

SCHEDULE C – CHINA LAW REQUIREMENTS

(Version 15 – 18 March 2026)

This Schedule shall apply to the services (“Services”) provided to the Citi entities incorporated in the jurisdiction of the People’s Republic of China (for the purpose of this Schedule, excluding Hong Kong Special Administrative Region, Macau Special Administrative Region and Taiwan) (“PRC”). Further, the terms that have been marked with “APPLICABLE TO CCCL ONLY” shall be applicable to Citibank (China) Co., Ltd. (“CCCL”) only and the terms that have been marked with “APPLICABLE TO CSRC REGULATED ENTITIES ONLY” shall be applicable to Citigroup Securities (China) Company Limited and Citigroup Futures (China) Company Limited only. All other terms without such marks shall be applicable to all Citi China entities.

A. Outsourcing (APPLICABLE TO CCCL ONLY, except for A.1.1, A.1.2 and A.1.9.2 which shall be applicable to all Citi China entities)

A.1 General Provisions

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.

2. Audit and Inspection Right

2.1 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 Agreement and/or the relevant work order or statements of work (“Work Order”) in relation to the Services. The Supplier shall cooperate with Citi’s internal and external auditors and regulators. The Supplier shall keep complete and accurate records of all of its work and expenses in connection with the Services for a period not less than two (2) years from the date which the record was created or such other longer period as requested by Citi in writing.

2.2 The Supplier shall procure its subcontractor, if any, to maintain complete and accurate records of all of its work and expenses in connection to the Service subcontracted to it. The Supplier shall ensure that these requirements are set forth in its agreements with its subcontractor(s).

2.3 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 for the purpose of exercising Citi’s rights herein; and (iv) inspect, examine and audit the Supplier’s operations and records insofar as they are relevant to the Services.

3. Cross-border Outsourcing¹

3.1. For any cross-border outsourcing, the Supplier shall be, and shall ensure its sub-contractor(s) be in one of the countries or jurisdictions set forth in the attached **Appendix A**, representing those countries or jurisdictions where the regulator(s) have signed a memorandum of understanding or other agreement (the “MOU”) with banking regulators of the PRC.² No cross-border outsourcing service can be provided by any organization or individual in the country or jurisdiction that is not listed in the attached Appendix A without the prior written consent of Citi.

¹ This provision is only applicable when the Supplier is incorporated outside of mainland China.

² Article 19.3 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

4. Controls

- 4.1 The Supplier shall regularly report Service related matters to Citi in accordance with Citi's reasonable requirements.³
- 4.2 The Supplier shall promptly notify Citi of any issue which may affect the provisions of the Services or of any problems, accidents or disruptions which may have a material impact on the Services.⁴
- 4.3 Except for the Services provided in the Agreement and/or the relevant Work Order, the Supplier shall not conduct any other activity in the name of Citi.⁵
- 4.4 The Supplier shall ensure that the software and/or hardware (if any) used for providing the Services shall not infringe upon any patent, copyright, trademark, trade secret or other proprietary right of Citi and any third party.⁶
- 4.5 The Supplier shall logically segregate and separate its service resources related to the Services provided to Citi from those of Supplier's other clients or customers,⁷ and ensure that only Citi has the highest access authority to Citi's business system and data.⁸

5. Continuity of Business

- 5.1 The Supplier and Citi shall each use reasonable efforts to develop, maintain and adhere to a plan providing measures to be taken by the Supplier in the event of contingencies, in order to ensure the Supplier's ability to continue providing the Services. The Supplier's established service continuity plans and its agreed targets therein shall be consistently managed by Supplier, and shall in all circumstances satisfy the requirements of business continuity of Citi.⁹

6. Termination¹⁰

- 6.1 In the following circumstances, Citi shall have the right, in addition to other rights or remedies that are available to Citi under the Agreement and/or the Work Order and/or applicable law, to terminate, with immediate effect upon notice, the services provided to or for the benefit of Citi in the PRC under any Work Order or relevant agreement:
 - (1) Where the Supplier is found to be unable to protect Citi's customer information or Citi's customer rights are jeopardized due to the Supplier's failure to protect Citi's customer information; and
 - (2) Where the Services provided by the Supplier infringes the rights of Citi's customer, or the complaints made by Citi's customer is verified to be true.

³ Article 16.1 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

⁴ Article 16.2 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

⁵ Article 16.5 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

⁶ Article 21.6 of Measures for the Supervision of Information Technology Outsourcing Risks of Banking and Insurance Institutions ("IT Outsourcing Guidelines") (银行保险机构信息科技外包风险监管办法, ("科技外包指引"))

⁷ Article 18.1 of IT Outsourcing Guidelines (科技外包指引)

⁸ Article 18.4 of IT Outsourcing Guidelines (科技外包指引)

⁹ Article 14.3 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

¹⁰ Article 16.4 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

7. Transition Services¹¹

- 7.1 Upon the termination of the Agreement and/or the relevant Work Order for any reason whatsoever (including a default by either party), each party shall provide such information, cooperation and assistance to the other party, as such other party may reasonably request, to assure an orderly return or transfer to the requesting party or its designee of all proprietary data (and related records and files) materials and/or facilities (if any) of the requesting party.
- 7.2 If the Agreement and/or the relevant Work Order is terminated for any reason other than a circumstance which could expose the Supplier to ongoing damages or liability, the Supplier shall provide such assistance to Citi as Citi reasonably requests to transition to another service provider of Citi's choice, subject to Citi's agreement to pay the Supplier's reasonable costs and expense for such transition assistance.

8. Assignment and Subcontracting

- 8.1 The Supplier is prohibited from (i) completely transferring/assigning or outsourcing all of the Services to a third party or do so in disguise, (ii) sub-contracting any key part of the Services to a third party. Additionally, the Supplier shall ensure that its sub-contractor(s) does not further transfer/assign the sub-outsourced business to any third party.¹² Supplier must enter into agreements with any subcontractors to ensure that subcontractors are obligated to fully uphold and comply with the same obligations and responsibilities as Supplier under the Agreement and any applicable Work Orders. Supplier is solely responsible for all acts and omissions of its subcontractors as if such acts and omissions were its own.¹³
- 8.2 If the Services are sub-outsourced, the Supplier shall monitor the subcontractor and shall, in accordance with the provisions of the Master Agreement and/or the relevant Work Order, obtain prior approval from or provide notice to Citi regarding the changes of subcontractor (if any).
- 8.3 All provisions of the Agreement and/or the relevant Work Order shall be binding upon and shall inure for the benefit of the Supplier and Citi and their legal successors and permitted assigns.

9. Other Terms

- 9.1 If the Service is an outsourcing service, Supplier shall not charge Citi's customers for the services related to such Service.¹⁴
- 9.2 The Agreement and/or Work Order in relation to the Services shall contain provisions addressing the following: (1) the scope and standards of the outsourcing service; (2) the arrangements for the confidentiality and safety of the outsourcing service; (3) the dispute resolution mechanism for outsourcing disputes; and (4) liabilities for breach of contract.

