

SCHEDULE D – HONG KONG LAW REQUIREMENTS

(Version 7 – 21 March 2025)

A. Definitions

For the purposes of this Schedule and its Appendices, the following terms shall have the following respective meanings:-

- A.1 **“Agreement”** means the Master Services Agreement to which this Schedule forms a part and is deemed incorporated, and all references to “the Agreement” shall include this Schedule;
- A.2 **“Applicable Law”** has the meaning defined in the Agreement and for avoidance of doubt, includes all laws, ordinances and regulations in Hong Kong, and all codes, orders, requirements, directives, decrees, decisions, judgments, interpretive letters, guidance and other official releases of any regulatory bodies in Hong Kong;
- A.3 **“HKMA”** means Hong Kong Monetary Authority;
- A.4 **“Hong Kong”** means the Hong Kong Special Administrative Region of the People’s Republic of China;
- A.5 **“OCC”** means the Office of the Comptroller of the Currency of the United States;
- A.6 **“SFC”** means the [Hong Kong Securities and Futures Commission](#);
- A.7 **“Supplier”** means the Supplier, its Affiliates or any third parties (if any and consented to by Citi) engaged by it to perform the Agreement or any Work Order; and
- A.8 **“Work Order”** shall include any work order, purchase order or statement of work to be performed in Hong Kong and deemed incorporated as part of the Agreement.

B. Provision of Services and/or Deliverables.

- B.1 During the term of the Agreement, each Party shall designate their respective representatives who will be the key contacts for coordinating management meetings/visits and addressing issues relating to the Services and/or Deliverables and such other arrangements or transactions as contemplated under the Agreement.
- B.2 Supplier agrees to participate in and report to Citi on performance reviews to be conducted on a regular basis as reasonably required by Citi.
- B.3 Supplier shall render Services and/or furnish Deliverables with due care according to proper security and operation control process and cybersecurity standards, which are designed to ensure accuracy, confidentiality, integrity, reliability, security and timeliness on all its service delivery. [Note: if the Supplier is an EDSP, the parties shall put in place information security protocols as an appendix to this Schedule – such as the configuration of security settings, workload protection and credential management between the parties, and Citi’s management who has the decryption and encryption keys to Confidential Information.]
- B.4 Supplier shall ensure that any records and reports (including but not limited to the invoices) in whatever form prepared by Supplier in accordance with the Agreement and any of Citi’s Confidential Information shall be subject to Citi’s document retention policy (a copy of which shall be provided by Citi to Supplier). Such records, reports and information shall be made available for Citi’s inspection at any time provided that sufficient prior written notice shall be given to Supplier.

B.5 The Agreement shall be reviewed by the parties regularly and be revised if needed in order to bring it in line with current market standards and to cope with changes in business strategies.

B.6 Supplier shall ensure that Services are provided in accordance with: (1) Citi's security and privacy policies, including without limitation its information security standards as set out in the Customer Standards for Suppliers set forth at <http://www.citigroup.com/citi/suppliers/supplierstandards.htm> or any Citi-designated successor site; or (2) Supplier's security standards if such standards have been approved by Citi through Citi's Information Security Assessment process set out in the Agreement. Supplier will defend, hold harmless and indemnify Citi, its Affiliates and their Personnel from and against any and all losses, claims, liabilities, costs and expenses (including taxes, fees, fines, penalties, interest, reasonable expenses of investigation and reasonable legal fees and reasonable disbursements) as incurred arising out of, or relating to any breach or alleged breach of provisions of Appendix I (Confidential Information, Personal Data and Information Security) to the Agreement.

B.7 Supplier shall report to Citi if there is any material change in the Services and/or Deliverables or any material problems, incidents, accidents or disruption which has/have a material impact on the Services and/or Deliverables.

B.8 Supplier warrants, represents and undertakes that Services and/or Deliverables shall not involve or include any data, information or content (including without limitation, any state secrets or sensitive information related to national security or interest), the disclosure of which will contravene any Applicable Law or is illegal.

C. Information Security.

C.1 Supplier shall (i) inform Citi the location of Supplier's data centres for the processing and storage of Citi's Confidential Information; and (ii) ensure that Citi's Confidential Information shall be segregated or compartmentalized from Supplier's own or its other customers' Personal Data.

