

SCHEDULE Q – VIETNAM LAW REQUIREMENTS

(Version 17 – 8 May 2026)

A. DEFINITIONS

For the purposes of this Schedule / Local Country Addendum and its Appendices, the following terms shall have the following meanings:-

- A.1. **“Agreement”** means the Master Agreement and all its attached documents including but not limited to this Schedule and related Work Order if any.
- A.2. **“Artificial intelligence” (“AI”)** is the electronic implementation of human intellectual capacities including learning, reasoning, perception, judgment and understanding natural language.
- A.3. **“AI system”** means a machine-based system designed to perform AI capabilities with different levels of autonomy that is capable of self-adaptation after deployment. Based on clearly defined or implicitly formed objectives, the system infers from input data to generate outputs such as predictions, content, recommendations or decisions that may affect the physical or digital environment.
- A.4. **“AI developer”** means an organization or individual engaging in designing, developing, training, testing or adjusting all or part of a model, algorithm or system of AI; and having the direct control over the technical methods, training data or model parameters.
- A.5. **“AI provider”** means an organization and individual who provides an AI system to the market, or puts it into operation under their own name, brand or trademark regardless of whether the system is developed by themselves or by a third party.
- A.6. **“AI implementer”** means an organization and individual using an AI system under their control in professional, commercial and service activities, excluding the use for personal or non-commercial purposes.
- A.7. **“AI user”** means an organization and individual who directly interact with the AI system or use its output.
- A.8. **“AI affected person”** means an organization and individual that is directly or indirectly affected to their legitimate rights, interests, life, health, property, reputation or opportunities to access to services due to the deployment or output of the AI system.
- A.9. **“AI serious incident”** means an event occurring during the operation of an AI system that causes or poses a risk of significant harm to life, health, human rights, property, cybersecurity, public order, environment, or disrupts the operation of important information systems related to national security.
- A.10. **“Citi Vietnam”** shall refer to Citi NA, Ha Noi Branch or Citi NA, Ho Chi Minh Branch and any Citi Affiliates in Vietnam (each **“Citi Vietnam”**);

- A.11. **“Cybersecurity”** refers to the stability, security, and safety of cyberspace, the protection of information systems, and assurance that information, data, and activities in cyberspace do not harm national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals¹;
- A.12. **“Cybersecurity Incident”** means any unusual occurrence in cyberspace which infringes upon national security, social order and safety and/or the lawful rights and interests of organizations and individuals as defined in the Law on Cybersecurity²;
- A.13. **“Customer Information”** shall be as defined in **Appendix I**;
- A.14. **“Confidential Information”** shall be as defined in C.1 below.
- A.15. **“Infrastructure”** means a computer or computer system;
- A.16. **“Outsourcing”** means a written agreement by a bank on hiring an individual, organization, credit institution or other foreign bank's branch (hereinafter referred to as a third party) to process data; identify customers; or perform one or several stages of the bank's business process (except for the bank's risky decision that are not allowed internally or by laws to be outsourced) on behalf of the bank, in accordance other applicable law ³.
- A.17. **“Permitted Purpose”** means any processing relating to or in connection with the particular project described in an Agreement or Work Order, as permitted by Citi Vietnam in writing;
- A.18. **“Third Parties”** include affiliates, agents, consultants, contract non-employee workers, contractors, sub-contractors, third party hires of the Supplier;
- A.19. **“Use”** means collection, processing, disclosure or other use;
- A.20. **“Personal Data”** means digital data or other forms of information that identifies or assists to identify a specific individual. Personal Data includes Basic Personal Data and Sensitive Personal Data;
- A.21. **“Basic Personal Data”** means personal data reflecting common personal details and background information, frequently used in transactions and social relations and specified by the Government of Vietnam, including but not limited to name, date of birth, place of birth, ID/passport number, nationality, contact information, gender, images, marital status, family relationship, personal digital account and other information associated with a specific person or to identify a specific person⁴.
- A.22. **“Sensitive Personal Data”** means personal data associated with individual privacy that, if infringed upon, would directly affect your legitimate rights and interests. This includes political and religious views; health status, personal/ family secrets and private life; information related to ethnic background and ethnic origin; biometric data, genetic characteristics; sexual life/ orientation; location is determined through location services; usernames and passwords to access electronic identification accounts; Images of identity cards; Username and password of the bank account; bank card information, data on transaction history of bank accounts; financial

¹ Article 2.1 of the Vietnam Cybersecurity Law (Law No. 116/2025 on Cyber Security of Vietnam will be effective from 1 July 2026).

² Article 2.13 of the Vietnam Cybersecurity Law.

³ Circular 83/2025/TT-NHNN dated 31 December 2025 on internal control (effective from 1 July 2026)

⁴ Law 91/2025/ QH15 dated 26 June 2025 and its guiding Decree 356/2025/ND-CP dated 31 December 2025, Article 3.

information, credit and information on activities, history of financial, securities and insurance transactions; data to track behavior, activities using telecommunications services, social networks, online communication services and other services in cyberspace and other personal data required by law to be kept confidential or strict security measures are required.⁵

- A.23. **“Personal Data Processing”** means one or more activities impacting personal data, including one or more of the following: collection, analysis, summary, encryption, decryption, modification, deletion, destruction, de-identification, provision, disclosure, transfer of personal data, and other activities impacting personal data.
- A.24. **“PDPL”** refers Law No. 91/2025/QH15 dated 26 June 2025 and its guiding Decree 356/2025/ND-CP dated 31 December 2025 on personal data protection and as amended from time to time.
- A.25. **“Work Order”** shall include “Purchase Order” or “Statement of Work” or other documents of the same nature and contents.