A.2 Special Requirements if the Service provided constitutes Information Technology Outsourcing (as defined below)

¹¹ Article 14.6 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

¹² Article 22 of IT Outsourcing Guidelines (科技外包指引); Article 17,18 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

¹³ Article 22 of IT Outsourcing Guidelines (科技外包指引)

¹⁴ Article 18 of CBIRC Guiding Opinions on Regulating the Administration of Adjusted Prices in the Banking Service Market (中国银保监会关于规范银行服务市场调节价管理的指导意见)

1.1 Definition of Information Technology Outsourcing¹⁵

Information Technology Outsourcing refers to the arrangement that Citi entrusts the Supplier to carry out the information technology activities that originally should be conducted by Citi.

1.2 If the Service constitutes Information Technology Outsourcing, in addition to the requirements provided in Section A.1, the following provisions shall apply as well:

- 1.2.1 Supplier and Citi shall specify the following elements in the relevant Work Order: Service scope, Service requirements, Service time and arrangement, responsibility allocation, description of deliverables, relevant condition requirements for the service renewal, service quality assessment and evaluation arrangement¹⁶, content and frequency for regular reports, reporting route, reporting method and time limit requirements for emergencies' reporting¹⁷, information assets that need to be accessed or used for outsourcing activities¹⁸.
- 1.2.2 The Supplier shall ensure compliance of applicable laws and regulations and Citi's internal policies, and ensure the regulatory requirements as notified by Citi from time to time are duly implemented.¹⁹
- 1.2.3 Supplier represents and warrants that the software and/or hardware applied to the Service shall not infringe upon any patent, copyright, trademark, trade secret or other proprietary right of any third party. Citi represents and warrants that any software, hardware or other technology, information or materials provided by Citi to Supplier in connection with the Services shall not infringe upon any patent, copyright, trademark, trade secret or other proprietary right of any third party. Unless otherwise specified in relevant Work Order, all Work Products resulting from the Services shall be the property of Citi and all Intellectual Property Rights in and to such work products shall vest exclusively in Citi to the fullest extent permitted under law.²⁰
- 1.2.4 The Supplier shall ensure that it, in any circumstance, will allocate sufficient resources to duly provide the Services to Citi.²¹
- 1.2.5 Supplier shall not use or disclose Citi's information beyond the scope permitted by the Agreement and/or the Work Order, and Supplier shall not in any form, transfer, misappropriate Citi's data or seek benefits other than those stipulated in the Work Order.²²
- 1.2.6 The governing law of the provisions applicable to the outsourcing services under the Agreement and/or the Work Order shall be the PRC law. The Supplier hereby agrees that the court of place where Citi is located shall have the exclusive jurisdiction over any dispute in connection with the outsourcing hereunder.²³

¹⁵ Article 3 of IT Outsourcing Guidelines (科技外包指引)

¹⁶ Article 21.1 of IT Outsourcing Guidelines (科技外包指引)

¹⁷ Article 21.10 of IT Outsourcing Guidelines (科技外包指引)

¹⁸ Article 32.2 of IT Outsourcing Guidelines (科技外包指引)

¹⁹ Article 21.2 of IT Outsourcing Guidelines (科技外包指引)

²⁰ Article 21.6 of IT Outsourcing Guidelines (科技外包指引)

²¹ Article 21.7, 31.2 of IT Outsourcing Guidelines (科技外包指引)

²² Article 21.8 of IT Outsourcing Guidelines (科技外包指引)

²³ Article 21.9 of IT Outsourcing Guidelines (科技外包指引)

- 1.2.7 Supplier shall submit Appendix B Specified Requirements for Disaster Recovery Plan / Continuity of Business Plan to Citi within certain days as specified under relevant Work Order upon execution of the relevant Work Order.²⁴
- 1.2.8 Supplier agrees to procure the execution of the Confidentiality and Secrecy Undertaking in the form specified in Appendix C by each of the personnel appointed or to be appointed to perform the Services or part thereof for and on behalf of Supplier.²⁵
- 1.3 Special Requirements if the Information Technology Outsourcing further constitutes Non-Stationed Information Technology Outsourcing (as defined below)
 - 1.3.1 Non-Stationed Information Technology Outsourcing²⁶.
Non-stationed Information Technology Outsourcing refers to the Information Technology Outsourcing where the Supplier is not required to provide on-site services at Citi's location.
 - 1.3.2 If the Service constitutes Non-stationed Information Technology Outsourcing, besides the requirements provided in Section A.2-1.2 above, the following provisions shall apply:²⁷
 - 1.3.2.1 The system resource of the Supplier allocated to Citi shall be separated from the resource allocated to the Supplier's other customer(s) in terms of system logic, and only Citi has the highest authority to access to the system and data related to Citi, which shall not be accessible by other customer of the Supplier.
 - 1.3.2.2 The Supplier shall have management systems and technical measures to ensure the integrity and confidentiality of Citi's data.
 - 1.3.2.3 The Supplier undertakes that for the purposes of the Service, it will not conduct unfair competition or circumvention the supervision by regulators.
- 1.4 Special Requirements for the Information Technology Outsourcing of Level2 & Level3 System Development²⁸
 - (1) If the Supplier provides outsourcing service of Level3 system development to Citi, before the delivery of the Service, the Supplier shall provide the source code or review report of the source code to Citi to ensure no back door and convert channel vulnerability issues therein.

B. Special Requirements if the information technology activity involves processing of Important Data or Personal Information (APPLICABLE TO CCCL ONLY)

- 1.1 If the information technology activity between Citi and the Supplier involves the processing of Important Data (as defined below) or Personal Information (as defined in Section C-1.1) of Citi's clients, the requirements under Section A.2 above shall also apply²⁹. Important Data refers to the data covering specific fields, specific groups, or specific regions or with certain accuracy and scale, which, once being tampered with, destroyed, divulged, illegally obtained or illegally used, may directly endanger national security, economic operation, social stability, or public

²⁴ Article 31.3 of IT Outsourcing Guidelines (科技外包指引)

²⁵ Article 32.1 of IT Outsourcing Guidelines (科技外包指引)

²⁶ Article 44 of IT Outsourcing Guidelines (科技外包指引)

²⁷ Article 18 of IT Outsourcing Guidelines (科技外包指引)

²⁸ Section 8.1.9.5 of PBOC Implementation guidelines for classified protection of cybersecurity of financial industry ("PBOC Implementation Guidelines") (关于落实网络安全保护重点措施深入实施网络安全等级保护制度的指导意见). The criteria of "Level3 System" should refer to PBOC Implementation Guidelines.

