

SCHEDULE N – SRI LANKA LAW REQUIREMENTS

(Version 8 – 11 March 2026)

The Bank has an obligation under the Common Law to keep the affairs of its customers confidential.

ADDITIONAL CLAUSES REQUIRED TO COMPLY WITH THE LAWS AND REGULATIONS APPLICABLE IN SRI LANKA

1. Outsourcing requirements

- 1.1 The Supplier shall do all such things necessary to ensure that Citi is in compliance with the Banking Act Direction No 02 of 2012 on the *Outsourcing of Business Operations of a Licensed Commercial Bank and Licensed Specialized Bank*, the following in particular:
 - 1.1.1 The Supplier shall have a satisfactory business continuity plan and conduct regular tests thereon.
 - 1.1.2 The Supplier shall do all such things and provide all such information necessary to enable Citi to make transaction reports and suspicious transactions reports to the Financial Intelligence Unit, as provided under the Financial Transactions Reporting Act No. 6 of 2006.

2. Audit and Inspection

In order to ensure compliance with Part V of the Banking Act No. 30 of 1988 as amended and **Section 61 of the Central Bank of Sri Lanka Act No. 16 of 2023** as amended, the Supplier shall comply with the additional clauses set out below :-

- 2.1 The Supplier shall:
 - 2.1.1 maintain such additional records as may be expressly agreed between Citi Sri Lanka and the Supplier relating to the Services provided by the Supplier under the Master Agreement. The Supplier shall procure that any sub-contractor shall also maintain complete and accurate records of all its work in relation to the Services sub-contracted to it;
 - 2.1.2 allow Citi, any duly authorised officer or representative of a regulatory or supervisory authority (including the Central Bank of Sri Lanka) or any agent appointed by any of them (i) to conduct audits on the Supplier, (ii) access the Supplier to obtain records and documents, of transactions, and information of Citi given to, stored at or processed by the Supplier, (iii) access any report and finding made on the Supplier, (iv) to inspect, examine and audit the Supplier's operations and records insofar as they are relevant to the Services provided by the Supplier under the Agreement, including but not limited to the internal controls adopted by the Supplier with respect to preservation of the confidentiality of data generally and Citi's information specifically (where applicable). The Supplier shall ensure and procure that these requirements are met in its arrangements with any sub-contractor that the Supplier may engage in the outsourcing (if applicable), including any disaster recovery and backup suppliers;
 - 2.1.3 adopt whatever supervisory actions and additional/corrective measures which the Central Bank of Sri Lanka, any competent court of law, or other judicial, quasi-judicial, statutory, regulatory or supervisory authority or any agent appointed by any of them may require to be taken by Citi, depending on the potential impact of the outsourcing

on Citi and the financial system, or as circumstances warrant, as communicated by Citi to the Supplier;

- 2.1.4 provide such information as may be required by Citi in a timely manner in order that Citi may comply with any requirements imposed on Citi by law, the Central Bank of Sri Lanka, any competent court of law, or other judicial, quasi-judicial, statutory, regulatory or supervisory authority.

3. Declarations of Secrecy

- 3.1 In terms of Section 77 of the Banking Act No. 30 of 1988, as amended and the Banking Act Direction No. 02/04/002/005/001 dated 1st December 1999, the Supplier shall procure its employees, servants, agents, representatives and contractors to execute a confidentiality undertaking, (as defined in Appendix I) provided that if such Services are obtained from an organization, and where confidentiality provisions are built in to the underlying service contract with such parties such undertaking as set out in Appendix I provided by the authorized signatory/signatories of the Supplier would suffice.

4. Special clause/condition in software maintenance agreements or service agreements with software companies

- 4.1 In terms of the Banking Act Direction No. 02/04/002/005/001 dated 1st December 1999 and Banking Act Direction No 02 of 2012 on the *Outsourcing of Business Operations of a Licensed Commercial Bank and Licensed Specialized Bank*, the Supplier shall ensure that where there are any agreements with third parties (appointed with Citi's prior written consent) with regard to any software maintenance or services such agreements shall include a confidentiality clause substantially similar to the clause set out below.

"The parties agree that all information provided pursuant to this Agreement by each party to the other party is confidential and proprietary to the party providing the information and no party shall use any information provided by the other party for any purpose other than as permitted or required for performance under this Agreement. Each party agrees not to disclose or provide any information provided by the other party to any third party (with the exception of (i) any affiliate or subsidiary, which is bound to retain the confidentiality of the information; (ii) employees who have a need to know in the course of receiving or performing the Services pursuant to this Agreement, as the case may be, and such disclosure shall be to the extent required, provided that such employees are bound to retain the confidentiality of the information and (iii) Citi's disclosure of data to its internal and external auditors) without the express written consent of the other party, and each party agrees to take all reasonable measures, including, without limitation, measures taken by each party to safeguard its own confidential information to prevent any such disclosure by employees, agents, or contractors. Nothing provided herein shall prevent any party from disclosing information to the extent the information (i) is or hereafter becomes part of the public domain through no fault of that party; (ii) is received from and furnished to a third party without similar restriction on disclosure by such third party; (iii) is independently developed by it; (iv) is required to be disclosed under law or any applicable regulation, at the order of a court of law, or at the request or order of any statutory, regulatory or supervisory authority with whom it customarily complies; or (v) is already known to it. If either party hires another person to assist it in the performance of this Agreement, or assigns any portion of its rights or delegates any portion of its responsibilities or

obligations under this Agreement to another person, the assigning or delegating party shall cause its assignee or delegate to be bound to retain the confidentiality of the information.”