B. PROVISION OF SERVICES (TO BE APPLICABLE FOR ALL TYPES OF SERVICES)

B.1 General Provisions:

- (a) During the term of the Agreement, each Party shall designate their authorised representatives who will be the key contacts for coordinating management meetings/visits and addressing issues relating to the Services and such other arrangements or transactions as contemplated under the Agreement.
- (b) Supplier agrees to participate in and report to Citi on performance reviews to be conducted on a regular basis if reasonably required by Citi Vietnam.
- (c) Supplier shall render Services with due care according to its security and operation control process and its cybersecurity standards, which are designed to ensure accuracy, confidentiality, integrity, reliability, segregation, security and timeliness on all its service delivery.
- (d) 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) to the Agreement.

B.2 Sub-contracting

- B2.1 Supplier is solely responsible for all acts and omissions of its sub-contractors, including the performance and risk management practices of such sub-contractors, as if such acts and omissions were its own and nothing herein shall be construed to create any contractual relationship between Citi Vietnam and any sub-contractor. Supplier

⁵ Law 91/2025/ QH15 dated 26 June 2025 and its guiding Decree 356/2025/ND-CP dated 31 December 2025, Article 4

warrants that any and all subcontractors engaged in the performance of services under this Addendum shall be contractually bound to comply with all applicable laws of Vietnam. The Supplier remains fully responsible for ensuring such compliance."⁶

B.2.2 Notwithstanding anything to the contrary in the Agreement and/or Work Order, the Supplier shall not assign, outsource or sub-contract any or all of its obligations set forth in the Agreement and/or Work Order to any third parties without the prior written consent of Citi Vietnam.

B.2.3 To the extent that the Supplier is so permitted by Citi Vietnam to assign, outsource or subcontract any of its obligations set forth in the Agreement and/or Work Order pursuant to the sub-clauses above, the Supplier shall procure the compliance by all assignees/ outsourcees/ sub-contractors (and their respective Personnel) with the provisions of the Agreement, Work Order and this Schedule / Local Country Addendum relating to the performance of such obligations (including, without limitation, provisions relating to security and confidentiality, audit and inspection and business continuity management).

B.2.4 The Supplier shall, and shall procure its sub-contractors to:

- i. Allow Citi Vietnam to obtain copies of any report or finding made on the Supplier and its sub-contractors in relation to the Services under the Agreement or Work Order, whether produced by the Supplier or its sub-contractors' internal or external auditors, or by agents appointed by the Supplier or its sub-contractors.
- ii. Allow Citi Vietnam, its internal or external auditors or agents and/or its regulators (the "**Citi Vietnam auditing parties**"), the opportunity of inspecting, examining and auditing Supplier's and its sub-contractors' operations and business records which are relevant to the Services provided, including but not limited to, Supplier's and its sub-contractors' critical processes, to confirm that such processes meet industry standards in areas such as security and control environment, incident management, 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;
- iii. Cooperate fully with the Citi Vietnam auditing parties to ensure a prompt and accurate audit. If Citi Vietnam provides recommendations for enhancing the Supplier's and its sub-contractors' critical processes, then the Supplier and its sub-contractors shall give due consideration to implementing such recommendations. The Supplier and its sub-contractors shall also use its best efforts to correct any practices which are found to be deficient as a result of any audit within a reasonable time after receipt of the audit report;
- iv. Adopt appropriate corrective measures, including enforcement actions to address violations of law and regulations or unsafe or unsound banking practices by Citi Vietnam or the Supplier.

B.2.5. Acknowledgment of final liability: The Supplier acknowledges and agrees that the subcontracting any services does not alter or delegate the Supplier ultimate responsibility for the performance of its obligations to the Citi, regulators and other stakeholders. The Supplier remains solely responsible for the results and compliance of any activities outsourced to the Subcontractor.

⁶Law No.134. on AI (Article 14), Law No. 91/2025/QH15 (Article 37) on Personal Data Protection (PDPL).

B.3 Notification of changes or adverse developments

B.3.1 Supplier shall immediately notify Citi Vietnam of any adverse developments or changes, including those affecting its Affiliates or approved assignees/outsources/sub-contractors (and their respective Personnel), that has or could be reasonably expected to have a material impact on the Supplier's ability to carry out (or Citi Vietnam ability to receive) the Services and/or Deliverables effectively and in accordance with the provisions of the Agreement or Work Order and this Schedule. Examples of adverse developments and changes, include but are not limited to:

- i. any interruption of Services (including unplanned unavailability of any systems, software or infrastructure Supplier uses to deliver the Services);
- ii. any event that could potentially lead to prolonged service failure or disruption to the Services;
- iii. any breach of security and confidentiality of Customer Information;
- iv. any force majeure or other event that would cause Supplier to invoke business continuity or disaster recovery plans;
- v. any strategic business change that could impact Service provision such as a change of control of Supplier; and
- vi. any issues identified by Supplier's internal or external auditors that may have or has a material adverse impact on the provision of the Services.

B.3.2 Incident Reporting Timeframe: Notwithstanding any other provision, for any information security incident, data breach, or system violation, the notification to Citi Vietnam required under Section B.3.1 and Section I.2 must be made within three (03) hours of detection by the Supplier. This notification must include all available details to enable Citi Vietnam to meet its regulatory reporting obligations, including but not limited to those under Circular 09/2020/TT-NHNN and the Law on Personal Data Protection (PDPL) and as amended from time to time.⁷

B.4 Audit and Inspection Right

B.4.1 Citi, its auditors, or its authorized regulator shall have the right to conduct risk assessment, to monitor, inspect and audit the Supplier to ensure compliance with the Master Agreement and/or the relevant Work Order in relation to the Services. Supplier shall cooperate with Citi's internal and external auditors and regulators. Supplier shall keep complete and accurate records of all of its work and expenses in providing the Services to Citi for a period not less than five (5) years from the date which the record was created or such other longer period as requested by Citi in writing or as required by local laws.

B.4.2 The Supplier shall require any subcontractor appointed (if applicable) to also maintain complete and accurate records of all of its work and expenses in relation to the Service subcontracted to it. Supplier shall ensure and procure that these requirements are set forth in its arrangements with any subcontractor.