C.2 The Receiving Party acknowledges and agrees that the unauthorized disclosure or use of any Confidential Information of the Disclosing Party may cause irreparable damage to such other party which could not be adequately compensated by monetary damages. The Receiving Party, to the extent possible, therefore authorizes the Disclosing Party to seek any temporary or permanent injunctive relief necessary to prevent such disclosure or use, or threat of disclosure or use, without proof of actual damages.

C.3 To the extent that Supplier receives, obtains or generates Citi's Confidential Information as a result of the performance of its obligations under the Agreement, and notwithstanding anything to the contrary contained in the Agreement, Supplier agrees that it will, and will ensure that each of its Personnel will, comply with the following requirements:

- (i) not access, process, transfer or use any of Citi's Confidential Information except to the extent necessary to carry out its obligations under or permitted by the Agreement and for no other purposes;
- (ii) not disclose or transfer any of Citi's Confidential Information to any third party, including, without limitation, its third party service providers without the prior written consent of Citi;
- (iii) host and use Citi's Confidential Information only in Hong Kong and not export or transmit Citi's Confidential Information to any other jurisdiction without the prior written consent of Citi;
- (iv) employ appropriate administrative, technical and physical safeguards to prevent unauthorized or accidental access, disclosure, transfer, processing, erasure, loss or use of Citi's Confidential Information received by it;

- (v) provide such information regarding its cybersecurity standards and its privacy and information security systems, policies and procedures (including information for the screening of its personnel and audit trails/data access logs (which should include information on timestamp, affect file, type of event, user ID and user location) of its personnel who have accessed to Citi's Confidential Information, provided that such personnel shall have no right of access or modification to such audit trails/data access logs) as Citi may request from time to time; and
- (vi) not keep any of Citi's Confidential Information for longer than is necessary for processing of such data. Upon the request by Citi or the cessation of the provision of certain Services and/or Deliverables to Citi, or at any time after any of such information has been processed by Supplier, Supplier will, at Citi's option, as soon as reasonably practicable return or securely destroy any such Information in its possession or under its control. Supplier will certify in writing that it has fully complied with its obligations under this subsection (and that no copies of such information have been retained) within seven (7) calendar days following the date it receives a request from Citi for such a certification.

C.4 Supplier warrants that its Personnel have been properly trained in respect of the handling of Citi's Confidential Information such that they will comply with the relevant requirements under the Agreement.

C.5 Supplier will have in place, and will regularly and thoroughly test, cybersecurity standards and security arrangements which are sufficient to:

- (i) protect the integrity and security of any of Citi's Confidential Information which has been disclosed to, processed by, generated by or otherwise handled by Supplier or any of its Personnel in the course of the performance of Supplier's obligations under the Agreement and any other agreement; and
- (ii) ensure that any of Citi's Confidential Information is not lost, destroyed, accessed, transferred, processed, used or disclosed without appropriate authorization or by accident while it is in the possession or under the control of Supplier or any of its Personnel.

C.6 Supplier will, as part of the Services and/or Deliverables provided, conduct an audit reviewable by Citi of the cybersecurity standards and security arrangements in place in the format and frequency set forth in the applicable Work Order, to ensure that the cybersecurity standards and security arrangements comply with the relevant policies in place to safeguard Citi's Confidential Information.

C.7 If Supplier becomes aware that the security of any of Citi's Confidential Information has been (or may be) compromised or breached, then it will immediately:

- (i) inform Citi;
- (ii) take whatever action is necessary to minimize the impact of the security breach, correct the causes of the breach to the fullest extent possible and advise Citi of the status of its remedial actions; and
- (iii) promptly investigate the underlying causes of the breach and prepare and deliver to Citi a written report which details the causes, and sets out the measures Supplier proposes to implement to prevent reoccurrence of the breach.

C.8 If Supplier is subject to any legal, regulatory, administrative or judicial obligation or requirement, or is required by any government or competent authority (whether within or outside Hong Kong), to disclose or supply any Confidential Information, Supplier shall promptly inform Citi of such obligation or requirement and shall seek written consent from Citi before complying with such obligation or

requirement Citi shall not unreasonably withhold or delay such consent, subject to obtaining consent from HKMA or other competent authorities, if applicable.

