigation by any Relevant Authority:

(i) in connection with the Applicable Standards; and

(ii) in relation to the Goods and/or Services; and

(c) of any circumstances which may suggest or indicate the actual, potential, or suspected physical security breach, Cybersecurity Event or Cybersecurity Incident affecting any Goods and/or Services, any Interconnected System therewith, or any other computer or computer system as may be determined by SMRT in its sole and absolute discretion;

3.3. In the event that the Supplier shall notify SMRT pursuant to any of Clauses (a) to 1.1(c) above (each a "**Relevant Cybersecurity Event**"), the Supplier shall in each case of a Relevant Cybersecurity Event:

(a) provide SMRT all information and assistance:

(i) as SMRT may request in relation thereto, including without limitation:

(1) for the Supplier to verify the nature and veracity of the Relevant Cybersecurity Event; and/or

(2) procedures for the preservation of evidence prior to the initiation of recovery process, including but not limited to log acquisition, seizure of evidence, acquisition computers or other equipment, placement of additional passive monitoring equipment to support investigation; and

(3) as may be required by Applicable Standards, in which case the Supplier shall comply with SMRT's directions and all reporting and notification requirements under Applicable Standards in connection therewith;

(b) without prejudice to the generality of the foregoing, provide SMRT (or such persons as SMRT may stipulate) in writing of all known details of the Relevant Cybersecurity Event and a root-cause and impact analysis in such format and with such details as SMRT may require, including without limitation:

(i) the Goods and/or Services, any Interconnected Systems or any other computer systems that were affected or may be affected by the Relevant Cybersecurity Event;

(ii) the extent of impact of such Relevant Cybersecurity Event on individual(s) and/or any computer systems, including a description of the nature of the Relevant Cybersecurity Event (including the categories and approximate number of affected parties and computer systems, and when and how the Relevant Cybersecurity Event occurred), the resulting effect that has been observed in respect of the affected Goods and/or Services, any Interconnected Systems therewith or any other computer systems and how they have been affected, as well as records concerned;

(iii) the cause(s) and suspected cause(s) of the Relevant Cybersecurity Event;

(iv) the measures and processes which the Supplier had put in place at the time of the Relevant Cybersecurity Event;

(v) a description of the measures taken or proposed to be taken to address the Relevant Cybersecurity Event (including, where appropriate, remedial measures and/or measures to mitigate any possible adverse effects); and

(vi) the name and contact details of the Supplier's designated representative who shall be SMRT's point of contact in relation to the Relevant Cybersecurity Event;

(c) mitigate any harmful effects thereof, including (if appropriate) isolating the Goods and/or Services, any Interconnected System therewith or any other computer system or blocking cyber access points, but if this will affect the performance or specifications of the Goods and/or Services, the Supplier shall first obtain SMRT's consent;

(d) assist SMRT (or such persons as SMRT may designate) in remediating or mitigating any actual or potential damage from the incident, and further provide SMRT with regular status updates (including without limitation actions, if any, taken by the Supplier to resolve the Relevant Cybersecurity Event) at mutually agreed intervals or times until the Relevant Cybersecurity Event is fully resolved and the Goods and/or Services are restored to full functionality;

(e) cooperate with SMRT's and any Relevant Authority's investigation of the incident;

(f) not disclose to third parties any information about the Relevant Cybersecurity Event without prior written permission of SMRT, unless required under Applicable Standards; and

(g) assist and cooperate with SMRT (or such persons as SMRT may stipulate) with notifying the incident to any Relevant Authority in accordance with Applicable Standards.

4. FURTHER OBLIGATIONS

4.1. If the supply of Goods and/or Services has been designated as Category B, then the Supplier shall additionally comply with the obligations set out in Part I of Annex 2.

4.2. If the supply of Goods and/or Services has been designated as Category A, then the Supplier shall additionally comply with the obligations set out in Parts I and II of Annex 2.