²⁹ Article 3 of IT Outsourcing Guidelines (科技外包指引)

health and security³⁰. The specific catalogue of Important Data is subject to issuance by competent departments of respective region and industry.³¹

C. Protection of Personal Information

C.1 General Provisions

- 1.1 “Personal Information” refers to a variety of information related to an identified or identifiable natural person that is recorded electronically or otherwise, excluding anonymized information,³² including but not limited to the personal financial information as defined in Section C-1.2.
- 1.2 **(APPLICABLE TO CCCL ONLY)** Personal information relating to Citi’s customer shall include personal financial information (“**PFI**”), which includes account information, identification information, financial transaction information, personal identification information, property information, loan information, and other information that reflects certain circumstances of specific personal financial information subjects, details are as follows³³:
- (1) Account information refers to account and account-related information, including but not limited to payment account number, bank card magnetic track data (or equivalent information such as chips, etc.), bank card validity period, security account, insurance account, account opening time, account opening institution, and account balance and payment markup information generated from the aforementioned information.
 - (2) Identification information refers to information used to verify whether the subject has the authorization to access or use, including but not limited to bank card passwords, prepaid card payment passwords; login passwords, account inquiry passwords, and transaction passwords of the Citi’s customer; card verification codes (CVN and CVN2), one-time passwords, SMS verification codes, password recovery question answers, etc.
 - (3) Financial transaction information refers to various types of information generated by Citi’s customers during the transactions, including but not limited to transaction amounts, payment records, overdraft records, transaction logs, transaction vouchers; securities entrustment, trading, position information; insurance policy information, insurance claim information, etc.
 - (4) Personal identity information refers to basic personal information, personal biometric information, etc.;
 - Basic personal information includes, but is not limited to, the Citi’s customer’s legal name, gender, nationality, ethnicity, occupation, marital status, family status, income status, ID card and passport and other credentials, mobile phone number, fixed phone number, email address, job and home address, and photos, audio and video information collected in the course of providing products and services;
 - Personal biometric information includes, but is not limited to, fingerprint, face, iris, ear print, palm print, vein, voiceprint, eye print, gait, handwriting and other biometric sample data, eigenvalues and templates.

³⁰ Article 62, Para 1, Item 4 of Regulation on Network Data Security Management (网络数据安全条例)

³¹ Article 21 of Data Security Law of the People's Republic of China (中华人民共和国数据安全法)

³² Article 4 of the PRC Personal Information Protection Law (中华人民共和国个人信息保护法)

³³ Article 4.1 of the Personal Financial Information Protection Technical Specification (个人金融信息保护技术规范)

- (5) Property information refers to the property information of Citi's customer collected or generated by the Citi in the course of providing financial products and services, including but not limited to personal income status, real estate ownership information, vehicle ownership information, tax amount, and accumulated fund payment amount, etc.
 - (6) Loan information refers to the information generated in the course of Citi's lending business with Citi's customer, including but not limited to, facility granting, credit card and loan granting, repayment, guarantee, etc.
 - (7) Other information:
 - Information generated by processing, analyzing of raw data, which can reflect certain circumstances of a particular individual, including but not limited to the consumption willingness, payment habits and other derived information of particular personal financial information subjects;
 - other personal information acquired and stored during the provision of financial products and services.
- 1.3 The Supplier agrees to take effective measure to protect the Personal Information obtained through the provision of the Service, ensure information security, confidentiality and avoid unauthorized disclosure or misuse during the collection, transmission, processing, storage and usage of such Personal Information.³⁴
- 1.4 **(APPLICABLE TO CCCL ONLY)** Upon the termination of the Agreement and/or the relevant Work Order, the Supplier shall destroy or return to Citi, subject to Citi's instruction, all personal financial information of Citi's customer obtained through providing the Services to Citi.³⁵
- 1.5 **(APPLICABLE TO CCCL ONLY)** Notwithstanding anything in the Agreement and/or the relevant Work Order to the contrary, without the Citi's consent, the Supplier shall promptly (within 24 hours) destroy the PFI which is categorized into C2 and C3 (as specified below³⁶). For the minimum PFI that indeed need to be retained in accordance with provisions and requirements of laws and regulations or out of the necessity of provision of the Services, the Supplier shall protect the retained data and implement security control measures and file relevant documents for inspection.
- 1) C3 category of PFI mainly refers to user identification information. Unauthorized access or alternation to such information will cause significant harm to the information security and property security of Citi's customer. C3 category of PFI including but not limited to:
 - bank card magnetic track data (or equivalent information such as chips) , card verification codes (CVN And CVN2), bank card validity period, bank card passwords, online payment transaction passwords;
 - account (including but not limited to payment account, security account, insurance account) login passwords, transaction passwords, inquiry passwords;
 - personal biometric information for identifying users;
 - 2) C2 category of PFI mainly refers to PFI that can identify a particular personal financial information subject and his/her financial status, and key information used for financial product and service. Unauthorized access or alternation to such information will cause

³⁴ Article 19.2 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

³⁵ Article 19.2 of Guidelines on Control of Outsourcing Risks of Banking Financial Institutions (银行业金融机构外包风险管理指引)

³⁶ Article 4.2 of the Personal Financial Information Protection Technical Specification (个人金融信息保护技术规范)

certain harm to the information security and property security of Citi's customer. C2 category of PFI including but not limited to:

- payment account and its equivalent information. Such as payment account, ID identification mark and ID information (ID card, passport, etc.), mobile phone number.
- Account (including but not limited to payment account, security account, insurance account) login username;
- User identification supplementary information, such as one-time passwords, SMS verification codes, password recovery question answers, one-time voice print passwords; if the user identification supplementary information upon combination use with the account can directly identify a user, then such user identification supplementary information belongs to C3 category of PFI.
- Information that directly reflects the PFI subject's financial status, such as personal property information (including internet payment account balance), loan information
- Critical information used for financial products and services, such as transaction information (such as transaction instruction, transaction bills, security entrustment, insurance claims) etc.;
- Media information such as photos, audios, videos of PFI subject collected during provision of products and services for compliance with Know Your Customer requirements or required by industrial regulators for the use of evidence documentation, preservation, etc.
- Other information that can identify a particular subject, such as home address, etc.

Note: C2, C3 categories of PFI refer to the categorization under the Personal Financial Information Protection Technical Specification.