⁷ Circular 09/2020, Article. 54.1; Law on PDPL, Article. 23.1

B.4.3 The Supplier shall allow Citi, its auditors and/or its regulators to (i) to obtain records and documents of transactions and information of Citi given to, stored at or processed by Supplier, (ii) access any report and findings made on the Supplier in conjunction with the Services performed for Citi, (iii) access to the business premises of the Supplier in the exercise of its rights herein; and (iv) inspect, examine and audit the Supplier's operations and records insofar as they are relevant to the Services.

B.5 Retention:

B.5.1 Supplier shall ensure that any records and reports (including but not limited to the Agreement, related 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 as stated in this Schedule (a copy of which shall be provided by Citi to Supplier if necessary). 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.5.2 The Supplier shall not retain Confidential Information (or any documents or records containing Confidential Information either electronic or otherwise) for any period of time longer than is necessary to serve Permitted Purposes. Upon the request by Citi Vietnam or the cessation of the provision of certain Services to Citi Vietnam, or at any time after any of such information has been processed by Supplier, Supplier will, at Citi Vietnam'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 Vietnam for such a certification.

B.6 Termination

B.6.1. Upon termination of the Agreement or Work Order, the Supplier shall allow Citi Vietnam to remove from the Supplier all documents, records of transactions and information previously provided to the Supplier (including without limitation, information incorporated in computer software or held in electronic storage media, together with any analyses, compilations, studies, reports or other documents or materials containing any such data, Customer Information, as are in the possession or control of the Supplier), and Citi Vietnam shall be allowed to delete, destroy or render unusable by the Supplier all such data or Customer Information previously given. The Supplier shall certify in writing to Citi Vietnam within seven (7) days of the termination of the Agreement and/or Work Order that it has not retained any such data or Customer Information in any form whatsoever.

C. CONFIDENTIAL INFORMATION

C.1. Confidential Information means information relating to Citi Vietnam or Citi Vietnam Affiliates or their respective Representatives received or accessed by the Supplier, Supplier Affiliates and their respective Representatives including Citi Vietnam's Personal Data, Citi Vietnam's Customer Information and other information relating to the Citi Vietnam's products and services and the terms and conditions on which they are provided, technology (including software, the form and format of reports and online computer screens), pricing information, internal policies, operational procedures and any other information which is either designated by the Bank as confidential at the time of disclosure or that a reasonable person would consider to be of a confidential or proprietary nature.

C.2 Without prejudice to the confidentiality provisions under the Agreement, the Supplier shall not disclose Confidential Information to any relevant Affiliate or Third Parties without consent from

Citi Vietnam unless this is on a “need to know” basis and for Permitted Purposes under the Agreement and such Affiliate or Third Party is bound to comply with the obligations of confidentiality at least as stringent as those set forth in the Agreement.

- (a) If the Supplier shall be under a legal, regulatory, administrative or judicial obligation to disclose any Confidential Information, the Supplier shall, where it is practical and legally able to do so, give the Citi Vietnam prompt notice thereof.
- (b) The Supplier shall (i) inform Citi Vietnam 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' information and prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar issues.
- (c) The Supplier acknowledges and agrees that the unauthorized disclosure or use of any Confidential Information of Citi Vietnam may cause irreparable damage to such other party which could not be adequately compensated by monetary damages. The Supplier, to the extent possible, therefore authorizes Citi Vietnam 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. The provisions of this sub-section shall survive the termination of the Agreement.
- (d) To the extent that Supplier receives, obtains or generates Citi Vietnam's Confidential Information as a result of the performance of its obligations under this Agreement, and notwithstanding anything to the contrary contained in this Agreement, Supplier agrees that it will, and will ensure that each of its Personnel will, comply with the following requirements:
 - (i) not access, alter, destroy, disclose, modify, transfer or use any of Citi Vietnam's Confidential Information except as permitted by this Agreement and to the extent necessary to carry out its obligations hereunder;
 - (ii) not disclose or transfer any of Citi Vietnam's Confidential Information to any Third Party, including, without limitation, its third party service providers without the prior written consent of Citi and subject to the further requirements of this section and other related sections provided below if appropriately required;
 - (iii) employ appropriate administrative, technical and physical safeguards to prevent unauthorized or accidental access, disclosure, transfer, processing, erasure, loss or use of Citi Vietnam's Confidential Information received by it;
 - (iv) comply with all the obligations of confidentiality at least as stringent as those applicable to Supplier and all applicable rules and regulations concerning confidentiality to ensure that Citi Vietnam's Confidential Information is protected against unauthorized or accidental access, disclosure, transfer, processing, erasure, loss or use; and
 - (vi) promptly 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 Vietnam may request from time to time.
- (d) The 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.

- (e) At all times during the duration of this Agreement, 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 this 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.

On request from Citi, Supplier will use all commercially reasonable efforts to demonstrate to Citi its compliance with this subsection, and will ensure that each of its relevant Personnel does so.

- (g) Supplier will, as part of the Services 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.
- (h) If Supplier becomes aware that the security of any of Citi Vietnam's Confidential Information has been (or may be) compromised, then it will **immediately**:
 - (i) inform Citi Vietnam;
 - (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 Vietnam of the status of its remedial actions; and
 - (iii) promptly investigate the underlying causes of the breach and prepare and deliver to Citi Vietnam a written report which details the causes, and sets out the measures Supplier proposes to implement to prevent reoccurrence of the breach.
- (i) If the Supplier is directed by court order, subpoena or other legal or administrative proceeding, regulatory or supervisory agency's request or similar process to disclose any Confidential Information, Supplier shall inform Citi of such examination and shall seek written consent from Citi Vietnam before releasing / disclosing such data and information to such governmental authority, as the case may be (unless it has a legal obligation to the contrary), with a copy of such document attached, in sufficient detail immediately upon receipt of such court order, subpoena, legal or administrative, regulatory or supervisory agency's request or similar process, in order to permit application by Citi Vietnam for an appropriate protective order. Citi Vietnam shall not unreasonably withhold or delay to provide to Supplier such written consent if it is required unless otherwise explicit restriction or constrains by related authority/ by applicable regulations.
- (a) The Supplier hereby acknowledges and consent that Citi may be requested at any time by the State Bank of Vietnam or other local competent authority to provide Supplier's information and statistical data for purposes of assessment, inspection and supervision of operations of the credit institutions and in such case.
- (k) The Supplier hereby acknowledges and undertakes that in case of receipt of a written notice from Citi Vietnam highlighting Citi Vietnam's obligations of confidentiality and data