- 4.2 The Supplier shall obtain confidentiality undertakings, in form and substance acceptable to Citi and the Supplier from such software companies and the employees of such software companies who are or will be engaged in the provision of the services contemplated in this Agreement.

5. Provisions applicable to technology initiatives under the Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks

Obligations of the Supplier when Supplier is engaged in any technology initiative of Citi Sri Lanka involving an Information System¹.

5.1 Citi owned, Supplier managed, and located in Sri Lanka

Supplier shall ensure compliance with provisions under 5.4 below.

5.2 Citi owned, Supplier managed, and located outside Sri Lanka

Supplier shall ensure compliance with requirements under 5.4 below. The Supplier shall also ensure the availability of multiple, fully independent telecommunications links, individually capable of serving full workload, with both primary and disaster recovery sites from Sri Lanka and between the primary and disaster recovery sites.

5.3 Supplier owned and located in Sri Lanka or outside Sri Lanka

Supplier shall ensure compliance with provisions under 5.4 below. Supplier shall also comply with the following:

- (i) Supplier owned information system infrastructure shall possess a certification for the latest edition of ISO 22301 - Business continuity management systems, from an accredited certification body; and
- (ii) Supplier shall provide details of its disaster recovery arrangements to Citi and shall cooperate with Citi's review of the same.

5.4 Requirements for using critical information systems² managed or owned by the Supplier and for information systems exposed to customer data or confidential non-customer data (where such critical information systems and information systems are identified in the Master Services Agreement)

Supplier shall ensure that:

- (i) Information system infrastructure managed or owned by Supplier shall possess a certification for the latest edition of ISO 27001 - Information security management systems, from an accredited certification body.

¹ Information system' is any information processing system, service or infrastructure or the physical location housing them

² "Critical information systems" has been defined in Section 3.2 of Direction No. 16 of 2021 as "any information system essential to the functioning of the licensed bank as identified by the Board of Directors of the licensed bank, including information systems of the licensed bank and relevant information systems of third party service providers and agents".

- (ii) In the event the third-party service obtained is cloud computing, the Supplier shall possess a certification for the latest edition of ISO 27017 – Security controls for cloud services, from an accredited certification body.
- (iii) The Central Bank of Sri Lanka shall have the right to examine Supplier with the services provided to Citi;
- (iv) Supplier shall make available any information or data requested by the Director of Bank Supervision of the Central Bank of Sri Lanka concerning the services provided to Citi;
- (v) The Sri Lankan judiciary shall have the right to request and obtain via appropriate judicial process and orders any information or data relating to the services provided to Citi through Citi;
- (vi) Supplier shall facilitate smooth transfer of data and systems at the end of the contract or whenever demanded by Citi;
- (vii) Supplier shall facilitate internal auditing requirements and information security testing requirements in accordance with Section 1 (Audit) above; and
- (viii) The Supplier implementing this model for critical information systems shall ensure the availability of multiple fully independent telecommunications links, individually capable of serving full workload with both primary and disaster recovery sites from Sri Lanka and between the primary and disaster recovery sites.

6. Compliance with the Data Protection Act, No. 9 of 2022.

6.1 Where the Supplier is processing any Personal Information as part of any Services provided under the Master Agreement or any relevant Work Order, the Supplier shall in addition to any other obligations set out in the Master Agreement or any relevant Work Order:

- (i) Ensure that processing activities are carried out only as per the written instructions of Citi as set out in the Master Agreement or any relevant Work Order;
- (ii) Ensure that its personnel are bound by contractual obligations on confidentiality and secrecy by the implementation of appropriate technical and organizational measures;
- (iii) Facilitate Citi to carry out compliance audits in accordance with Section 1 (Audit) above; and
- (iv) Upon the written instructions of Citi, erase existing copies of Personal Information or return all Personal Information to Citi after the completion of the provisions of Services relating to processing.

Where the Supplier fails to comply with the provisions of paragraph (i) above, the Supplier shall, be deemed to be in breach of the Master Services Agreement.

6.2 Where the Supplier engages another processor (hereinafter referred to as the “**sub-service provider**”) for carrying out specific processing activities, the Supplier shall ensure that the provisions of Section 6.1 above shall be made applicable to and in relation to such sub-service provider via contractual means.

6.3 Where a sub-service provider fails to fulfil its obligations under Section 6.2 above, the Supplier shall be liable to Citi for such breach.

6.4 Cross border data flow

6.4.1. The Supplier should ensure compliance with provisions of Part I, Part II and sections 20, 21, 22 ,23 ,24 and 25 of PDPA

6.4.2. The Supplier may process Personal Information provided to the Supplier by Citi Sri Lanka outside Sri Lanka only where Citi expressly authorizes the Supplier to do so under the Master Agreement or any relevant Work Order.

6.5 The following defined terms shall apply;

- (i) “**Personal Information**” shall include, any information that can identify a data subject directly or indirectly, by reference to– (a) an identifier such as a name, an identification number, financial data, location data or an online identifier; or (b) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person;
- (ii) “**Processor**” means , a natural or legal person, public authority or other entity established by or under any written law, which processes Personal Information on behalf of the Controller;
- (iii) “**data subject**” means, an identified or identifiable natural person, alive or deceased, to whom the Citi Personal Information relates;
- (iv) “**financial data**” means, any alpha-numeric identifier or other personal data which can identify an account opened by a data subject, or card or payment instrument issued by a financial institution to a data subject or any personal data regarding the relationship between a financial institution and a data subject, financial status and credit history relating to such data subjects, including data relating to remuneration.

[APPENDIX I - UNDERTAKING³](#)

³ Note: for Supplier’s employees, servants, agents, representatives and contractors to execute.