- 1.6 Informed Consent of Personal Information Subjects. When the Supplier discloses any Personal Information to Citi in connection with the Services provided to Citi, the Supplier shall warrant and undertake that it had informed the Personal Information subjects of Citi's name, contact information, processing purpose, methods and the type of Personal Information to be processed, and the applicable Citi Privacy Statement (accessible at the address below or any Customer-specified URL <https://www.citigroup.com/rcs/citigpa/storage/public/Citi-Non-Employee-Supplier-Online-Privacy-Notice.pdf>) or other applicable privacy policy and obtained consent from such Personal Data Subjects in accordance with the applicable laws and regulations, and prior consent of Personal Information subjects of Personal Information disclosed to Citi have been obtained by the Supplier, for the Supplier to disclose their Personal Information to Citi to further process in connection with the Services.³⁷
- 1.7 The Supplier shall process Personal Information according to the Agreement and/or the Work Order agreement, refrain from processing Personal Information beyond the agreed purposes, methods, etc. of processing. The Supplier shall return the Personal Information to Citi or delete the same, and shall not keep the Personal Information where the contract fails to take effect, is invalid or is cancelled or terminated. Without Citi's prior written consent, Supplier shall not further entrust others to process Personal Information.³⁸
- 1.8 Personal Information Outbound Transfer. In principle, the Personal Information disclosed by the Supplier to Citi will be stored inside China. However, for purposes of the Services, such Personal Information may be transferred by Citi to, or accessed from, offshore jurisdictions of Citi's affiliates or other suppliers. Please see the table (CCCL: accessible at <https://www.citibank.com.cn/rcs/citi-china/storage/public/BusinessInformationandServices/CH/BusinessInformationandServices/CN-gysxgwj.pdf>; Citigroup Services and Technology (China) Limited: accessible at <https://www.citibank.com.cn/rcs/citi-china/storage/public/BusinessInformationandServices/CH/BusinessInformationandServices/gysxgwj-CSTC.pdf>) for the name, contact information of the overseas recipient, and types of

³⁷ Article 13 and 17 of the PRC Personal Information Protection Law (中华人民共和国个人信息保护法)

³⁸ Article 21 of the PRC Personal Information Protection Law (中华人民共和国个人信息保护法)

Personal Information to be transferred or accessed outbound as well as the processing measures and purposes as well as the method and procedure for personal information subjects to exercise the rights against of overseas recipients. In compliance with the notification period and method requirements under applicable laws and regulations (if any), Citi will inform the Supplier of the update of the aforementioned contents in a timely manner in the form of public announcement on the website (currently: CCCL: <https://www.citibank.com.cn/rcs/citi-china/storage/public/BusinessInformationandServices/CH/BusinessInformationandServices/CN-gysxgwj.pdf>; Citigroup Services and Technology (China) Limited: <https://www.citibank.com.cn/rcs/citi-china/storage/public/BusinessInformationandServices/CH/BusinessInformationandServices/gysxgwj-CSTC.pdf>). The Supplier presents and undertakes that it had effectively notified and gained separate consent from the Personal Information subjects re the Personal Information outbound transfer issues. In the event of subsequent updates regarding the outbound transfer of Personal Information, the Supplier will also promptly inform the relevant Personal Information subject of the updated situation and obtain their separate consent again.³⁹

In the event that the Supplier may further transfer Personal Information disclosed by Citi to its affiliates or an associated service provider agreed by Citi outside of PRC, the Supplier presents and undertakes that it had complied or will comply with the applicable Personal Information Cross-border compliance requirements, namely, (a) data export security assessment, (b) standard contract filing, or (c) personal information protection certification.⁴⁰

C.2 **PROVISIONS WHICH APPLY WHERE THERE IS A CROSS-BORDER DATA TRANSFER FROM CITI THAT IS LOCATED IN CHINA TO THE SUPPLIER THAT IS LOCATED OUTSIDE OF CHINA⁴¹.**

Notwithstanding any provision to the contrary in this Schedule, Section C.2 shall apply if there is any cross-border Personal Information **and/or Important data** transfer from Citi (the “**Data Controller**” in this Section) to the Supplier outside the PRC (the “**Overseas Recipient**” in this Section).

I. **DEFINITIONS AND INTERPRETATION**

1. In Section C.2 of this Schedule, unless the context otherwise requires:

1.1 “**Data Controller**” refers to the entity that independently decides on the purposes and methods of processing during **Data** processing activities;

1.2 “**Overseas Recipient**” refers to organizations or individuals located outside of the People's Republic of China and receiving **Data** from the Data Controller;

1.3 “**Data**” refers to any record of information in electronic or any other form⁴²

1.4 “**Data Subject**” refers to the individuals identified or associated with the Personal Information, as well as the legal persons and/or individuals identified or associated with the Important Data;

³⁹ Article 39 of the PRC Personal Information Protection Law (中华人民共和国个人信息保护法)

⁴⁰ Article 38 of the PRC Personal Information Protection Law (中华人民共和国个人信息保护法) and Article 5 of the Regulations on Promoting and Regulating Cross-border Data Transfers (促进和规范数据跨境流动规定)

⁴¹ Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

⁴² Article 3 of Measures for the Data Security Management of Banking and Insurance Institutions (银行保险机构数据安全管理办法)

- 1.5 "Data Leakage" refers to any accidental or illegal destruction, loss, tampering, leakage, transfer or unauthorized provision access or use in relation to Data;

II. OBLIGATIONS OF THE PARTIES

1. The Overseas Recipient hereby represents, warrants and undertakes as follows:
 - 1.1 Data shall be processed according to the corresponding Work Order and applicable laws and regulations;
 - 1.2 In case of Data Leakage of the Data processed, it will⁴³:
 - (a) timely take appropriate action to enable the Data Controller to take remedial measures to reduce any adverse impact on the Data Subject;
 - (b) inform the Data Controller immediately and assist the Data Controller in its efforts to report to the Regulatory Authorities of the People's Republic of China and/or to notify the Data Subject in accordance with Applicable Laws.
 - 1.3 When there is any material change in the actual control or business scope of the Overseas Recipient, any material change in the data security protection policies, regulations and cybersecurity environment, or any occurrence of other force majeure events in the country or region where the Overseas Recipient is located which makes it difficult to ensure data security, the Overseas Recipient shall immediately notify the Data Controller of the changes and timely take appropriate remedial measures to reduce the adverse impact on the Data Subject⁴⁴;
 - 1.4 It will not provide any Data to a third party outside the People's Republic of China unless so instructed by the Data Controller, or as otherwise agreed in the Agreement.⁴⁵
 - 1.5 The Overseas Recipient shall not further transfer Data to any third party to process the Personal Information, unless the Data Controller obtains the consent of the Data Subject and provides written instruction (including via the Work Order or as otherwise agreed in the Agreement) to the Overseas Recipient to undertake such transfer⁴⁶.
2. The Data Controller and the Supplier shall ensure that the corresponding Work Order will specify the items listed in Appendix D "Details of Cross-border Transfer of Data".

III. PROTECTION OF DATA SUBJECTS

1. Data Controller acknowledges that the Data Subject, in accordance with Applicable Law, has the right to be informed and to make decisions on the processing of their Personal Information, the right to restrict or refuse the processing of their Personal Information by others, the right to request access to, copy, correct, supplement or delete their Personal Information, and the right to request an explanation of the rules governing the processing of their Personal Information.

⁴³ Subparagraph 6 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

⁴⁴ Subparagraph 4 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

⁴⁵ Subparagraph 3 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

⁴⁶ Subparagraph 3 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

2. When the Data Subject requests the exercise of the aforementioned rights in respect of Personal Information that has transferred outbound, the Data Subject may request the Data Controller to take appropriate measures to realize the inquiries. If the Data Controller is unable to achieve this, it shall notify and request the Overseas Recipient for assistance. The Overseas Recipient will provide reasonable assistance and cooperation with the Data Controller in handling the inquiries or complaints from the Data Subject within a reasonable period of time as per the applicable regulation.
3. If the Overseas Recipient is unable to assist and cooperate with the Data Controller in responding to the Data Subject's inquiries, it shall inform the Data Controller of the reasons. The Data Controller shall inform the Data Subject of the channels available to file a complaint with the Regulatory Authorities and to seek judicial remedies.