privacy under State secrets protection and IT system security under the laws of Vietnam, the Supplier hereby that the Supplier shall fully understand and strictly comply with the local laws and regulations applicable to the services provided by the Supplier under the Agreement and Work Order and as per guidance, notification of Citi Vietnam.

D. CUSTOMER INFORMATION

Along with the general requirements in Section C above, the following provisions shall also apply to Confidential Information which particularly constitutes as Customer Information:

- D.1 Notwithstanding anything to the contrary and subject to the provisions in this Schedule / Local Country Addendum, the Supplier shall not, without Citi Vietnam's prior written consent, disclose Customer Information provided pursuant to any Agreement or Work Order in any manner except as expressly authorized by the Agreement or Work Order. The Supplier undertakes to Use Customer Information solely for the Permitted Purpose and in accordance with all of Citi Vietnam's further instructions relating to such Use which Citi Vietnam may issue from time to time (including instructions to completely cease Use of any specific Customer Information).
- D.2. Where the Supplier provides Services to or deals with a Citi Vietnam entity that is subject to the Law on Credit Institutions, including without limitation, Citibank, N.A., - Ho Chi Minh City Branch and Citibank, N.A., - Ha Noi Branch, the following provisions shall apply:-
- D.2.1 The Supplier hereby acknowledges receipt of a written notice from Citi Vietnam highlighting Citi Vietnam's obligations of confidentiality under Law on Credit Institutions and guiding regulations of such laws (collectively referred to as "**Law on Credit Institutions** "). The written notice is attached hereto as **Appendix I**.
- D.2.2 The Supplier agrees to execute the Confidentiality and Privacy of Customer Information Undertaking in the form specified in **Appendix II** and the Supplier hereby acknowledges that it is aware and understands the effect of, and agrees and undertakes to, and to procure all its employees, servants, agents, representatives and Personnel to observe all precautionary measures and prevent disclosure of information that will cause Citi Vietnam or any of its Affiliates to violate its statutory duty pursuant to the Law on Credit Institutions⁸ not to disclose any Customer Information of Citi Vietnam to any person except as expressly provided in the Law on Credit Institutions. For the avoidance of doubt, the term "person" includes the Supplier's Affiliates.
- D.2.3 The Supplier further agrees and undertakes that it will not, and will covenant all employees, servants, agents, representatives and Personnel not to do anything which will cause Citi Vietnam or its Affiliates to violate any provision of Law on Credit Institutions or otherwise be guilty of an offence thereunder.
- D.2.4. The Supplier shall procure the execution of the Confidentiality and Privacy of Customer Information Undertaking in the form specified in **Appendix III** by each of the Supplier's Personnel appointed or to be appointed in connection with Work Order and/or to perform the Services or part thereof for and on behalf of Supplier.
- D.2.5 The Supplier and its employees (i) shall not without Citi Vietnam's prior written consent further disclose Customer Information in any manner to any Third Parties unless required to do so by law and (ii) shall treat information with at least the same degree of care that it treats its own confidential information, but in no event with less than a reasonable degree of care. For the avoidance of doubt, the Supplier's Affiliate (other than one approved by Citi Vietnam to provide the Services) shall be considered a Third Party for the purposes of this clause.

⁸ Art 13 of Law on Credit Institutions

E. OUTSOURCING

Outsourcing is defined in Section A above. Once the Service under the Agreement is outsourced by Citi Vietnam to the Supplier, the following provisions shall also apply:

E.1 Cooperation for Outsourcing Due Diligence

Prior to the outsourcing of any Services by Citi to Supplier, the Supplier shall reasonably cooperate with Citi to fulfill all legal and regulatory requirements in respect of the Services for the purpose of Citi's due diligence of the Supplier.

E.2 Business Continuity Management

E.2.1 The Supplier represents, warrants and covenants that it has in place satisfactory business continuity plans ("BCP"), evidencing how the Supplier shall, under exceptional circumstances, be in a position to perform its obligations under the Agreement or Work Order, including but not limited to continuity of service, disaster (whether natural or man-made) recovery plans that minimize the probability and impact of interruption to Citi Vietnam business including recovery time objectives, recovery point objectives and resumption operating capacities, back up processing, protecting program and data files and equipment for the orderly and expeditious provision of the Services. The Supplier will provide Citi Vietnam with all required information in relation to the BCP, including any alternative locations or sites established by the Supplier for such purposes. The Supplier further represents and warrants that the BCP shall be in place for the entire term of the Agreement or Work Order.

E.2.2 The Supplier shall test the BCP in relation to the Services and all facilities used by it in connection with the BCP on a regular basis and notify Citi Vietnam of any test finding that may affect the Supplier's performance. Where requested, Supplier shall also allow Citi Vietnam to participate in and jointly test Supplier's BCP and disaster recovery exercises. The Supplier will ensure that all relevant personnel receive regular training in activating the BCP and executing recovery procedures. If the Supplier makes any substantial change(s) to the BCP or there are any adverse developments that may substantially impact the Services, it shall notify Citi Vietnam in writing and provide a full description of such significant change(s) and/or adverse developments immediately.