C.9. Notwithstanding anything herein to the contrary, this Section C shall survive termination of the Agreement.

D. Data Protection

Part 1 – All Personal Data

D.1 In this Section D:

- (i) **“Applicable Data Privacy Laws”** means all applicable data privacy legislation and regulations (including without limitation the PDPO). and any other related guidance or directives issued by the Data Privacy Commissioner of Hong Kong from time to time in relation to Personal Data;
- (ii) **“PDPO”** means Personal Data (Privacy) Ordinance (Cap. 486) of the laws of Hong Kong, as may be amended from time to time;
- (iii) **“Permitted Jurisdictions”** mean the place(s) listed in the relevant Agreement or Work Order or as otherwise agreed in writing between the parties from time to time, where the Transfer Data may from time to time be processed or held in accordance with the Agreement or any Work Order;
- (iv) **“Personal Data”** means any data (1) relating directly or indirectly to a living individual, (2) from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and (3) in a form in which access to or processing of the data is practicable; for present purposes Personal Data includes names, addresses, emails, dates of birth, telephone numbers.
- (v) **“Data Subject”** means an individual who is the subject of any part of the Transfer Data, and for present purposes Data Subjects include Citi’s past and present customers whose personal data is transferred to Supplier (for the avoidance of doubt, “past customers” refer to customers who cease their banking relationship with Citi after personal data is transferred to Supplier);
- (vi) **“Retention Period”** means any period of time as specified in Citi’s data retention policy;
- (vii) **“Transfer Purposes”** means the purposes designated by Citi and/or its Affiliates in Hong Kong and for which the Transfer Data is transferred to Supplier, as expressly provided for in the Agreement and/or relevant Work Order, in order to enable the Supplier to provide the Services and perform the Work Order or the directly related purposes; and
- (viii) **“Transfer Data”** means any Personal Data of the types or categories listed in the Agreement or the relevant Work Order or as otherwise agreed in writing between the parties from time to time relating to Citi’s customers or any individual transferred or to be transferred by Citi and/or its Affiliate(s) in Hong Kong to Supplier in connection with the Agreement or any Work Order.

D.2 Supplier acknowledges that Citi is subject to the Applicable Data Privacy Laws including without limitation the Data Protection Principles (“**DPP**”) under the PDPO. Supplier agrees that it shall, and shall ensure that each of its Personnel shall, comply with the Applicable Data Privacy Laws from time to time.

D.3 If Supplier engages any third party, whether within or outside Hong Kong, to process the Transfer Data on behalf of Supplier (and Citi’s prior written consent has been obtained), Supplier shall adopt

contractual or other means (i) to prevent any Transfer Data transferred to such third party from being kept longer than is necessary for processing of the data; and (ii) to prevent unauthorized or accidental access, processing, erasure, loss or use of the Transfer Data transferred to such third party for processing.

D.4 Supplier represents, warrants and undertakes the following:-

- (i) Supplier shall hold, process or use the Transfer Data for the Transfer Purposes only to the exclusion of any other purpose and in the Permitted Jurisdiction(s) only. Where the Transfer Data is to be used for a new purpose or in a place outside Hong Kong other than the Permitted Jurisdiction(s), Supplier shall obtain Citi's prior written consent, or with Citi's permission, obtain the prescribed consent of the Data Subject under the Applicable Data Privacy Laws;
- (ii) Supplier shall ensure that the Transfer Data is adequate but not excessive in relation to the Transfer Purposes;
- (iii) Supplier shall hold the Transfer Data securely in accordance with the requirements of DPP4 and the Applicable Data Privacy Laws, and the security measures set out in the Agreement and/or the relevant Work Order. Supplier shall have in place appropriate technical and organizational measures and standards to protect the Transfer Data against unauthorized or accidental access, processing, erasure, loss or use, including without limitation:-
 - (A) having robust policies and procedures in place and providing adequate training for its staff; and
 - (B) adopting physical and computer security measures;
- (iv) Supplier shall not retain the Transfer Data longer than is necessary for the fulfillment of the Transfer Purposes and, in any event, not longer than any applicable Retention Period;
- (v) Supplier shall take all practicable steps to erase the Transfer Data, once it is no longer required to be retained for the fulfilment of the Transfer Purposes or, in any event, once any applicable Retention Period has lapsed or as otherwise instructed by Citi;
- (vi) Supplier shall take all practicable steps to ensure that the Transfer Data is accurate, having regard to the Transfer Purposes, and that any inaccurate Transfer Data (i) should not be used or processed unless it is rectified or (ii) should be erased;
- (vii) Supplier shall use or process the Transfer Data exclusively for the Transfer Purposes and shall not transfer or disclose, either free of charge or in return for any benefits, the Transfer Data to any third party, nor use, sell, or transfer the Transfer Data for its or any third party's provision or marketing of services or product to customers. If and to the extent that the Services and the Transfer Purposes include the deployment of any form of online tracking, Supplier undertakes to comply with all the obligations and requirements under the Applicable Data Privacy Laws in relation to online tracking;
- (viii) Supplier shall immediately rectify, erase or return the Transfer Data on receiving instructions to this effect from Citi. Supplier undertakes to rectify, erase or return all or part of the Transfer Data if it appears that such measures are required by the requirements of the Applicable Data Privacy Laws;
- (ix) Supplier has and shall at all times have in place accessible documents which clearly specify its policies and practices in relation to Personal Data;
- (x) Supplier shall ensure or provide such assistance as may be reasonably required by Citi to ensure that Data Subjects have rights of access to and correction of their Personal

