

SCHEDULE H – KOREA LAW REQUIREMENTS

(Version 6 – 11 February 2026)

This Schedule shall apply to the services (“**Services**”) provided to the Citi entities incorporated in the jurisdiction of the Republic of Korea (“**Korea**”). To the extent that the terms and conditions of the Agreement are inconsistent with this Schedule, the terms and conditions herein will prevail.

1. Requirements under the (i) Personal Information Protection Act and (ii) Use and Protection of Credit Information Act:

The following provisions shall apply to the Supplier to the extent that the Supplier receives Personal Information under the Personal Information Protection Act (“**PIPA**”). Personal information refers to information pertaining to a living individual which contains information identifying a specific person with a name, a resident registration number, or similar in a form of an image, etc. (including information that does not, by itself, make it possible to identify a specific person but that when combined with other information readily identifies such a person). For the avoidance of doubt, Personal Information includes any credit information that relates to determination of credit rating or credit transactions capacities of a person as such term is defined under the Use and Protection of Credit Information Act (“**CIA**”). Any terms not separately defined herein shall have the meanings ascribed to them in PIPA and CIA, and its subordinate statutes.

1.1 The Supplier shall not transfer or sub-delegate all or part of the Services to a third party unless it has obtained prior consent from Citi.

1.2 During and after the term of the Agreement, the Supplier shall not use, provide or divulge to a third party, the personal information beyond the scope of performance of the delegated Services. Upon termination or expiration of the Agreement, the Supplier shall, at Citi’s option, immediately destroy or return to Citi or a third party designated by Citi the personal information it retains in relation to the delegated services.

1.3 The Supplier shall take managerial and technical measures to ensure safety of personal information in accordance with PIPA, CIA and its subordinate statutes, including establishment and operation of facilities and systems, to achieve the following in connection with processing any Personal Information:

- prevent any distortion of access records to the Personal Information;
- encrypt the Personal Information for transmission purposes; and
- examine the Personal Information access records on a regular basis.

In addition, the Supplier shall take such other measures necessary to protect the Personal Information as reasonably required by Citi.

1.4 Upon occurrence of any breach of the Personal Information Protection Procedures or theft of the Personal Information (the “Occurrence”), the Supplier shall, without delay, take necessary measures to minimize the damage or loss and immediately notify Citi and Citi’s Project manager of the Occurrence and the following information as applicable:

- the items of the Personal Information that are disclosed or stolen;
- the time and details of the Occurrence;
- measures that victims of the Occurrence may take to minimize their damage or loss;
- measures adopted by and reliefs to be provided by the Supplier to remedy the Occurrence; and
- contact information to which the victims may report their damage or loss.

1.5 The Personal Information pertaining to an individual must be made available for review, correction, or deletion, or must be subject to suspension of being processed upon such individual’s request. In the event that such individual to which the Personal Information pertains raises any objection to the

manners in which his/her request concerning the foregoing matters are addressed by Citi, the Supplier shall endeavor to assist Citi in dealing with such objection.

1.6 Citi shall have the right to supervise the Supplier's compliance with the PIPA and its subordinate statutes, within the scope of Citi's statutory obligations, and the Supplier shall provide necessary cooperation.

1.7 In the event that the Supplier, officers and employees of the Supplier or the Supplier's delegatee breaches its obligations hereunder in the course of performing the services delegated or sub-delegated hereunder or inflicts damages on Citi, the information principal or other third parties due to causes attributable to the Supplier, officers and employees of the Supplier, or the Supplier's delegatee, the Supplier shall compensate for such damages. If Citi has fully or partially compensated for damages suffered by the information principal or a third party, Citi may seek indemnification from the Supplier

1.8 The Supplier shall, once a year, conduct training for its employees regarding the prevention of fabrication, theft, leakage, alteration, or damage of personal credit information, and the safe processing of credit information, and shall provide relevant evidence upon Citi's request.

2. Delegation Matters under the Regulations on Business Delegation by Financial Institutions

The Supplier shall maintain a continuity of business ("COB") plan designed to deal with a major destruction or incapacity of its facilities and/or systems. Pursuant to the COB plan, the Supplier shall maintain resources, guidelines, general action steps and backup sites, facilities and systems to resume business in case of disruption due to natural disaster, accidents or system failure. The COB plan shall include procedures including, but not limited to, for business site relocation, restoration of business functions and telecommunications resumption. Redundant servers shall be in place for several key systems and daily tape backups shall capture all key data and be stored offsite. The Supplier's COB plan shall be updated and tested on an ongoing basis.

3. Requirements under Regulation on Outsourcing of Data Processing of Financial Companies

Where the Services entail outsourcing of data processing under the Regulation on Outsourcing of Data Processing of Financial Companies, the following provisions shall apply

- 3.1 Citi shall delegate to the Service Provider the data processing to the extent necessary for the scope of the relevant Services. The access to the data is restricted to a "need to know" basis and the necessary controls and conditions to delegate the data processing are incorporated in the Agreement including but not limited to
- (i) access and control to data transferred,
 - (ii) Supplier's responsibility with regard to damage or loss suffered by Citi's customer arising from an IT incident,
 - (iii) inspection right on the Supplier by the regulator of Citi and ,
 - (iv) jurisdiction in the event of legal dispute between Citi and Supplier.
- 3.2. The Supplier shall not transfer or subcontract all or part of the data processing services to its affiliate or a third party unless it has obtained prior consent from Citi. The Supplier understands and acknowledges that Citi shall report such subcontract of data processing to the regulator and the Supplier shall require subcontractors to comply with equivalent terms to this Schedule and the Agreement and use its best efforts to facilitate the report process.

3.3 The outsourcing agreement of data processing shall be governed by and construed in accordance with the laws of the Republic of Korea. Any dispute concerning the Service Provider over the outsourcing agreement is subject to the jurisdiction of the courts of the Republic of Korea.

4. **Requirements under the Financial Investment Services and Capital Markets Act (FISMA)**

The Supplier understands and acknowledges that, Citi shall report an agreement related to the business delegation under the FISMA to the Financial Services Commission and the Supplier shall use its best efforts to facilitate the report process.