E.2.3 In the event that such test(s) on the BCP in relation to the Services are reasonably required by Citi Vietnam in connection with the testing of its own business continuity plan, the Supplier shall co-operate fully with Citi Vietnam to ensure that such test(s) are carried out as soon as reasonably practicable and accurately in accordance with Citi Vietnam reasonable requirements.

E.2.4 The Supplier shall at all times be capable logically or physically segregating, clearly identifying and protecting all Customer Information, documents, records, information and assets such that in adverse conditions, all such information, documents, records of transactions and information given to the Supplier, and assets of Citi Vietnam, can be either promptly removed from the possession of the Supplier in order to continue its business operations, or deleted, destroyed or rendered unusable.

E.3 Monitoring and control of outsourcing arrangements

E.3.1 The Supplier agrees to meet with Citi Vietnam at any time and from time to time upon prior written notice being given to the Supplier at the reasonable request of Citi Vietnam to review all aspects of the Services provided by the Supplier pursuant to an Agreement or Work Order and/or other matters of mutual interest to the Supplier and Citi Vietnam and adopt any recommendations and/or measures reasonably proposed by Citi Vietnam to ensure, inter alia, compliance with legal and regulatory obligations.

E.4 **Mandatory Supervision Mechanism**⁹:

The Supplier agrees to participate in and be subject to the official supervision mechanism established by Citi Vietnam. This mechanism includes, but is not limited to:

- (i) regular, scheduled performance reviews against the agreed Service Levels and key risk indicators, taking place at least quarterly,
- (ii) continuous monitoring of the Supplier's risk profile, including financial stability, operational resilience, and compliance with legal and regulatory requirements.
- (iii) provide periodic reports to Citi Vietnam, in the format and frequency determined by Citi Vietnam, detailing performance, risk assessment and any material changes to the Supplier's operations or control environment.

F. **PERSONAL DATA PROTECTION**

Along with the general requirements in Section C above, the following provisions shall also apply for Personal Data:

- F.1. Notwithstanding anything to the contrary and subject to the provisions in this Schedule / Local Country Addendum, the Supplier shall not, without Citi Vietnam's prior written consent, disclose Personal Data provided pursuant to any Agreement or Work Order in any manner except as expressly authorized by the Agreement or Work Order. The Supplier undertakes to Processing Personal Data solely for the Permitted Purpose and in accordance with all of Citi Vietnam's further instructions relating to such Processing which Citi Vietnam may issue from time to time (including instructions to completely cease Processing of any specific Personal Data).
- F.2. Notwithstanding anything stated to the contrary, Supplier shall comply with all its obligations under the PDPL with respect to the Processing of Personal Data provided by Citi Vietnam.
 - F.2.1. **Consent Obligations**: Where the Supplier collects any Personal Data directly from Citi Personnel or any other persons, including the Supplier's own personnel or from any third party, it shall limit the collection of such Personal Data to the Permitted Purposes, and only with consent of the individual ("**Subject Individuals**") in such manner set out in the PDPL and as Citi Vietnam may prescribe.
 - F.2.2. Where required by Citi Vietnam in respect of Personal Data, Supplier shall provide Citi Vietnam with full details of its internal procedures and processes with regards to its Processing of Personal Data ("**Data Protection Processes**") and will work with Citi Vietnam within the agreed timescales to prepare and agree in writing (amending its current procedures as required), a method for ensuring its procedures comply with Citi Vietnam's requirements as notified to Supplier. If at any time the Supplier changes any of its Data Protection Processes affecting the Agreement and/or Work Order as agreed with Citi Vietnam pursuant to this sub-clause, it will promptly notify Citi Vietnam in writing of such changes and refrain from implementing and using any such changes unless and until agreed by Citi Vietnam.
 - F.2.3. **Transfer of Personal Data**: The Supplier shall not transfer Personal Data to a place outside Vietnam without Citi Vietnam's prior written consent. If such consent is provided, the Supplier acknowledges that such activity constitutes a cross-border transfer of personal data under PDPL, and the Supplier shall:

⁹ Article 40 of State Bank of Vietnam's Circular 83/2025/TT-NHNN on internal controls.

- i. only store and process such Personal Data in the locations specified in the Agreement or Work Order;
- ii. comply with Vietnamese cross-border data transfer regulations. The Supplier acknowledges the requirements of Vietnam's PDPL concerning cross-border data transfers. The Supplier shall, upon request and in a timely manner, furnish Citi Vietnam with all necessary information, documentation, and assessments required for Citi Vietnam to prepare and submit its 'Dossier for Cross-Border Personal Data Transfer Impact Assessment' to the competent Vietnamese authorities. This includes, but is not limited to, details on data receiving parties, data processing and storage locations, data flow diagrams, and a summary of the technical and organizational data protection measures applied by the Supplier and its subcontracts.¹⁰, and
- iii. ensure that any third party overseas (including the Supplier's subsidiaries, affiliates, and subcontractors) involved in the processing of such data contractually commits to data protection standards that are sufficient to meet the requirements of PDPL and the aforementioned impact assessment.

F.2.4. Security

The Supplier shall protect Personal Data in the Supplier's control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information & communications technology measures) to prevent unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Personal Data, or other similar risks. For the purpose of this Schedule / Local Country Addendum, "reasonable security arrangements" include security arrangements set out in Citi Vietnam's policies and processes referenced in the Agreement.

- F.2.5. The Supplier shall provide Citi Vietnam with access to the Personal Data that the Supplier has in its possession or control, as soon as practicable upon Citi Vietnam's written request.
- F.2.6. The Supplier shall put in place adequate measures to ensure that the Personal Data in its possession or control remain or is otherwise accurate and complete. In any case, the Supplier shall take steps to correct any errors in the Personal Data, as soon as practicable upon Citi Vietnam's written request.
- F.2.7. The Supplier shall immediately notify Citi Vietnam when the Supplier becomes aware of a breach of any of its obligations in Sections F.2.1. to F.2.6. above.
- F.2.8. For the purpose of this section F.2.8, "**Data Breach**" shall mean the unauthorized (including accidental or intentional) access, collection, use, disclosure, copying, modification, disposal, loss, damage or destruction of Personal Data, and "**Affected Individual**" shall mean any individual to whom any Personal Data affected by a Data Breach (as defined above) relates. Without limiting the provisions in Section F.2.8 and Section F.3. in this Schedule / Local Country Addendum:

¹⁰ The requirement are under Article 20 of the Law 91 and Articles 17-18 of Decree 356.