Data in the same way as they would have had under the Applicable Data Privacy Laws;
and

- (xi) Supplier shall not disclose, transfer or allow access to the Transfer Data to a third party data user or data processor (“**Sub-transferee**”) whether located within or outside Hong Kong unless it has obtained the prior written consent from Citi and:
 - (A) the Sub-transferee is located, and will only hold, process or use the Transfer Data, in Permitted Jurisdiction(s);
 - (B) the sub-transfer is made to a Permitted Jurisdiction that has in force any law which is substantially similar to, or serves the same purposes as the Applicable Data Privacy Laws;
 - (C) such Sub-transferee becomes a signatory to the Agreement or another written data transfer agreement which imposes the same or substantially similar obligations on it as are imposed on Supplier under this Section D; and
 - (D) Supplier has adopted all reasonable non-contractual measures and auditing mechanisms to the reasonable satisfaction of Citi to monitor the Sub-transferee’s compliance with the obligations under this Section D as if they are applicable to that Sub-transferee.

D.5 Upon Citi’s request, Supplier shall submit its data processing facilities, policies and procedures, data files, documentation and any other relevant information for reviewing, auditing and/or certifying by Citi or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by Citi, to ascertain compliance with its warranties and undertakings in this Schedule.

D.6 Supplier has no reason to believe that there are currently in force any local laws that would have adverse effect on its warranties or undertakings above, and Supplier shall notify Citi if it becomes aware of any such laws.

D.7 Supplier has the legal capacity and the authority to give the warranties and undertakings in this Section D.

- (a) D.8 Supplier shall promptly inform Citi of its inability to fulfill any of its obligations in this Section D.

D.9 Supplier shall promptly notify Citi about any abnormalities or any loss, accidental or unauthorized access or processing, erasure or other use of the Transfer Data.

D.10 Supplier shall deal with promptly and properly all reasonable enquiries from Citi relating to the fulfillment of its obligations hereunder and Supplier shall abide by the reasonable instructions and advice (if any) of Citi or any supervisory authority in this regard.

D.11 Supplier shall ensure its staff who handles the Transfer Data will carry out the security measures and obligations specified in this Section D.

D.12 Supplier shall notify Citi about Supplier’s contact person in relation to the handling of the Transfer Data, and shall cooperate with Citi, Data Subjects and relevant authorities concerning all enquiries within reasonable time.

D.13 In the event of a dispute or claims brought by a Data Subject or the privacy enforcement authority concerning the processing of the Transfer Data hereunder against any or all parties hereto, the parties shall cooperate with a view to settling them amicably in a timely fashion.

D.14 If the Services and/or Deliverables involve the Supplier processing Transfer Data in offshore data centre, the Supplier warrants and represents that it is not aware of any restrictions or regulations pertaining to cross-border or cross-boundary transfers of data back to Citi from the jurisdiction

where the Transfer Data are processed, and shall promptly notify Citi if it becomes aware of any such restrictions or regulations.