IV. TERMINATION⁴⁷

1. If the Overseas Recipient violates its obligations under Section C.2, the Data Controller may suspend the transmission of Data to the Overseas Recipient until the breach is corrected or the engagement between the Data Controller and the Overseas Recipient is terminated.
2. In case of any of the following circumstances, the Data Controller has the right to terminate the engagement between itself and the Overseas Recipient, and to notify the Government Body when necessary:
 - (a) the Data Controller has suspended the transmission of Data to the Overseas Recipient for more than one month in accordance with the provision of Section C.2-IV-1;
 - (b) the Overseas Recipient's compliance with Section C.2 of this Schedule will violate the laws and regulations of the country where it is located;
 - (c) the Overseas Recipient seriously or continuously violates its obligations under Section C.2 of this Schedule;
 - (d) the Overseas Recipient or Data Controller violates the provisions of Section C.20 of this Schedule according to the final decision of the competent court or regulatory body of the Overseas Recipient, which cannot be appealed;

In the case of item (a), (b) or (d) above, the Overseas Recipient may also terminate the engagement between itself and the Data Controller.

3. If the Government Body makes a decision that the Cross-border Transfer of Data is not in accordance with the applicable Laws and Regulations, such Data Cross-border Transfer security assessment, either party may terminate the engagement.
4. When the agreed Data retention period is reached, the Data processing purpose of the engagement is fulfilled, and/or the engagement is terminated, the Overseas Recipient shall comply with the relevant provisions in the Agreement with respect to return of Data, that to return (or purge its systems and files of, and suitably account for) all Confidential Information supplied to, or otherwise obtained by, the Supplier in connection with an Agreement and/or Work Order.⁴⁸

⁴⁷ Subparagraph 5 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

⁴⁸ Subparagraph 2 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

V. LIABILITY FOR BREACH⁴⁹

1. The party shall be liable to the other party for any damage caused to the other party due to its breach of Section C.2 of this Schedule.
2. The liability of the breaching party is limited to the losses suffered by the non-breaching party.
3. For any material or non-material damage caused to the Data Subject, each party who violates the rights of the Data Subject due to the violation of Section 0 shall be liable to the Data Subject. The Data Subject has the right to claim for compensation.
4. The Data Controller has the right to get indemnified by the Overseas Recipient for any losses, liability or expense which the Data Controller may suffer, directly or indirectly, in connection with any breach by the Overseas Recipient of its obligations under Section C.2.

VI. DISPUTE RESOLUTION⁵⁰

Section C.2 of this Schedule shall be governed by the law of and subject to the exclusive jurisdiction in the country/region where the Data Controller is established.

D. Special Requirements under Cybersecurity Law and Data Security Law

- 1.1 If the Supplier constitutes a provider of network products or service under the PRC Cybersecurity Law, the Supplier shall comply with all applicable requirements thereunder, including but not limited to⁵¹:
- (1) providing network products or service that satisfy the compulsory requirements of relevant national standards;
 - (2) not setting up malwares in the network products or service it provides;
 - (3) promptly notifying Citi and timely verify the security bug and complete the remediation and reporting to the competent authority if the Supplier finds the network products or service provided to Citi have security defects, bugs or other risks; if the security vulnerability relating to the Service cannot be remediated in a timely manner, Service Provider shall conduct impact assessment and risk mitigation according to its internal process, and report the assessment results and risk mitigation status to Citi in a timely manner;⁵²
 - (4) continuously providing security maintenance for the network products and service provided to Citi and not discontinuing the security maintenance during the term of service;
 - (5) explicitly indicating to users and obtaining prior consent of users if the network products or service provided by the Supplier have the function of collecting users' information, and where personal information of users is involved, complying with relevant provisions governing the protection of personal information under the Cybersecurity Law and other PRC laws and administrative regulations.

⁴⁹ Subparagraph 5 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

⁵⁰ Subparagraph 5 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)

⁵¹ Article 22 of the PRC Cybersecurity Law (中华人民共和国网络安全法)

⁵² Article 8 of the Provisions on the Management of Security Vulnerabilities of Network Products (网络产品安全漏洞管理规定)

1.2 If the Supplier provides critical network equipment or dedicated cybersecurity products⁵³ to Citi, such equipment or products shall pass the security certification or security tests conducted by qualified institutions in accordance with the compulsory requirements of relevant national standards.⁵⁴

1.3 If the Supplier constitutes a network provider under the PRC Cybersecurity Law, it shall adopt the technical measures for monitoring and recording the network's operation status and the cybersecurity incidents and keeping relevant network logs for at least 6 months in accordance with relevant requirements.⁵⁵

1.4 Any data processing activities associated with the Services carried out by the Supplier shall be conducted in accordance with the applicable laws and regulations, with a sound full-process data security management system. The Supplier shall, among others, take necessary technical to ensure data security. When data processing activities are carried out through the internet and other information networks, the above-mentioned data security protection obligations shall be fulfilled based on the network security level protection system.⁵⁶

1.5 The Supplier shall strengthen risk monitoring during the data processing activities associated with the Services. When risks such as data security defects and loopholes are discovered, remedial measures should be taken immediately. When a data security incident occurs, disposal measures should be taken immediately, and the Supplier shall inform Citi in a timely manner.⁵⁷

1.6 The Supplier shall comply with legal and legitimate methods in collecting data associated with the Services and shall not steal or obtain such data by other illegal means. Where relevant laws and administrative regulations have provisions on the purpose and scope of the collection and use of such data, such laws and administrative regulations shall be complied with.⁵⁸

E. Cloud Computing Services (APPLICABLE TO CCCL ONLY)

1.1 The Supplier that provides cloud computing services to Citi for important information systems shall satisfy the following conditions:

- (1) pass the banking industry cloud service provider assessment, and obtain the bank industry cloud computing certificate issued by the regulatory authorities or the institution(s) recognized by relevant PRC regulatory authorities;
- (2) adopt the SM (domestic) Algorithm for encryption. "SM Algorithm" herein refers to the PRC national standard SM4 block cipher algorithm; and
- (3) obtain the certificate of level 3 or better in accordance with the "Banking Industry IT System Security Classified Protection Assessment".

The aforesaid "important information system" refer to the system that its system failure may cause Citi's clients' fund losses or leakage of clients' personal information.

F. Information Security (APPLICABLE TO CCCL ONLY)

1.1 If the Supplier provides wireless network service on behalf of Citi, the Supplier shall be responsible for the security of the wireless network. The Supplier shall provide wireless network

53 The definition and scope of "critical network equipment or dedicated cybersecurity products" shall refer to the Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products formulated and promulgated by the Cyberspace Administration of China and relevant departments under the State Council.