- i. Supplier must **immediately** notify the Citi point of contact and/or Citi Vietnam of any Data Breach and shall provide a detailed description of the Data Breach, the type of Personal Data that was the subject of the Data Breach and the identity of each Affected Individual, as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Citi Vietnam may reasonably request relating to the Data Breach). The notification provided by the Supplier under this section shall include, at a minimum, the nature of the incident, the categories of data and number of data subjects concerned, and the technical and organizational measures taken by the Supplier to address the incident. This is to ensure the Client has sufficient information to meet its own statutory reporting obligations under Vietnamese law, including any requirement to notify competent authorities or affected data subjects.

Furthermore, in the event of a data breach involving personal location data or biometric data, the Supplier shall notify Citi and/or Citi Vietnam within a timeframe that allows Citi Vietnam to meet its obligation of notifying the affected data subject matter within 72 hours (or another specific timeframe given by local applicable laws) from the time the violation is detected.¹¹

- ii. Supplier shall provide full cooperation and assistance to Citi Vietnam in respect of its efforts to (i) investigate, remediate, and mitigate the effects of the Data Breach and (ii) comply with notification obligations to individuals, clients or regulatory authorities.

F.2.9. The Supplier shall, upon the request of Citi Vietnam, provide full cooperation and assistance to Citi Vietnam to comply any data porting request made under the PDPL, including without limitation, (a) providing Citi Vietnam with all Personal Data it holds in relation to the relevant individual within the timescales required by Citi Vietnam, (b) fulfilling any requirements under the applicable law and regulations for providing and transmitting the applicable data under a porting request, and (c) assisting Citi Vietnam to comply with the individual's porting request within the relevant timescales set out by Citi Vietnam and in accordance with Citi Vietnam's instructions.

F.2.10. The Supplier acknowledges that Citi, as a Data Controller (or Data Controller cum Processor if the case may be), is required to conduct a Personal Data Processing Impact Assessment ("DPIA"). The Supplier shall provide all necessary cooperation, information, and assistance in a timely manner to enable Citi to prepare and submit its DPIA to the competent Vietnamese authorities in compliance with the PDPL.¹²

F.3. Data Subject Rights: To the extent that the Supplier receives, from an individual (or a person/entity acting on the individual's behalf), a request, complaint, or other communication related to Personal Data, it will promptly notify Citi Vietnam. The Supplier shall provide its full

¹¹ As required by Article 29 of Decree 356/2025/ND-CP.

¹² To comply with Article 21 of Law 91 and Article 19 of Decree 356

and timely cooperation and assistance to enable Citi Vietnam to respond to and comply with all data subject requests under the PDPL, including but not limited to rights to be informed, view, modify, access, delete, restrict processing, withdraw consent, and object to processing. Such assistance shall be provided in a manner that allows Citi Vietnam to meet the statutory timeframes for response and implementation as prescribed in PDPL.

F.4 Data storage in Vietnam: Notwithstanding any other provision, where Supplier provides services on telecommunications networks, the internet, or value-added services in cyberspace in Vietnam, Supplier shall comply with all data storage and localization requirements (if applicable) under Vietnamese law that includes the obligation to store personal information of service users, data generated by service users in Vietnam, and data on the relationships of service users in Vietnam for the period prescribed by the Government of Vietnam. Supplier shall provide Citi Vietnam with evidence of such compliance upon request¹³.

F.5 Personal protection in emerging technologies

F.5.1 Where Supplier's services involve the use of artificial intelligence, metaverse, or blockchain technologies for processing personal data, Supplier shall comply with all applicable requirements under the applicable laws and regulations related to personal data collected in Vietnam (including but not limited to Articles 10 and 11 of Decree 356/2025/ND-CP on personal data protection), and applicable laws and regulations applicable to AI providers and AI implementers in Vietnam (including under Law 134/2025.

F.5.2. For AI systems, Supplier shall be responsible for notifying data subjects of automated processing, explaining the operating principles of algorithms, and providing an opt-out mechanism, in the manner required by law.

F.5.3 For blockchain applications, Supplier warrants that it will not store personal data directly on the blockchain, and will only store such data where it has been de-identified or where hash values of the personal data are stored.

F.5.4 Supplier shall conduct periodic assessments of its compliance with these specific personal data protection regulations annually and provide the results to Citi Vietnam upon request.

F.6. Data Protection Personnel (DPO) : The Supplier warrants and represents that it has appointed, and will maintain throughout the term of the Agreement, a data protection unit and/or personnel satisfying the competency conditions and being responsible for performing the tasks outlined in PDPL in regard to personal data collected from Vietnam¹⁴. The Supplier shall provide evidence of such compliance upon Citi Vietnam's request.