Part 2 – PRC-originated Personal Data

D.15 Without prejudice to Part 1 of Section D, in this Part 2 of Section D:

- (i) **“PRC”** means the People's Republic of China excluding the Special Administrative Regions of Hong Kong Special Administrative Region and Macau Special Administrative Region, and Taiwan;
- (ii) **“PRC-originated Personal Data”** means any Transfer Data that was collected from a Data Subject in the PRC that is protected by Applicable PRC Data Privacy Laws;
- (iii) **“Applicable PRC Data Privacy Laws”** means all applicable data privacy legislation and regulations (including without limitation the PRC Personal Information Protection Law, the PRC Data Security Law, and the PRC Cybersecurity Law) and any other related rules or guidance implemented in the PRC from time to time in relation to PRC-originated Personal Data; and
- (iv) **“PRC-originated Sensitive Personal Data”** means PRC-originated Personal Data that once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his or her personal safety or property, including information such as biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, as well as the PRC-originated Personal Data of a minor under the age of 14 years.

D.16 Supplier acknowledges that, in respect of PRC-originated Personal Data, Citi may be subject to an obligation to process such data in a manner that meets the protection standards stipulated in the Applicable PRC Data Privacy Laws. Without prejudice to Part 1 of this Section D, Supplier agrees that it shall, and shall ensure that each of its Personnel, shall comply with the Applicable PRC Data Privacy Laws in respect of the processing of PRC-originated Personal Data.

D.17 [Without prejudice to Section D.4(vii), when using PRC-originated Personal Data for automated decision making, Supplier shall ensure transparency in decision-making in relation to Data Subjects as well as fairness and impartiality of the results, and not apply unreasonable differential treatment as a result of any automated decision making to any Data Subject in terms of transaction conditions such as transaction price; when using automated decision-making for commercial marketing, Supplier shall provide each Data Subject with options that allow the Data Subject to receive commercial marketing which is not based on the targeting of personal characteristics or provide the Data Subject with a convenient way to refuse commercial marketing.]

D.18 Without prejudice to Section D.4(x), Supplier shall also ensure or provide such assistance as may be reasonably required by Citi to ensure that Data Subjects have rights to be informed and to make decisions on the processing of their Personal Data, the right to restrict or refuse the processing of their Personal Data by others, the right to request copy or delete their Personal Data, and the right to request an explanation of the rules governing the processing of their Personal Data.

D.19 Supplier agrees that the conditions set out under Section D.4(xi) shall also apply when providing the PRC-originated Personal Data to a Sub-transferee located outside the PRC, and the Supplier shall:

- (i) have a business need for providing the PRC-originated Personal Data to a Sub-transferee as acceptable to Citi; and
- (ii) ensure that when processing the PRC-originated Personal Data, such Sub-transferee will comply with the personal data protection standards stipulated by the Applicable PRC Data Privacy Laws and assume legal liability for any infringement of the rights of a Data Subject as a result of the provision of the PRC-originated Personal Data to such sub-transferee outside of the PRC.

D.20 Without prejudice to Sections D.4(x), D.9 and B.7, if the PRC-originated Personal Data transferred to Supplier is or is suspected to be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorisation (“**Personal Data Breach**”), Supplier shall, without undue delay:

- (i) take appropriate measures to address the Personal Data Breach, including measures to mitigate its adverse effects on the Data Subjects; and
- (ii) facilitate any obligation that Citi may have to notify the provider of the PRC-originated Personal Data, supervisory authority and/or any Data Subject in the case of a Personal Data Breach, including to notify Citi of: (1) the categories of PRC-originated Personal Data involved in, and the reasons for the Personal Data Breach and the possible harm caused by, the Personal Data Breach; (2) the remedial measures that have been adopted; (3) the measures that can be adopted by the Data Subject to mitigate the harm; and (4) the contact information of the person or team of the Supplier responsible for handling the relevant situation.

E. Compliance and Audit.

E.1 Supplier undertakes to comply with the Applicable Law (as defined in the Agreement) and not to use any payment from Citi pursuant to the Agreement and/or any Work Order for illegal purposes.

