EXHIBIT I – PROCUREMENT AGREEMENT

Digital Operational Resilience Act (DORA) Terms

1. Parties and Scope. This Exhibit applies only in respect of services which constitute ICT Services (as defined in paragraph 2 below) constitutes an integral part of the Procurement Agreement, including any SOWs thereunder (collectively, the "Agreement"). In the event of any inconsistency or conflict between existing terms of the Agreement and the terms of this Exhibit then the terms of this Exhibit shall prevail. The Agreement shall remain otherwise unchanged and in full effect.

2. Definitions. Capitalised terms used in this Exhibit shall have the meaning given thereto in the Agreement or, where applicable, in DORA. Any other capitalised term shall have the meaning given to it in this Exhibit.

New definitions:

Critical ICT Services shall mean ICT Services supporting critical or important functions as defined in DORA;

Hitachi Data shall mean information, data and other content provided by Hitachi or Hitachi's Customer to Supplier in the course of the Hitachi's or Hitachi's Customer receipt of ICT Services under the Agreement;

DORA shall mean Regulation (EU) 2022/2554 of the European Parliament and the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, including the related regulatory technical standards, each as amended, supplemented, superseded and/or replaced from time to time;

DORA Regulator shall mean any supervisory authority defined as such by DORA which has competence to make a determination which is legally binding upon a Party;

Good Industry Practice shall mean standards, practices, methods and procedures conforming to applicable laws and regulations and the degree of skill, care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced provider of the type of services provided by Supplier under the Agreement in the relevant Service Location;

ICT shall mean information and communication technology;

ICT-related Incident shall have the meaning given to such term in DORA;

ICT Services shall have the meaning given to such term in DORA;

Service Location shall mean a location where any ICT Services will be received (including, for example but without limitation, a storage location), as defined in any relevant document agreed between the Parties or otherwise provided by Hitachi.

3. Changes to Products and Services. The Parties will give due consideration to continued compliance with DORA when agreeing mutually any changes to ICT Services to be provided under the Agreement. Where the Agreement permits unilateral variation then the Party making the change will not in making such change diminish materially the other Party's compliance with DORA.

4. Subcontracting.

4.1. Where subcontracting by Supplier of the provision of ICT Services is currently permitted under the Agreement then such subcontracting is subject to the following conditions:

a. Supplier has clear contractual terms in place with its relevant subcontractor, which address the security of any Hitachi Data being processed under the relevant subcontract;

b. Supplier ensures by verification that the technical and organisational measures implemented by the subcontractor provide at least the level of protection for Hitachi Data required by the Agreement and DORA; and

c. to the extent required by Hitachi, Supplier and its subcontractor shall maintain (or obtain) a valid Legal Entity Identifier (LEI), which LEI Hitachi will confirm promptly upon Hitachi's written request.

d. Supplier shall establish the monitoring and reporting obligations of the subcontractor, which the subcontractor must fulfil towards the Supplier and thereby also towards the Hitachi;

e. Supplier shall ensure continuous provision of the service according to the agreed service levels; and

f. Supplier shall ensure continuous compliance with ICT security standards and, if applicable, additional security features by the subcontractor in accordance with the technical regulatory standards required by DORA Regulator.

4.2. Where Supplier wishes to change a subcontractor providing, or to appoint a new subcontractor to provide, Critical ICT Services under the Agreement then Supplier shall provide Hitachi with not less than 60 (sixty) calendar days' prior written notice of the following information related to the proposed incoming subcontractor: (i) the full company name of the subcontractor, (ii) the location from which the subcontractor would provide its services and (iii) the Hitachi Data to be shared by Supplier with the subcontractor and any reasonably required information to enable Hitachi and its Customers to comply with their respective obligations under DORA.

4.3. Hitachi shall have the right to object to any proposed new or replaced subcontractor within thirty (30) calendar days of receiving notice under paragraph 4.2. If Hitachi objects to a proposed subcontractor, Supplier shall not proceed with the proposed change until the Parties have reached agreement on a mutually acceptable solution.

5. Service Levels. The Parties will ensure that the Agreement contains mutually agreed service levels to be met to ensure compliance with DORA. Where Supplier then does not meet such a service level in respect of ICT Services then Supplier will promptly, upon Hitachi's request, identify, document, and remedy the root cause of the breach of the service level and thereafter keep Hitachi informed of progress with remedying the issue. Supplier will then confirm if and when the issue has been remedied.

6. Data Protection, Access, Recovery and Return.

6.1. Supplier shall have and maintain documented data management and disaster recovery plans, including in relation to Hitachi Data and which at minimum comply with Good Industry Practice, ensuring: (i) adequate standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit, and (ii) in case of insolvency, resolution or discontinuation of the business operations of Supplier or termination of the Agreement that Hitachi Data is accessible and recoverable in an easily accessible format.

6.2. Where the Parties agree that Supplier is providing Critical ICT Services, Supplier will (i) regularly, not less than once per year, review and test its disaster recovery plans in line with Good Industry Practice and (ii) notify Hitachi , with a level of detail that Hitachi ought reasonably expect, if Supplier implements any updates or changes to its disaster recovery plan(s) which would decrease materially the overall ICT security or resilience, continuity and availability of the Critical ICT Services.

6.3. Upon termination or expiration of the Agreement, Supplier shall: (a) Return all Hitachi Data in an industry-standard format specified by Hitachi; (b) provide reasonable transition assistance to Hitachi or its designated replacement provider; and (c) securely delete all Hitachi Data from Supplier's systems and provide a certificate of deletion upon Hitachi's request.