5. REPRESENTATIONS AND WARRANTIES

5.1. The Supplier hereby represents and warrants to SMRT that:

(a) it shall perform its obligations under this Contract in accordance with all Applicable Standards;

(b) the Goods and/or Services, and any Interconnected System therewith, and any part thereof, will conform to the applicable regulations and statutes of any competent authority and laws of Singapore (including without limitation Applicable Standards);

(c) any information or data (including, without limitation to those provided in the documentation, any recommendations, system or network configurations and/or design, technical, operational and functional specifications, implementation and user guides, blueprints) and any Supplier System provided by the Supplier to SMRT, shall:

(i) be correct and sufficient to enable the use of the Goods and/or Services, and any Interconnected System therewith, by SMRT for all purposes contemplated under this Contract;

(ii) be a full and accurate description of the operation, features, functionality and performance of the Goods and/or Services, and any Interconnected System therewith; and

(iii) comply with best industry practice, including without limitation in relation to Applicable Standards; and

(d) all Supplier Personnel and those of its subcontractors or agents deployed to perform the Supplier's obligations are suitably qualified and competent to carry out the tasks required of it, and possess such qualifications and certifications as SMRT may specify.

6. LIABILITY AND INDEMNITY

6.1. Notwithstanding any other provision of this Contract, to the maximum extent permitted under Applicable Law, in no event shall SMRT (and/or its affiliates, and their respective directors, partners, permitted assigns or representatives)

be liable to the Supplier or any other party for any Losses, fines, penalties or other levies or charges imposed by any governmental or regulatory authority, even if informed of the possibility thereof, arising from or in connection with:

(a) the instructions, directions, orders, requests, and/or guidelines of a Relevant Authority;

(b) any Relevant Authority accessing, inspecting, testing, examining, taking, removing, detaining, making copies of, taking extracts from, and/or seizing any premises, information, book, data, computer output, record, document, apparatus, equipment, computer, computer system (e.g., the System), instrument, material, or article;

(c) any Relevant Authority:

(i) giving evidence in respect of, or producing any document containing, any information which has been obtained from: (1) any Goods and/or Services, and any Interconnected Systems therewith; and/or (2) the Supplier; and/or

(ii) disclosing any information which is contained in: (1) any Goods and/or Services, and any Interconnected Systems therewith; and/or (2) Confidential Information;

(d) the Supplier's (and/or its member's, officer's, employee's, subcontractor's or agent's) act, omission, default or failure to perform its obligations; and

(e) any Relevant Cybersecurity Event.

6.2. The Supplier shall have a duty to use at least commercially reasonable efforts to mitigate any liability suffered by SMRT in connection with this Schedule, including without limitation to stop security breaches and reduce data loss.

6.3. Notwithstanding anything in this Contract, the Supplier hereby unconditionally and irrevocably undertakes to indemnify, defend and hold harmless each SMRT Indemnified Party from and against any and all Losses which may be sustained, instituted, made or alleged against (including without limitation any Claim or prospective Claim in connection therewith), or suffered or incurred by any SMRT Indemnified Party, and which arise (whether directly or indirectly) out of or in connection with any act or omission by the Supplier, its agents and/or subcontractors of this Schedule.

ANNEX 1

APPLICABLE STANDARDS

In this Contract, "**Applicable Standards**" shall include:

(a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other instrument addressing cybersecurity, including any subsidiary legislation, regulations and any codes of practice, standards of performance, advisories, guidelines, frameworks, or written directions issued thereunder, including without limitation the CMA, the Cybersecurity Act, the Rapid Transit Systems Act 1995, in each case as amended, consolidated, re-enacted or replaced from time to time;

(b) all advisories, policies, guidelines, circulars or notices relating to cybersecurity and data protection as may be issued, amended, consolidated, re-enacted or replaced by a Relevant Authority from time to time, including, without limitation, advisory guidelines published by the Cyber Security Agency of Singapore (including such guidelines jointly published with the Personal Data Protection Commission of Singapore), and the publications available at https://www.csa.gov.sg/legislation/supplementary-references (e.g. the Guide to Conducting Cybersecurity Risk Assessment for CII and the Guidelines for Auditing Critical Information Infrastructure);

(c) any policies or guidelines provided by SMRT from time to time relating to the cybersecurity of the System and Interconnected Systems, including without limitation, the SMRT Cybersecurity Policy, SMRT Cybersecurity Code of Conduct Policy and SMRT Cybersecurity Incident Response Policy;

(d) without prejudice to the generality of the foregoing, in respect of the provision of the Goods and/or Services, measures set out in the SMRT Application Security Standard and SMRT Cloud Security Operating Standards;

(e) such other physical, administrative, procedural and information and communications technology measures, as well as technical and organisational cybersecurity measures as are up-to-date and commensurate with the cybersecurity risk profile associated with the supply of the Goods and/or Services, including without limitation:

  (i) "privacy by design" and "security by design" principles (including without limitation any principles as may be set out in frameworks such as the Security by Design Framework issued by the Cybersecurity Agency of Singapore accessible at https://www.csa.gov.sg/legislation/supplementary-references and other publication locations from time to time made available by the Relevant Authority); and

  (ii) meeting or exceeding the best available security practices and systems which are no less rigorous than industry standards for security management.