E.2 Supplier agrees that the Services it performs and/or the Deliverables it furnishes for a branch of U.S. bank in Hong Kong are subject to examination of the HKMA and OCC and other competent authorities. Supplier agrees to cooperate with Citi’s internal and external auditors and the relevant regulatory or competent authorities including, but without limitation, HKMA, SFC, and the Hong Kong Privacy Commissioner for Personal Data for their (or any person appointed by them) review, supervision, audit, or inspection of materials or the status of operation by Supplier in connection with the Services and/or Deliverables provided by Supplier pursuant to the Agreement. Supplier shall, upon reasonable notice, allow Citi, its management, its auditors and/or its regulators, access to its data, IT systems, premises, records and personnel for the purpose of obtaining, inspecting, examining and auditing Supplier's operations, contingency plans and the business and financial records which are relevant to the Services and/or Deliverables provided hereunder by Supplier including but not limited to Supplier's critical processes to confirm that Supplier's processes meet or exceed industry standards in such area of contingency planning, continuity of business plans, software engineering and test processes, change control procedures, critical staff succession planning and compliance with applicable laws and regulations. Supplier shall cooperate fully with Citi's internal or external auditors to ensure a prompt and accurate audit.

E.3 If an audit leads to a conclusion that Supplier has breached the provisions of the Agreement or that any of Supplier's business or professional practices related to its performance of Services and/or its furnishing of Deliverables presents any deficiencies, Supplier shall use its best efforts to implement any recommended and/or corrective measures and/or correct any practices which are found to be deficient as a result of any such audit within a reasonable time.

- E.4 Supplier will submit a independent audited financial report to Citi, as may be reasonably required by Citi from time to time, for assessing Supplier's financial soundness in supporting the Services and/or Deliverables.
- E.5 For the avoidance of doubt, nothing in the Agreement or any Work Orders shall have the effect of restricting or impeding the unconditional rights, scope and/or frequency of a regulator (and/or its representatives or designees) to conduct audits or access information for supervisory inspection and review of operations and controls of the Supplier, and this provision shall override any contractual terms which might provide to the contrary.
- E.6 Notwithstanding any terms under the Agreement to the contrary, to the extent that any term in the Agreement is in conflict with any applicable Hong Kong laws, regulatory requirements, guidelines or policies, or any change thereto, Citi may notify Supplier with suggested amendment to the Agreement to the extent necessary to comply with such laws, regulatory requirements, guidelines or policies, or any such change, in which event Supplier shall have the option either to accept such amendments (which shall become effective upon notification) or to terminate the Work Order(s) or a part thereof to be performed for or relating to the relevant Citi entity(ies) in Hong Kong by giving 30 days' notice in writing to Citi.

F. Continuity of Business.

- F.1 If any of the disaster or disruption events occurs, shall have occurred, happened or come into effect; namely the circumstances are beyond the reasonable control of the Supplier, which affects the provision or receipt of the whole or any of the Services and/or Deliverables, the Supplier must:
- (i) immediately notify and consult Citi; and
 - (ii) provide recovery services and otherwise do everything reasonably necessary to re-establish the provision of the Services and/or the Deliverables.
- F.2 If a party receives advance warning or notice of the possibility of the occurrence of any disaster or disruption, that party shall notify the other party and the parties shall use their best endeavours to make such alternative or emergency arrangements as may be necessary or desirable in order to ensure that the Services and/or the Deliverables are continuously provided in accordance with the Agreement.
- F.3 Supplier will maintain a contingency plan and related processes or controls for the continuation of business ("**Disaster Recovery Plan**") to help ensure that Supplier will be able to provide the Services and/or the Deliverables and perform its obligations from alternate locations or with replacement Personnel no later than the applicable recovery time prescribed under the Disaster Recovery Plan.
- F.4 Supplier must review and test its Disaster Recovery Plan at least annually in accordance with Citi's requirements. Within ten (10) Business Days (or the period of time that is specified in any Work Order) after completing each test, Supplier will provide Citi with a summary of the test objectives, the test plan and the test results, including the timeframes required to recover critical business functions and evidence of the test results (e.g. screen shots).

G. Subcontracting

- G.1 Supplier may not subcontract the performance of any of its obligations in the Agreement without (i) informing Citi the location of Supplier's or subcontractor's data centres for the processing and storage of Citi's Confidential Information; and (ii) the prior written consent of Citi. To the extent that Supplier subcontracts to third parties any of its obligations set forth in the Agreement with the consent of Citi, Supplier shall remain fully responsible for such obligations and for all acts or omissions of its subcontractors or agents. Nothing in the Agreement shall be construed to create any contractual relationship between Citi and the Supplier's subcontractors or agents.

