HITACHI
Inspire the Next

EXHIBIT C – PROCUREMENT AGREEMENT
INFORMATION SECURITY REQUIREMENTS

1. Introduction

These Information Security Requirements (the "**ISR**") reflect the Parties' agreement with respect to the minimum standards that the Supplier shall employ for the entire term of the Procurement Agreement including any SOWs thereunder.

2. Definitions

Unless expressly defined in this ISR, all capitalized terms shall have the same meaning as in the Procurement Agreement. In this ISR, the following terms have the following meanings:

Hitachi Data: any Hitachi Data, including but not limited to data shared under or pertaining to the Procurement Agreement, Services, Deliverables, invoicing and business processes. Hitachi Data includes Hitachi Customer data.

Hitachi Systems: any Hitachi networks, computing systems, applications, cloud services that provide access to or store, process or transmit Hitachi Data.

Products: See the Procurement Agreement.

Production Environment: Supplier Systems used to provide Services or Deliverables to Hitachi.

Security Breach: any accidental or unauthorized access, destruction, disclosure, modification or transfer of Personal Data.

Supplier Systems: Supplier networks, computing systems, applications and/or cloud services that access, provide access to, store, process or transmit Hitachi Data or access Hitachi Systems.

Test And Development Environment: Supplier Systems used for the purpose of development and/or testing a product or service, but not directly used to deliver Services or Deliverables to Hitachi or Hitachi's Customer.

3. General Requirements

(a) Supplier will maintain organizational, physical and technical safeguards that meet or exceed industry best practices – e.g. as set forth in ISO/IEC 27001:2022/27002:2022 or NIST SP 800-53 or NIST SP 800-218 and provide Hitachi a copy of the documentation of its information security program and practices upon request.

(b) Supplier will maintain an information security program under the oversight of a Chief Information Security Officer (CISO) or a senior leader who is accountable for an effective information security program and exercises necessary and appropriate supervision over relevant Personnel to maintain appropriate confidentiality, integrity, availability, and security of Hitachi Data, Hitachi Systems, Supplier Systems and Products.

(c) Supplier will provide for the term of the Procurement Agreement a SOC 2 Type II report or ISO/IEC 27001:2022 certification with associated Statement of Applicability or an equivalent attestation or certification, from an independent third party covering its operation pertaining to the Services or Deliverables.

4. Third Party Management

(a) Supplier shall assess the information security risks associated with third party services that are material to the delivery of the Services or Deliverables and identify remedial actions to mitigate such risks. Existing third-party services shall be monitored and periodically evaluated for information security risks and risk mitigation measures shall be taken by Supplier.

(b) Supplier shall disclose in advance the names of any third-party subcontractors that may access, process, store or transmit Hitachi Data.

5. Personnel Security

(a) Supplier shall ensure all Personnel with access to Hitachi Data or Hitachi Systems undergo a formal information security awareness training annually.

(b) Supplier will assure all Personnel with access to Hitachi Data or Hitachi Systems have undergone an adequate background check prior to access to Hitachi data and Hitachi Systems.

6. Access Control

(a) Supplier shall secure access to Hitachi Data, Hitachi Systems and relevant Supplier Systems by techniques that conform to security industry standards and guidelines, for example strong passwords or multi-factor authentication (MFA).

(b) Access to Hitachi Data is granted strictly on a business-need basis and reviewed on a periodic basis.

(c) Supplier shall ensure all Personnel that are connecting remotely (from outside the Supplier's facilities) to access Hitachi Data, Hitachi Systems, or relevant Supplier Systems are authenticated using multi-factor authentication and remote connections are encrypted.

7. System Security

Supplier shall use technical and procedural means to continuously secure Supplier Systems, including but not limited to:

(a) anti-malware, advanced threat protection;

(b) firewalls, secure gateways, network access security, intrusion prevention systems (IPS), intrusion detection systems (IDS);

(c) secure hardening and configuration of Supplier Systems;

(d) periodic vulnerability scans and remediation of vulnerabilities commensurate to the criticality of vulnerabilities;

(e) patching of firmware, OS, middleware, applications to the latest patch available;

(f) penetration testing of externally accessible Supplier Systems at least annually; and

(g) logging, monitoring of and responding to information security events and abnormal conditions.

8. Data Protection

Supplier shall ensure the following technical and procedural controls are in effect to protect Hitachi Data unless otherwise approved by Hitachi in writing:

(a) Hitachi Data is stored and processed physically or logically segregated from that of Supplier's other customers and segregated from Supplier's other environments.

(b) Hitachi Data is encrypted when in transit (transmitted) using strong and secure encryption methods and protocols utilized (specifically TLS 1.2 and higher).