7. ICT Incident Notification and Assistance. Supplier shall report to Hitachi in writing without undue delay any ICT-related Incidents of which it becomes aware that have a material negative affect for any ICT Services that it is providing for Hitachi and thereafter provide free of charge any assistance and information available to Supplier reasonably required to enable Hitachi to comply with its notification obligations under DORA.

7.1. The information about the ICT-related Incident shall include at least information on the time and type of the incident (including information as to what data is affected and how), the system affected, the number and type of data subjects affected, the time of discovery, the contact information of the Supplier's persons handling the security incident (telephone number, e-mail address etc.), any potential adverse consequences of the security incident, including their likelihood of occurrence, and the measures taken and proposed by the Supplier to mitigate adverse effects. Further information in accordance with any other applicable legal regulations shall remain unaffected.

7.2. The first information to Hitachi has to take place immediately after becoming aware of the ICT-related Incident. A further, detailed notification of Hitachi, which must contain all information in accordance with Section 7.1., shall be made without undue delay and if possible within 48 hours of becoming aware of the ICT-related Incident. If this detailed notification is not possible within 48 hours, Hitachi shall be provided with a justification for the delay together with information as to when the complete and proper detailed notification will be provided.

8. Cooperation with DORA Regulators. Supplier will cooperate with DORA Regulators to the extent required by applicable law. Hitachi is entitled to terminate the Agreement where this is required by a DORA Regulator and where failure to terminate would be a breach of applicable law. Such termination must however be effected in accordance with any term(s) of the Agreement dealing with termination due to DORA Regulator instruction.

9. Termination rights. Notwithstanding any provision(s) of the Agreement to the contrary, whether express or implied, Hitachi may terminate the Agreement by providing written notice to Supplier and Supplier does not take reasonable steps to remedy the matter within 30 days of first notice from Hitachi:

9.1. in the event of a material breach by Supplier of the terms of this Exhibit;

9.2. in the case of any weakness of Supplier's overall ICT risk management which compromises the availability, authenticity, integrity and confidentiality of Hitachi Data; or

9.3. where long or complex chains of subcontracting of ICT Services impacts a Regulator's ability to fully monitor the contracted functions and the ability of the Regulator to effectively supervise Hitachi or Hitachi's Customer in respect of the ICT Services.

9.4. In the event of repeated service level failures for Critical ICT Services, regardless of whether such failures have been remedied.

10. Participation in training. Upon request, Supplier and its subcontractors shall participate in Hitachi's and/or Hitachi's Customer's ICT security awareness programs, as applicable and digital operational resilience training provided for its own staff and/or suppliers. Supplier shall bear its own costs for such participation.

11. Notice periods and reporting obligations. Where Supplier is providing Critical ICT Services for Hitachi or Hitachi's Customer, Supplier will: (a) inform Hitachi in writing without undue delay of any developments that may have a material negative impact on Supplier's ability to effectively provide the Critical ICT Services in line with any service levels previously agreed by the Parties.

12. Business continuity. Where Supplier provides Critical ICT Services for Hitachi or Hitachi's Customer:

12.1. Supplier shall have an up to date and maintained Business Continuity Plan in place which covers the provision of the ICT Services. The Business Continuity Plan must be designed to prevent negative impacts by unplanned disruptions and to ensure that Supplier can continue to function through operational interruption and continue to provide Services as specified in the Agreement;

12.2. Supplier will provide Hitachi a complete copy of its Business Continuity Plan upon request, which shall be subject to Hitachi's review and approval; and

12.3. Supplier shall perform, at least annually, an appropriate test of its Business Continuity Plan (and confirm for Hitachi upon request that it has done so) and remedy without undue delay any material weakness(es) identified during such test(s).

13. Testing. Where Supplier provides to Critical ICT Services for Hitachi, Supplier shall participate in and co-operate with, and, where applicable, shall ensure that its subcontractors participate in and co-operate with, Hitachi's or its Customer's threat-led penetration testing (TLPT) as referred to in Articles 26 and 27 of DORA (if and to the extent applicable to Hitachi or its Customer), as reasonably requested by Hitachi.

14. Monitoring. Where Supplier provides Critical ICT Services for Hitachi:

14.1. Supplier hereby grants to Hitachi, a DORA Regulator and to a third party appointed thereby for such purpose and to whom Supplier does not raise reasonable objection, an unrestricted right of access, inspection and audit to confirm Supplier's compliance with the provisions of this Exhibit, subject to Supplier's reasonable requirements in respect of confidentiality;

14.2. If and to the extent the rights of Supplier's other customers would be impacted by the exercise of Hitachi's rights under paragraph 14.1 then Supplier shall have the right to propose an alternative way to provide a similar level of assurance for Hitachi, which alterative way Hitachi will not reject unreasonably;

14.3. If Supplier objects to a third party appointed by Hitachi to carry out an audit, on the basis that the third party is a competitor to Supplier, Supplier shall in its notice to Hitachi include at least three reputable audit firms operating in the relevant market that Supplier does not consider to be its competitors, and who therefore may carry out the audit;

14.4. Hitachi may conduct audits of Critical ICT Services as reasonably necessary for regulatory compliance, customer requirements, risk management, or suspected breaches of this Exhibit; and

14.5. Hitachi, the DORA regulator and/or the appointed auditor, as applicable, shall be entitled when reasonably required to make copies of all relevant documents in the course of the audit.

15. Exit. Supplier shall develop and maintain an exit plan for the orderly transition of services to Hitachi or a replacement provider in the event of termination or expiration of the Agreement for the purposes of Article 28 (8) and Article 30 (3) f) of DORA. The exit plan shall be provided to Hitachi within 60 days of the effective date of the Agreement and updated annually thereafter.