54 Article 23 of the PRC Cybersecurity Law (中华人民共和国网络安全法)

55 Article 21.3 of the PRC Cybersecurity Law (中华人民共和国网络安全法)

56 Article 27 of the PRC Data Security Law (中华人民共和国数据安全法)

57 Article 29 of the PRC Data Security Law (中华人民共和国数据安全法)

58 Article 32 of the PRC Data Security Law (中华人民共和国数据安全法)

security assessment reports or other equivalent documents as approved by Citi on an annual basis and shall ensure the wireless network is in good function at any time.⁵⁹

- 1.2 Voiceprint recognition based design, development, testing, application and risk control for mobile finance service shall comply with the specifications provided in the PBOC Notice on Release of Financial Industry Specifications - Standardizing the Application of Voiceprint Recognition Technology in China's Financial Industry (YinFa No. [2018] 235).
- 1.3 The transfer, copy and migration of data from production environment to non-production environment can only be carried out upon prior consent from Citi.⁶⁰
- 1.4 If the Supplier provides information products and services, the Supplier shall cooperate with Citi's investigation on its security capabilities, assume security responsibilities, and provide Citi with a list of third-party or open source components involved in software products. When third-party or open source components have security vulnerabilities, Supplier should provide necessary technical support.⁶¹

G. Technology (APPLICABLE TO CCCL ONLY)

- 1.1 If the Supplier uses open source technology to provide services, the Supplier shall ensure that the open source technologies they use are legal and compliant, comply with relevant national and industry standards (if applicable), and can provide open source technology evaluation reports according to Citi's requirements.⁶²

H. Citi's Customers' Rights and Interests Protection

- 1.1. The Supplier shall take effective consumer rights protection measures, including but not limited to establishing respective consumer rights protection policies to ensure the Supplier to perform the Services in accordance with the consumer rights protection policy. The Supplier shall, upon Citi's request, cooperate with Citi to conduct consumer rights protection assessment on the Supplier and regularly submit complaint management data report to Citi.⁶³
- 1.2. The Supplier shall not charge the Citi's customer in the name of Citi. Citi has the right to understand what the Supplier charges Citi's customer, and the Supplier shall not charge the Citi's customer excessively high.⁶⁴
- 1.3. If the Supplier is an Internet platform or other cooperative institution to Citi, Supplier shall not charge Citi's customers any fees in the name of Citi, and both parties should agree in the

⁵⁹ Article 8 of the Notice by the General Office of the China Banking and Insurance Regulatory Commission of Strengthening the Administration of Wireless Network Security (中国银保监会办公厅关于加强无线网络安全管理的通知)

⁶⁰ Article 22 of Measures for the Commissioning and Change of Important Information Systems of Banking Institutions (银行业金融机构重要信息系统投产及变更管理办法)

⁶¹ Letter on Supply Chain Security Risk Warning (关于供应链安全风险提示的函 (银保监统信函【2021】371号))

⁶² Article 12 of Opinions on Regulating the Application and Development of Open Source Technology in the Financial Industry (关于规范金融业开源技术应用与发展的意见第12条)

⁶³ Article 2.3.7 of the Guiding Opinions of the China Banking and Insurance Regulatory Commission on Banking and Insurance Institutions Strengthening the Building of Working Systems and Mechanisms for Protection of Consumer Rights and Interests (中国银保监会关于银行保险机构加强消费者权益保护工作体制机制建设的指导意见). If the Supplier is engaged in consumer facing activities, this clause shall be kept.

⁶⁴ Article 5 of the Notice by the China Banking and Insurance Regulatory Commission, the Ministry of Industry and Information Technology, the National Development and Reform Commission, the Ministry of Finance, and the State Administration for Market Regulation of Further Regulating Charges for Credit Financing and Reducing the Comprehensive Financing Costs of Enterprises (中国银保监会、工业和信息化部、发展改革委、财政部、人民银行、市场监管总局关于进一步规范信贷融资收费 降低企业融资综合成本的通知). If the Supplier relates to credit financing product services and engaged in corporate customer facing activities, this clause needs to be retained.

Framework Documents of the information disclosure requirements of service price, dispute resolution responsibilities and obligations among the Supplier, Citi and Citi's customers.⁶⁵

- 1.4. The Supplier shall cooperate with Citi to strictly prevent and control information disclosure risks of Citi's customers and protect the information security of Citi's customers.⁶⁶
- 1.5. The Supplier shall not carry out or participate in any part of illegal activities in any method (including but not limited to securities activities) using the name of Citi.

**I. Special Requirements under PRC Securities and Futures Laws and Regulations
(APPLICABLE TO CSRC REGULATED ENTITIES ONLY)**

- 1.1. The Qualified Supplier shall build up a well-established internal quality control mechanism, monitor relevant products or services on a periodical basis, and if there is any evident quality problem during the provision of relevant products or services, it shall immediately verify the relevant information, take necessary handling measures, specify the time limit for the completion of recovery, and complete the recovery work in a timely manner.⁶⁷
- 1.2. The Qualified Supplier confirms that it has built up a well-established cybersecurity and information security management system, appointed appropriate security and compliance management personnel, and established a cybersecurity and information security management mechanism which is compatible with the provision of the relevant products or services to Citi.⁶⁸
- 1.3. The Qualified Supplier acknowledges that when any abnormal circumstance occurs to it, as required by the applicable laws and regulations, Citi may conduct internal assessment and examination according to its emergency response plan; and if it turns out that the relevant products or services loss its features of availability, integrity, or confidentiality as a result of the Qualified Supplier's short of capability, Citi may replace the Qualified Supplier in a timely manner.⁶⁹
- 1.4. The Qualified Supplier acknowledges and agrees that for any product or service provided to Citi, there shall a written product/service agreement and confidentiality agreement between Citi and the Qualified Supplier, in which terms required by applicable laws and regulations shall be included, such as the rights, obligations and responsibilities of all parties, and the quality assessment standards, continuous monitoring mechanism, the abnormal circumstances handling mechanism, service change or termination disposal process, confidentiality requirements for on-site service providers. And Citi has the right to continuously oversee the implementation of such agreements.⁷⁰

⁶⁵ Article 19 of CBIRC Guiding Opinions on Regulating the Administration of Adjusted Prices in the Banking Service Market (中国银保监会关于规范银行服务市场调节价管理的指导意见)

⁶⁶ Article 3(10) of Guiding Opinions of the General Office of the State Council on Strengthening the Protection of Financial Consumers' Rights and Interests (国务院办公厅关于加强金融消费者权益保护工作的指导意见)

⁶⁷ Article 50 of Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions (证券基金经营机构信息技术管理办法)

⁶⁸ Article 9 of Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (证券期货业网络和信息安全管理办法)

⁶⁹ Article 46 of Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions (证券基金经营机构信息技术管理办法)

⁷⁰ Article 45 of Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions (证券基金经营机构信息技术管理办法)