G. CLOUD COMPUTING SERVICES

¹³ Article 25 of the Cybersecurity Law 2025

¹⁴ Articles 13 and 14 of Decree 356

Along with the general requirements in Section B above, the following provisions shall also apply for Cloud Computing Services as the case may be:

- G.1 Where the Supplier has been approved by Citi Vietnam to provide public or private cloud computing services or a portion of the Services that Supplier has been approved by Citi Vietnam to provide involve the use of public or private cloud architecture, technology or a multi-tenanted system, such as Software as a Service ("SaaS"), Platform as a Service ("PaaS") or Infrastructure as a Service ("IaaS"), the Supplier shall:
- G.1.1. comply with the standards of protection required under the PDPL when they process Personal Data as data intermediaries;
 - G.1.2. clearly identify and segregate all Customer Information using strong physical or logical controls that have been reviewed and approved by Citi Vietnam;
 - G.1.3. implement robust access controls that have been reviewed and approved by Citi Vietnam to protect all Customer Information at all times;
 - G.1.4. not make changes to the approved and contracted service structure and any security settings without the prior written consent of Citi Vietnam. The Supplier hereby acknowledges and agrees that breach of this Section G.1.4. shall entitle Citi Vietnam to terminate the Work Order in accordance with the relevant termination provisions in this Schedule / Local Country Addendum.
 - G.1.5. store such data only in the specific locations (cities and countries) designated in the applicable Work Order, and for the period as required by Vietnam regulations. The Supplier shall not change these locations without prior written consent from Citi Vietnam and shall provide evidence of such compliance upon requests;¹⁵ and
 - G.1.6. all Personal Data stored or processed within the cloud environment is encrypted both at rest and in transit, and is protected by strict access authorization controls.¹⁶

H. TECHNOLOGY RISK MANAGEMENT

H.1. Supplier Personnel

At Citi Vietnam's request, the Supplier shall ensure that all its Personnel involved in the provision of the Services who have access to Citi Vietnam's information assets¹⁷ participate in and complete an IT security awareness training program.

Supplier shall ensure that all its Personnel involved in the provision of the Services are assessed to meet and comply with Citi Vietnam hiring policies and standards, as made known

¹⁵ Article 26.3 of the Law on Cybersecurity No. 116/2025/QH15

¹⁶ Requirements of Article 12.4 of Decree 356 on Personal Data Protection.

¹⁷ Information assets include data, hardware and software. Information assets are not limited to those that are owned by the financial institution ("FI"). They also include those that are entrusted to the FI by customers or third parties, rented or leased by the FI, and those that are used by service providers to deliver their services to the FI.

to Supplier, for the respective services or roles they are providing or performing. Examples of the relevant assessment criteria, include but are not limited to:

- i. whether they have been the subject of any proceedings of a disciplinary or criminal nature;
- ii. whether they have been convicted of any offence (in particular, that associated with a finding of fraud, misrepresentation or dishonesty);
- iii. whether they have accepted civil liability for fraud or misrepresentation; and
- iv. whether they are financially sound.

I. CYBERSECURITY

Along with the general requirements in the above Section B, the following provisions shall also apply in respect of Cyber Security:

- I.1 Where required by Citi Vietnam, the Supplier will co-operate with and provide, or procure its sub-contractors to co-operate with and provide, prompt assistance to Citi Vietnam in relation to any obligations or requirements under the Law on Cybersecurity (as may be amended from time to time) that Citi Vietnam is required to comply with in relation to the Services and/or Deliverables and/or the Infrastructure used to deliver the same.
- I.2 Supplier must **immediately** notify Citi Vietnam of any Cybersecurity Incident in respect of the Services and/or the Infrastructure when the Supplier becomes aware of the Cybersecurity Incident¹⁸. The notification must be provided with sufficient details required by the competent local authority, including but not limited to the following information systems facing the incident,
 - Importance level of the information system facing the incident;
 - Time of detection of the incident;
 - Severity level of the incident;
 - Type of incident.

J. ARTIFICIAL INTELLIGENCE SYSTEMS

- J.1. To the extent that any Services provided or implemented under the Agreement involve the use of an AI System, the Supplier warrants that it is in full compliance with local requirements under the Law on AI No. 134/2025/QH15 and as amended from time to time (the “AI Law”).
- J.2. Risk Classification and Conformity: The Supplier shall:
 - i. classify its AI system according to the risk levels defined in AI Law and provide Citi with the complete classification dossier for any medium-risk or high-risk system.
 - ii. for any high-risk AI system, conduct a conformity evaluation as required by AI Law and provide the results to Citi and/or Citi Vietnam before putting the system into operation.

¹⁸ Article 41.1.b of Law on Cybersecurity.

J.3. Transparency and Labeling: The Supplier shall ensure that any content (text, audio, images, video) generated or edited by its AI system is clearly marked or labeled to distinguish it from human-made content.

J.4. Provider obligations for high-risk AI systems: For any high-risk AI system, the Supplier, in its capacity as the Provider and or Implementer, accepts all responsibilities outlined in the AI Law, including but not limited to maintaining risk management measures, ensuring human oversight capabilities, and providing operational explanations to competent authorities upon request. In details:

J.4.1. Providers of high-risk AI systems are responsible for:

- i. promulgating and maintaining risk management measures, and regularly reviewing the systems when there is a significant change or a new risk arise;
- ii. administer the training, testing and operational data to ensure the quality in accordance with technical capabilities and the system's purpose;
- iii. prepare, update and archive technical dossiers and activity logs at a level that is necessary for conformity evaluation and post-deployment inspection; provide this information to competent state authorities in accordance with necessary principles and inspection purpose without disclosing trade secrets;
- iv. design the systems that ensure human oversight and intervention capabilities;
- v. fulfill transparency obligations and perform incident handling as prescribed in the AI Law;
- vi. provide explanation to competent state authorities on the use purpose, operational principles regarding functional description, main types of input data, risk management and control measures, and other necessary information for inspection; provide users and affected persons with public information regarding functional description, operational methods and risk warnings during operation. The explanation and provision of information shall not include the disclosure of source codes, detailed algorithms, parameter sets or information related to trade secrets or technical secrets;
- vii. cooperate with competent state authorities and deployers in inspecting, evaluating, post-inspecting and fixing incidents related to the systems.

J.4.2. Implementer of high-risk AI systems are responsible for:

- i. operating and supervising the systems in accordance with classified purpose, scope and risk level without generating new or higher risks;
- ii. ensure data security and human intervention during operation;
- iii. maintain compliance with standards and technical regulations on AI during operation;
- iv. fulfill transparency obligations and perform incident handling as prescribed in the AI Law;
- v. provide explanation to competent state authorities on operation, risk controlling measures, incident handling and necessary information inspection; provide users and affected persons with public information regarding functional description, operational methods and risk warnings during operation;
- vi. cooperate with providers and competent state authorities in inspecting, evaluating, post-evaluating and fixing incidents.