H. Termination.

- H.1 Citi shall have the right to terminate the Agreement and/or any Work Order with immediate effect and without penalty by giving three (3) days prior written notice to the Supplier in the event that (i) HKMA or any other competent authority requires Citi to do so, or to make alternative arrangements in relation thereto (it being agreed that a certificate from Citi that this has occurred shall be conclusive of that fact); or (ii) Supplier does not comply with Applicable Law (as defined in the Agreement) or causes Citi to violate Applicable Law. The right of termination in this paragraph is in addition and independent to those in the Agreement.

- H.2 If the Agreement and/or any Work Order is terminated for any reason or expires, Supplier shall:

- (i) immediately return to Citi all property, information, data (including all Personal Data) and material (including copies) belonging to Citi then in the possession, power or control of Supplier or any of its Associated Persons in such format and on such media as Citi reasonably requests, or, if specifically required by Citi, securely destroy such property, information, data or materials (to be certified by an officer of Supplier) or transfer it to a replacement service provider in accordance with timescales agreed between the parties in relation thereto;
- (ii) comply with all reasonable instructions from Citi relating to termination and shall take steps to mitigate any costs which Citi may incur as a result of such termination, including providing (in a readily readable form), upon request by Citi, those documents, records and information (in addition to those referred to in Section H.2(i) above) without which Citi, in its reasonable opinion, would be unable (or unable without incurring significant cost) to continue to carry on in the same manner the activities to which the Services and/or Deliverables relates; and
- (iii) render reasonable assistance to Citi if requested and to the extent necessary to effect an orderly assumption by Citi and/or any replacement service provider of Services and/or Deliverables previously performed by Supplier. Where such assistance requires additional resource to be deployed by Supplier or is required following the termination date, in circumstances where termination is not due to a breach by Supplier, Citi shall pay Supplier at reasonable time and materials rates for the assistance provided.

- H.3 If the Agreement and/or any Work Order is terminated for any reason or expires, and notwithstanding anything to the contrary therein, Citi may retain copies of Deliverables, Supplier Materials and any related documentation for archival purposes and to satisfy its obligations under all Applicable Law (as defined in the Agreement).

I. Governing law.

- I.1 This Schedule shall be governed by, and construed in accordance with, the laws of Hong Kong, and the parties hereby agree to submit to the non-exclusive jurisdiction of the Hong Kong courts.

- I.2 Nothing in this Schedule, whether expressed or implied, is intended to, or will, confer on any person any benefit or any right to enforce any term which such person would not have but for the Contracts (Rights of Third Parties) Ordinance (Cap. 623 of the Laws of Hong Kong).

J. Additional Provisions applicable to Suppliers of Artificial Intelligence (AI) System/Solution involving the use of Personal Data

J.1 Supplier agrees and undertakes to:

- (i) implement measures to minimise the risk of attacks against machine learning models, such as malicious input / prompts or training data being fed into the AI system (data poisoning attacks), or the deliberate generation of incorrect or unsafe output (adversarial attacks);
- (ii) implement internal guidelines for staff on the acceptable input to be fed into and the permitted/prohibited prompts to be entered into AI systems;
- (iii) establish multiple layers of mitigation to prevent system errors or failures at different levels or in different modules of the AI system;
- (iv) establish contingency plans to promptly suspend the AI system and trigger fallback solutions if necessary;
- (v) establish mechanisms to ensure that the operations of the AI system is sufficiently transparent to enable end-users to interpret its output;
- (vi) establish mechanisms to enable the traceability and auditability of the AI system's output by, for example, where appropriate and in accordance with the data minimisation principle, automatically recording events (i.e., logs) while the AI system is operating;
- (vii) conduct periodic review of the AI models to ensure that they are operating and performing as intended;
- (viii) if requested by Citi, provide information on and explanations of AI output to enable effective exercise of human oversight; and
- (ix) maintain proper documentation on the procurement, risk assessment, risk mitigation measures taken, data sources, data preparation, customisation, testing and validation, implementation and use of the AI system.