ANNEX 2

FURTHER OBLIGATIONS

The Supplier shall ensure and procure its compliance with the terms set forth in this Annex as follows:

(a) in relation to the supply of Goods and/or Services been designated as Category B, Part I of Annex 2;

(b) in relation to the supply of Goods and/or Services been designated as Category A, Parts I & II of Annex 2;

Part I

1. **INFORMATION**

1.1. The Supplier agrees and undertakes to provide SMRT (and/or such persons as SMRT may designate), upon request by SMRT, detailed and comprehensive specifications and information, in such format and manner as SMRT may specify, relating to

1.2.

(a) the design, configuration and security of the Goods and/or Services, any Interconnected System therewith, or any other computer or computer system, that is interconnected with or that communicates with SMRT's systems and any Interconnected System therewith; and

(b) the operation of the Goods and/or Services, any Interconnected System therewith, or any other computer or computer system, that is interconnected with or that communicates with SMRT's systems and any Interconnected System therewith.

Part II

2. **INFORMATION AND NOTIFICATION**

Furnishing of information

2.1. Without prejudice to the generality of Clause (b), the Supplier agrees and undertakes to provide SMRT (and/or such persons as SMRT may designate), upon request by SMRT, detailed and comprehensive specifications and information, in such format and manner as SMRT may specify, relating to:

(a) the functions of the Goods and/or Services, and any Interconnected System therewith, and any technical or implementation details relating thereto;

(b) the design, configuration and security of the Goods and/or Services, and any Interconnected System therewith, including software and hardware configurations and parameters;

(c) the operation of the Goods and/or Services, and any Interconnected System therewith (including, if any, the identity of any outsourced service provider supporting the Goods and/or Services, and any Interconnected System therewith, and the nature of the outsourced service), and any access or security logs;

(d) such documents, information or materials as SMRT and/or any Relevant Authority may require in relation to the Goods and/or Services, and any Interconnected System therewith, including information that each or any of them may require to ascertain the level of cybersecurity of the Goods and/or Services, and any Interconnected System therewith (as the case may be); and/or

(e) relating to an audit and/or cybersecurity risk assessment conducted by SMRT pursuant to the Applicable Standards and/or on instruction by any Relevant Authority.

Notification of changes

2.2. The Supplier shall ensure that no change or modification shall be made to the Goods and/or Services (including without limitation any changes to the design, configuration, security or operation of the Goods and/or Services, or any new connection or modification to an existing connection to the Goods and/or Services) or any specifications thereof previously approved by SMRT unless the prior written agreement of SMRT has been obtained. The Supplier shall provide details of all changes or modifications which are intended to be implemented, and any other information SMRT may require in connection therewith, no later than ten (10) Business Days before such change or modification is made.

2.3. If at any time the Supplier becomes aware of any change affecting the design, configuration, security, cybersecurity or operation of the Goods and/or Services, or any Interconnected System therewith, and/or the ability of SMRT (or any Affiliate of SMRT) to respond to a Cybersecurity Event and/or Cybersecurity Incident relating thereto, or any circumstances which may reasonably so affect the Goods and/or Services, or any Interconnected System therewith, the Supplier shall provide SMRT written notice of such change or circumstances immediately after the Supplier becomes aware of the same, together with any other information SMRT may require in connection therewith. The Supplier shall, in connection with the foregoing, provide any assistance required by SMRT as may be instructed or directed by SMRT.

2.4. The Supplier shall provide SMRT with written notice of any change in the beneficial or legal ownership (including any share in such ownership) of the Goods and/or Services, or any Interconnected System therewith, immediately upon the change in ownership, together with any other information SMRT may require in connection therewith.