- 1.5. If the Qualified Supplier identifies any security defects, loopholes and other latent risks and dangers in cybersecurity and information security products or services, it shall conduct verification, reinforcement and rectification in a timely manner; and if such latent risks and dangers would bring significant impact to the secure and stable operation of networks and information in the securities and futures industries, the Qualified Supplier shall report to CSRC.⁷¹
- 1.6. In facing any cybersecurity incidents, the Qualified Supplier shall assist in troubleshooting and repair of the information system failures and cooperate with the risk troubleshooting and rectification in a timely manner.⁷²
- 1.7. When receiving industry notification and early warning on relevant security defects, security loopholes and other latent risks and dangers from CSRC, the Qualified Supplier shall investigate and take risk prevention measures in a timely manner.⁷³
- 1.8. The Qualified Supplier shall cooperate with the inspection and investigation made by CSRC.
- 1.9. The Qualified Supplier confirms that it will not:⁷⁴
 - (1) participate in any part of securities and futures business services provided by Citi or release any information that may cause misunderstanding of Citi's securities business to investors and the public;
 - (2) intercept, store, forward or use business data or client's information relating to Citi's securities and futures business activities;
 - (3) entrust a third party to provide the relevant products or services when Citi is unaware of;
 - (4) provide relevant products or services with relevant functions, operating procedures, system authority and parameter configuration which is in violation of any existing law or regulations;
 - (5) close system interface or set technical barrier without any justifiable reasons;
 - (6) disclose information security loopholes, information system stress testing results or any other network security information, or leak any non-public information to the public; or
 - (7) carry out any other activities prohibited by applicable laws and regulations.
- 1.10. As to the products and services related to the securities business, the Qualified Supplier confirms that it has complied and will comply with the applicable filing and reporting obligations and procedures as required by CSRC from time to time and provide true, accurate and complete data and information. The Qualified Supplier further acknowledges that Citi may conduct internal examination of the Qualified Supplier and relevant information systems in accordance

⁷¹ Article 36 of Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (证券期货业网络和信息安全管理办法)

⁷² Article 39 of Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (证券期货业网络和信息安全管理办法)

⁷³ Article 58 of Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (证券期货业网络和信息安全管理办法)

⁷⁴ Article 51 of Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions (证券基金经营机构信息技术管理办法)

with applicable laws and regulations and submit examination reports and relevant materials to CSRC.⁷⁵

- 1.11. As to the products and services related to the futures business, the Qualified Supplier acknowledges that the provision of information technology system services for futures trading and relevant activities shall comply with the applicable technical management provisions and standards relating to information security issued by PRC futures regulators, and the Qualified Supplier confirms that it has complied and will comply with the filing and reporting obligations and procedures as required by CSRC from time to time.⁷⁶

The Qualified Supplier further acknowledges that CSRC may require the disclosure of the materials on information technology systems as provided in the Services and it shall and provide true, accurate and complete data and information as required.

- 1.12. Under this Section,⁷⁷

- (1) a *Qualified Supplier* refers to IT system service provider that provides products or services such as development, testing, integration, evaluation, operation and maintenance, and routine safety management of *important information systems* for securities and futures business activities as stipulated in the *Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries* (《证券期货业网络和信息安全管理办法》) and *Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions* (《证券基金经营机构信息技术管理办法》) and other rules and regulations CSRC may issue from time to time.
- (2) *Important information systems* refer to information systems that carry key business activities in the securities and futures industries and whose abnormal system services, data leakage, and other circumstances will have a *significant impact* on the securities and futures markets and investors.
- (3) *Significant impact* refers to circumstance under which a cybersecurity incident of relatively large level or above may be triggered according to the relevant measures for the investigation and handling of cybersecurity incidents.
- (4) CSRC refers to China Securities Regulatory Commission (being CSRC) and its branches (including its successor).

- 11.1 The Qualified Supplier will comply, and will cause any directors, officers, employees, agents, auditors, consultants or other representatives of the Qualified Supplier to comply, with all applicable laws and regulations related to the PRC securities and futures industry or issued by CSRC.

⁷⁵ Articles 44 and 47 of Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions (《证券基金经营机构信息技术管理办法》), Article 9 of Provisions on the Administration of Filing of Securities Service Institutions Engaging in Securities Services (《证券服务机构从事证券服务业务备案管理规定》) and Articles 23, 57 and 72 of Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (《证券期货业网络和信息安全管理办法》)

⁷⁶ Article 101 of Futures and Derivatives Law (《期货和衍生品法》) and Articles 23, 57 and 72 of Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (《证券期货业网络和信息安全管理办法》)

⁷⁷ Article 3 of Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions (《证券基金经营机构信息技术管理办法》) and Article 71 of Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (《证券期货业网络和信息安全管理办法》)

J. Governing Law and Jurisdiction

- 1.1. Where both Citi and Supplier are entities incorporated in China, the governing law shall be the PRC law, and all claims or disputes arising out of or in connection with Agreement and/or the relevant Work Order shall be submitted to the PRC court where Citi is located.

[Appendix A – Memorandum of Understanding List \(subject to updates from National Financial Regulatory Administration \(NFRA\) from time to time\)](#)

Appendix B

SPECIFIED REQUIREMENTS for DISASTER RECOVERY PLAN / CONTINUITY OF BUSINESS PLAN

CoB Header Information

CoB Entity ID	
CoB Entity Name	
CoB Process ID(s)	
CoB Process Name(s)	
Primary Site	
Alternate Site(s)	

CoB Requirements and Strategy

In addition to the requirements set forth in the [Agreement] and in the Citi Standards for Suppliers, during a CoB event, defined as any event that would prevent the Supplier from performing the Services at 100% capacity, the Supplier is required to, at a minimum, meet the requirements stated hereunder in their entirety, including, but not limited to, the volume of transactions set forth in the column titled "Recovery Capacity" and within the Recovery Time Objective (RTO) specified.

Citi shall permit the Supplier the relaxations during a CoB event as specified in the column titled "SLA Relaxation". Further changes to SLAs may be mutually agreed in writing with the Citi manager responsible for this SOW.

Supplier is required to specify the Site and City CoB Strategies for each activity/service/process below so as to meet these requirements (please add rows as applicable). If the information technology activity between Citi and the Supplier involves the processing of Important Data or Personal Information of Citi, and if the Service constitutes important outsourcing service and may cause significant impact to the management of CoB, the priority level for responding and recovery should be the highest in principle.