J.4.3. Any explanation shall comply with technical capabilities of systems without disclosing trade secrets in accordance with the laws.

J.4.4. AI Providers and Implementer are encouraged to participate in civil liability insurance or apply measures to fulfill other obligations to promptly fix incidents and pay damages.

J.4.5. Local Presence: Foreign providers having high-risk AI systems that are provided in Vietnam shall have a legal contact point in Vietnam. In cases where a system is subject

to mandatory conformity certification before being put into operation, it must have a commercial presence or an authorized representative in Vietnam.

- J.5. Incident handling: In the event of a serious AI incident, the Supplier shall promptly apply technical measures to fix, suspend, or recall the system, notify competent authorities and Citi in accordance with AI Law. The report and handling of incidents shall be carried out via the single-window website on AI or as guided by Vietnam competent authority;
- J.6. Third-Party monitoring, audit, and reporting for AI systems: In compliance with State Bank of Vietnam regulations for AI applications in the banking sector, the Supplier shall:
- i. provide to Citi and/or Citi Vietnam, on an annual basis, an independent audit report on its information technology compliance, conducted by a qualified independent auditor.
 - ii. provide to Citi and/or Citi Vietnam, on an annual basis, a comprehensive report on the results of the inspection and assessment of the quality and performance of the outsourced AI model.
 - iii. provide Citi and/or Citi Vietnam with access to a tool or dashboard to continuously monitor the performance and key risk indicators of the AI model, including but not limited to, model drift, data drift, and accuracy degradation.
 - iv. upon request, provide Citi and/or Citi Vietnam with all necessary information on the AI model's technical characteristics, limitations, update mechanisms, and security measures to enable Citi to conduct its own risk assessments.
- J.7. AI system Service Continuity: In addition to the general Business Continuity Management obligations in Section E.2, the Supplier commits to ensuring continuity for any outsourced AI system. The Supplier shall maintain a specific contingency plan and an appropriate transition plan to be activated if support for the AI model is discontinued or a material change in the model occurs, to prevent disruption to Citi 's operations.
- J.8. AI Supply Chain Security. For any AI system provided to Citi Vietnam, the Supplier shall:
- i. Establish and maintain an information security inspection process for all third-party or open-source software libraries, datasets, and pre-trained models used. The Supplier shall provide the results of such inspections to Citi and/or Citi Vietnam upon request.
 - ii. Develop and maintain a detailed, up-to-date list of all software components of the AI system, including AI libraries, model versions, and dependent components, and make this list available to Citi to facilitate security tracing and incident response.
 - iii. For any high-risk AI system, conduct a periodic audit or assessment of its supply chain risk management, at least annually, and provide the results to Citi and/or Citi Vietnam.
- J.9. Intellectual Property of AI Systems and Output:
- i. Output generated by Citi using Trained AI or GenAI shall be deemed to be owned by Citi, and the Supplier hereby assigns (and shall procure that its Personnel assign) all present and (on creation) future Intellectual Property Rights in or to such Output to Citi.
 - ii. To the extent that the Trained AI has been created using Citi data, Supplier hereby assigns (and shall procure that its Personnel assign) all present and (on creation) future Intellectual Property Rights in or to such Output to Citi.
 - iii. Training Data provided by or on behalf of Citi shall be deemed to be Content.

K. WITHHOLDING TAX

The Supplier being foreign contractors shall incur value added tax and corporate income tax imposed on the Services and/or Deliverables under the Master Agreement and applicable Work Order as required by laws of Vietnam, and Citi will pay such taxes on behalf of the Supplier pursuant to local applicable regulations¹⁹.

L. GOVERNING LAW AND JURISDICTION

- L.1 The Master Agreement (solely as it applies between or among the Parties to the related Work Order), the Work Order and related non-contractual matters shall be governed by the governing law applicable to Master Agreement and/or the Work Order and resolved by the jurisdiction as agreed at the parties' discretion therein, provided, however, any claims or disputes arising out of or in connection with the Master Agreement and/or the relevant Work Order which is performed, in whole and/or in part, in Vietnam, including any question regarding its existence, validity or termination and shall be referred to and finally resolved by the non-exclusive jurisdiction of court in Vietnam. And in case the legal proceeding is brought in a court sitting in Vietnam, the Master Agreement (solely as it applies between or among the Parties to the related Work Order), the Work Order and related non-contractual matters shall be governed in accordance with the laws of Vietnam

M. SURVIVAL

- M.1 The provisions of this Schedule that, by their nature and content, must survive the completion, rescission, termination or expiration in order to achieve their fundamental purpose and effect hereof, shall so survive the Agreement and Work Order, and continue to bind the Supplier.

[APPENDIX I – PRIVACY OF CUSTOMER INFORMATION UNDER THE LAW ON CREDIT INSTITUTIONS APPLICABLE TO CITIBANK, N.A., - HO CHI MINH CITY BRANCH AND CITIBANK, N.A., - HA NOI BRANCH](#)

[APPENDIX II – VIETNAM LAWS AND REGULATION – CONFIDENTIALITY AND PRIVACY OF CUSTOMER INFORMATION UNDERTAKING \(FOR THE SUPPLIER\)](#)

[APPENDIX III – VIETNAM LAWS AND REGULATIONS - CONFIDENTIALITY AND PRIVACY OF CUSTOMER INFORMATION UNDERTAKING \(FOR SUPPLIER'S EMPLOYEES/AGENTS/SERVANTS/PERSONNEL\)](#)

¹⁹ Article 1.1, Article 5.1 and Article 11 Circular 103/2014/TT-BTC dated 6 August 2014 (as amended/ replaced from time to time).