3. DIRECTIONS AND STANDARDS

3.1. The Supplier shall have a continuing obligation to SMRT:

(a) to take all necessary measures to ensure that it keeps itself appraised of all prevailing Applicable Standards and any changes thereto, and to perform its obligations under this Contract in a manner which meets or exceeds the Applicable Standards;

(b) to comply in all respects with the provisions of all Applicable Laws (including without limitation the Applicable Standards);

(c) to obtain and maintain all the necessary licences, consents, approvals, waivers or authorisations required under Applicable Standards for the Supplier to perform its obligations under this Schedule;

(d) to comply, without undue delay, with all requirements, rules, directions, standards, guidelines, operating procedures, and policies in connection with this Schedule as may be issued by SMRT from time to time;

(e) to allocate sufficient resources to ensure the smooth implementation and carrying out of all of its obligations under this Contract, and notify SMRT as soon as practicable if, at any time, the Supplier becomes unable to perform its obligations as set out in this Schedule; and

(f) to cooperate with SMRT and provide such information as SMRT may require from time to time to enable SMRT to meet its obligations under this Contract and Applicable Standards.

4. EVENT AND INCIDENT MONITORING, DETECTION

4.1. The Supplier shall establish and implement effective mechanisms and processes to:

(a) monitor, detect and identify Cybersecurity Events and Cybersecurity Incidents in respect of the Goods and/or Services (including any Supplier Systems), or any Interconnected System therewith;

(b) collect and store records of all such Cybersecurity Events and Cybersecurity Incidents (including, where available, logs relating to such Cybersecurity Events and Cybersecurity Incidents);

(c) analyse all such Cybersecurity Events and Cybersecurity Incidents, including correlating between Cybersecurity Events and Cybersecurity Incidents, and determining whether there is or has been any Cybersecurity Incidents; and

(d) provide SMRT regular information feeds and updates of such events and information in such manner and form as SMRT may from time to time specify,

and at all times in accordance with any directions that may be issued by SMRT to the Supplier from time to time.

4.2. The Supplier shall conduct a review of such mechanisms and processes at least once every year to ensure their efficacy and accuracy, and obtain the approval of SMRT before implementing any changes thereto. Upon SMRT's request, the Supplier shall provide SMRT with the records, documentation and/or any other information in relation to such review.

4.3. The Supplier shall provide SMRT the name and contact information of one or more employee(s) of the Supplier who shall serve as SMRT's points of contact for all physical security breach and Cybersecurity Event and Cybersecurity Incident matters, which employee(s) shall be available to assist SMRT at all times in resolving matters associated with a physical security breach, Cybersecurity Event or Cybersecurity Incident.

4.4. The Supplier shall not exploit any Cybersecurity Event and Cybersecurity Incident to the detriment of SMRT.

5. **AUDITS AND RISK ASSESSMENT**

5.1. The Supplier shall allow SMRT (or such persons as SMRT may designate) and/or any Relevant Authority to conduct periodic audits at all locations and sites in which the Supplier is supplying or has supplied Goods and/or Services under this Contract, as well as of any Interconnected System therewith to ensure compliance with this Contract and/or Applicable Standards. Without prejudice to the generality of Clause (b), the Supplier shall fully cooperate with and provide to SMRT (and such persons as SMRT may designate):

(a) support, access (including to the Goods and/or Services, and any Interconnected System therewith), information, documents, materials and assistance in connection with any such audits, and to provide copies or extracts thereof; and

(b) access to such sites or premises as SMRT may require in connection therewith.

5.2. The Supplier shall, at the Supplier's sole cost and expense, make available to SMRT the results of any cybersecurity reviews or cybersecurity audits conducted by the Supplier in connection with the Goods and/or Services, and any Interconnected System therewith, including copies of any such audit reports (or parts of such reports) which relate to cybersecurity which are conducted by or on behalf of the Supplier. Without prejudice to the foregoing, the Supplier shall conduct in relation to the Goods and/or Services, and any Interconnected System therewith:

(a) at least once every year (or earlier and/or at such higher frequency as may be stipulated by the Relevant Authority and/or SMRT from time to time), a cybersecurity risk assessment. Such assessment shall:

(i) identify, as far as is reasonably practicable, every cybersecurity risk to the Goods and/or Services and any Interconnected Systems therewith;

(ii) evaluate the likelihood of the occurrence, and the possible consequences, of the materialisation of each identified cybersecurity risk;

(iii) identify the action(s) to be taken in respect of each identified cybersecurity risk; and

(iv) be in accordance with any directions and/or instructions as may be issued or prescribed by SMRT and/or the Relevant Authority, and at all times be in compliance with the Applicable Standards; and

(b) at least once every two years (or earlier and/or at such higher frequency as may be stipulated by the Relevant Authority and/or SMRT from time to time), a cybersecurity audit conducted by a qualified and reputable independent audit firm acceptable to SMRT. The scope of such audit shall include without limitation compliance with the Applicable Standards,

and provide the results thereof to SMRT within seven (7) days of the completion thereof. The results of the aforesaid shall be provided to SMRT in such form and manner and contain such information as SMRT may from time to time prescribe.