#	Services / Processes (Citi to specify)	Criticality & RTO (Citi to specify)	Recovery Capacity (Citi to specify)	SLA Relaxati on (Citi to specify)	CoB Strategy – Site Outage (Supplier to specify)	CoB Strategy – City Wide Outage (Supplier to specify)
01		☐ Franchise Critical: 4 hours or less ☐ Criticality 1: 4 hours or less ☐ Criticality 2: 4 to 24 hours ☐ Criticality 3: 24 to 72 hours ☐ Criticality 4: 72 hours to 30 days	☐ 0% ☐ 10% ☐ 20% ☐ 30% ☐ 40% ☐ 50% ☐ 60% ☐ 70% ☐ 80% ☐ 90% ☐ 100% ☐ Other – specify below	☐ None ☐ Other – specify below	☐ Split Operations ☐ Staff Transfer ☐ Work Transfer ☐ Return to Citi ☐ None (no CoB required)	☐ Split Operations ☐ Work Transfer ☐ Return to Citi ☐ None (no CoB required)

02		☐ Franchise Critical: 4 hours or less ☐ Criticality 1: 4 hours or less ☐ Criticality 2: 4 to 24 hours ☐ Criticality 3: 24 to 72 hours ☐ Criticality 4: 72 hours to 30 days	☐ 0% ☐ 10% ☐ 20% ☐ 30% ☐ 40% ☐ 50% ☐ 60% ☐ 70% ☐ 80% ☐ 90% ☐ 100% ☐ Other – specify below	☐ None ☐ Other – specify below	☐ Split Operations ☐ Staff Transfer ☐ Work Transfer ☐ Return to Citi ☐ None (no CoB required)	☐ Split Operations ☐ Work Transfer ☐ Return to Citi ☐ None (no CoB required)
----	--	---	---	---	--	--

Notes:

As used in the above table:

1. **Split Operations** means that the Supplier team providing services under this SOW will be evenly distributed across a minimum of two Supplier locations in different cities such that the Supplier resources located at each such location are able to provide adequate coverage for the other team so that the Supplier is able to meet all of the CoB requirements specified for this SOW.
2. **Staff Transfer** means that the Supplier will physically relocate the staff from the impacted location to an alternate location, which is not impacted nor is expected to be impacted by the ongoing CoB event, for the purpose of providing the required services for meeting the CoB requirements specified for this SOW.
3. **Work Transfer** means that the Supplier will transfer the responsibilities of performing the required services so as to meet the CoB requirements specified for this SOW to a backup team, not ordinarily part of the Supplier team providing services under this SOW, provided such a backup team is located in a different city and are adequately trained and kept updated on a regular basis so as to be able to perform such services.
4. **Return to Citi** means that the Supplier will transfer the responsibilities of performing the required services so as to meet the CoB requirements specified for this SOW back to Citi, provided that such an arrangement is agreed upon beforehand and documented under this SOW.

Recovery Duration

The Recovery Duration for all activities / services / processes is 30 calendar days or as specified in the Citi Standards for Suppliers, whichever is higher.

Recovery Point Objective (RPO)

The Supplier must recover all data that existed up until that point in time that is no earlier than the following amount of time (the “RPO”) prior to the applicable incident resulting in data loss:

(Citi to specify)

☐ RPO is Not Applicable – the Supplier is expected to not store anything outside the Citi environment

☐ The Supplier shall fulfill the below RPO

☐ 15 minutes

☐ 1 hour

☐ 4 hours

☐ 24 hours

CoB Strategy Testing Process

Suppliers must conduct CoB testing as per the applicable Citi Standards for Suppliers. This includes, but is not limited to, adherence to the applicable advance notice period, testing objectives and requirements, and test evidences.

(Supplier to specify)

First CoB test to happen within ☐60 / ☐90 / ☐120 days.

Type of Test	Frequency		
	(Supplier to specify)		
Simulation	☐ Annual	☐ Semi-Annual	☐ Never
Tabletop	☐ Annual	☐ Semi-Annual	☐ Never
Denial of Access (DoA)	☐ Annual	☐ Semi-Annual	☐ Never
Denial of Service (DoS)	☐ Annual	☐ Semi-Annual	☐ Never
Call Tree	☐ Annual	☐ Semi-Annual	☐ Never

APPENDIX C

CONFIDENTIALITY AND SECRECY UNDERTAKING (refer to Article 12.2.8)

(for Supplier's employees/agents/servants)

I, _____, acknowledge that ("Supplier") and _____⁷⁸ have entered into a Agreement and/or the relevant Work Order ("**Agreement**"). I have been advised by Supplier that under the Agreement, Supplier has agreed to treat certain information and materials received or otherwise obtained from Citi as confidential, and to exercise at least the same degree of care with respect to Citi's Confidential Information that Supplier exercises to protect its own confidential information from unauthorized disclosure or use. I have been further advised by Supplier that as a condition to my performing any services for Citi, I must agree, and I do hereby agree, to abide by the obligations of confidentiality assumed by Supplier, which include the following:

1. not to disclose Citi's Confidential Information, except to other employees of Supplier on a "need to know" basis and only to the extent necessary to fulfil Supplier's obligations under the Agreement;
2. not to reproduce Citi's Confidential Information in any media without the express written approval of Citi;
3. not to remove or transmit Citi's Confidential Information from Citi's premises without Citi's express prior written consent;
4. not to remove any copyright or other proprietary notice or indication of confidentiality contained on or included in any item of Citi's Confidential Information; and
5. not to reproduce any copyright or other proprietary notice or indication of confidentiality on any reproduction, modification or translation of such Confidential Information.

I agree that for purposes of this Confidentiality and Secrecy Undertaking, "Confidential Information" shall mean and include all tangible or intangible information and materials, in any form or medium (and without regard to whether the information is owned by Citi or by a third party), that is furnished or disclosed to Supplier or any of its personnel by Citi, or otherwise obtained by Supplier or any of its personnel from Citi.

By signing this Confidentiality and Secrecy Undertaking, I intend for both Supplier and Citi to rely upon my adherence to the obligation of confidentiality set forth above in permitting me to work on the project contemplated by the Agreement.

Signed by:

In the presence of:

Name: _____
NRIC or Passport No: _____
Nationality: _____
Date: _____

Name: _____
NRIC or Passport No: _____
Nationality: _____
Date: _____

⁷⁸ Please fill in the official name of the Citi entity

Appendix D

Details of Cross-border Transfer of Data⁷⁹

A. Personal Information- Please specify the details of cross-border transfer of Personal Information when Citi provides Personal Information outside of mainland China to overseas recipient (as the Supplier)

Scenario of Cross-border Data Transfer	Purpose of Cross-border Data Transfer/Processing	Manner of Cross-border Data Transfer	Scope/Type of Cross-border Data Transfer	Method of Processing Data by Overseas Recipients	Storage Location of Data after Cross-border Transfer	Data Storage Period after Cross-border Transfer	Volume of Cross-Border Data

B. Important Data - Please specify the details of cross-border transfer of Important Data when Citi provides Important Data outside of the mainland China to overseas recipient (as the Supplier):

Scenario of Cross-border Data Transfer	Purpose of Cross-border Data Transfer/Processing	Manner of Cross-border Data Transfer	Scope/Type of Cross-border Data Transfer	Method of Processing Data by Overseas Recipients	Storage Location of Data after Cross-border Transfer	Data Storage Period after Cross-border Transfer

⁷⁹ Subparagraph 1 and 2 of Article 9 of Measures of Outbound Data Transfer Security Assessment (数据出境安全评估办法)