(c) Hitachi Data is always encrypted when stored at rest, including on backup storage media or when ephemerally stored during transit using strong encryption methods.

(d) Access to Hitachi Data and Hitachi Systems is granted strictly on a need-to-know basis and access is immediately revoked when no longer needed.

(e) Programmatic access to Hitachi Data or Hitachi Systems is secured using authentication tokens or certificates, and tokens or certificates are rotated on a regular basis.

(f) Production Environments are separate from Test and Development Environments, and Hitachi Data is segregated. Test and development activities are not performed in Production Environments and not on Hitachi Data stored in any Production Environment.

(g) Any Hitachi Data used for testing or development is adequately protected, *i.e.* by using test data only (not production data) or by masking or obfuscation of production data.

(h) Access to Hitachi Data is recorded and logs are retained for at least 1 year.

(i) No Hitachi Data is stored on personal removable media, such as portable hard drives, USB drives, DVDs, etc.

(j) No Hitachi Data is stored in third-party cloud services without prior written approval by Hitachi.

(k) If Supplier stores Hitachi Data, then Hitachi Data and Supplier Systems are backed up to support the Recovery-Point-Objective (RPO) and Recovery-Time-Objective (RTO) as either (1) specified in the Procurement Agreement; or (2) with an RPO of 24 hours and RTO of 24 hours, whichever is lesser.

(l) All Hitachi Data, including media containing Hitachi Data, shall either be returned to Hitachi or shall be rendered totally unrecoverable upon termination of the Procurement Agreement or an applicable SOW.

9. Application Security

(a) For each major release the Supplier will perform at least the following Product security and vulnerability assessment prior to making the release available and remediate vulnerabilities found during testing in a timely manner:(i) threat modeling, (ii) Static Application Security Testing (SAST), (iii) Vulnerability scans, (iv) penetration testing, (v) Third Party software composition analysis (SCA), and (vi) Dynamic Application Security Testing (DAST).

(b) Products will not have any critical or high severity vulnerability on final (GA / General Available) release.

(c) Supplier will promptly inform Hitachi of any security vulnerabilities, along with their CVSS rating, that have been found in writing.

(d) Supplier will remediate security vulnerabilities found during testing within 15 days (Critical), 30 days (High), 60 days (Moderate), and 90 days (all other severity levels).

At any time and at Hitachi's sole request, Supplier shall provide documentation of its application security practices to Hitachi.

10. Physical Security

(a) Supplier shall ensure that Hitachi Data is only stored, processed and accessed by authorized Personnel in a secure environment.

(b) Supplier shall ensure that all media containing Hitachi Data are stored and accessed by authorized Personnel in a secure environment.

(c) Supplier shall ensure that Supplier Systems can only be removed or added with authorization from Supplier's management.

(d) Supplier shall ensure its remote workforce is trained on and required to apply secure practices when working remotely.

11. Reporting Security Incidents

(a) In the case of a Security Breach, Supplier will notify Hitachi at both privacy@hitachi-digital.com and cybersecurity@hitachivantara.com within twenty-four (24) hours of Discovery of the Security Breach, providing all relevant information that Supplier knows or ought reasonably to know. Within five (5) business days after its Discovery, Supplier will provide Hitachi a written report setting out at a minimum the following details, to the extent Supplier knows or ought reasonably to know: (i) Security Breach description; (ii) occurrence date of Security Breach; (iii) Discovery date of Security Breach; (iv) the identity and last known mailing address of affected individuals; (v) the affected categories of Personal Data for each individual or categories of Confidential Information; (vi) a description of the steps taken to date, or that otherwise should be taken, to respond to, deal with or otherwise mitigate any impacts of the Security Breach and the details of the person or entity which has, will or should be taking such steps; (vii) an identification of any law enforcement agency contacted about the Security Breach and contact information for the relevant official; (viii) a description of the steps that have been, or will be, taken to prevent a recurrence and the details of the person or entity which has, will or should be taking such steps; and (ix) contact information for the individual principally responsible for responding to the Security Breach. Supplier will update the written report as new, material information is Discovered.

(b) If there is a Security Breach resulting from Supplier's acts or omissions, or the acts or omissions of one of Supplier's Personnel or agents, Supplier will promptly reimburse Hitachi for all costs reasonably incurred by Hitachi in connection with the Security Breach, including, but not limited to, notification and credit monitoring services.

(c) Each Party agrees to cooperate in any Security Breach investigation undertaken by, or otherwise involving, the other Party and to take reasonable measures to mitigate the harmful effects of any Security Breach of which that Party becomes aware.

(d) Supplier shall provide an email or telephone point of contact for security inquiries and incident follow-up by Hitachi prior to commencement of the Services.