6. RECTIFICATION PLAN

6.1. Where the Supplier becomes aware and/or is notified by SMRT of any non-compliance with the requirements prescribed under Applicable Standards or this Contract, the Supplier shall immediately inform SMRT of such fact in writing, and at the request of SMRT submit a rectification plan to SMRT within fifteen (15) days ("**Rectification Plan**") containing:

(a) an evaluation on any recommendation by any auditor(s), including the feasibility of implementing such recommendation; and

(b) details of the remediation actions which the Supplier intends to take to address all areas non-compliance, including the timelines for implementing the actions thereof.

6.2. SMRT may, in its sole discretion, require the Supplier to revise the Rectification Plan and resubmit the revised Rectification Plan to SMRT within such timeframe as may be prescribed by SMRT.

6.3. Upon approval of SMRT, the Supplier shall implement the Rectification Plan (including any such revisions to the Rectification Plan as may be required by SMRT of the Supplier to remedy non-compliance with Applicable Standards and/or this Contract (as the case may be), hereinafter referred to as a "**Rectification**") and complete all Rectification works to the satisfaction of SMRT within the timeframes as may be prescribed by SMRT.

7. GENERAL

Dealings with Relevant Authority

7.1. The Supplier shall have a continuing obligation:

(a) subject to Clause 7.3, to do and execute or procure to be done and executed all such deeds, things and documents: (i) as may be instructed, directed, ordered, and/or requested by a Relevant Authority; and/or (ii) to comply with codes of practices and guidelines issued by a Relevant Authority from time to time; and

(b) to fully co-operate with and provide SMRT (and/or such persons as SMRT may designate) with access to inspect, test, and/or make copies of any premises, information, book, data, computer output, record, document, apparatus, equipment, computer, computer system, instrument, material, or article, as SMRT may require from time to time in connection with any guidelines, instruction, direction, order and/or request by a Relevant Authority for SMRT to provide or produce the same and/or furnish any information.

Cybersecurity Exercises

7.2. Without prejudice to the generality of Clause 7.1, the Supplier undertakes and agrees to (and will procure that the Supplier's personnel shall):

(a) participate in, cooperate and assist SMRT with cybersecurity exercises conducted by any Relevant Authority and/or SMRT, including exercises to test the state of readiness of the Supplier in responding to significant cybersecurity incidents affecting the Goods and/or Services, and any Interconnected Systems therewith, and/or any review of such cybersecurity exercises; and

(b) attend and participate in all cybersecurity awareness programmes, trainings and/or briefings conducted by SMRT or any Relevant Authority, including but not limited to cybersecurity obligation briefings for vendors and service providers, training and/or briefings in relation to Applicable Standards, standards and/or procedures pertaining to the usage, deployment and access to critical information infrastructure, and/or any review of such programmes and briefings.

Preservation of Secrecy

7.3. Notwithstanding Clause (a) and in any event in all its communications with the Relevant Authority, the Supplier shall:

(a) prior to disclosing Confidential Information to the Relevant Authority, obtain SMRT's written consent thereto;

(b) implement all necessary measures as required under Applicable Standards (including the Cybersecurity (Confidential Treatment of Information) Regulations 2018 read with Section 43 of the Cybersecurity Act) to ensure that, unless an exception applies under Applicable Standards, a Relevant Authority shall not disclose any Confidential Information; and

(c) in any event, when disclosing Confidential Information to the Relevant Authority for any reason, identify (with a written supporting statement giving reasons why the information is confidential) to the Relevant Authority that such information is Confidential Information, as far as possible accompanying such identification with a confidential version of the document containing (and clearly identifying) the information claimed to be Confidential Information as well as a redacted version of the document (in which the information claimed to be Confidential Information has been removed in such manner as will preserve the readability of the redacted version of the document).