Data Security Exhibit
to Order Form

This Data Security Exhibit (the "**Exhibit**") is incorporated into the Order Form between the CUBE entity identified the Order Form ("**CUBE**") and the Customer identified in the Order Form. This Exhibit sets forth the obligations of both parties during the Term of any Order Form regarding the security of the other party's information including any Customer Data. In the event of a conflict between this Exhibit and the Exhibit, the terms and conditions of this Exhibit will apply.

1. Information Security Program.

1.1. Written Information Security Program. CUBE will maintain a written information security program that adopts, is based on, in compliance with, or materially aligns with an industry information security standard, which may include ISO2700x series, SOC 2 Type 2, and/or Center for Information Security (CIS) Benchmarks.

Such program will include, but is not necessarily limited to, the following:

1.1.1. Information security policy framework to define applicable CUBE roles and responsibilities to protect information resources;
1.1.2. Program documentation;
1.1.3. Auditable controls;
1.1.4. Compliance records;
1.1.5. Developing an information security team with identification of key information security specialists, which may include security officer and information security personnel; and
1.1.6. Ongoing obligation to periodically review the program.

1.2. Information Security Policies. CUBE will maintain information security policies, procedures, and/or processes designed to protect the confidentiality and integrity of sensitive and/or confidential information, which may include Customer Data within CUBE's possession, which will include the following policies, procedures, and/or processes designed to:

1.2.1. Information access restriction, with end user rights and privileges to information based on a least-privilege basis;
1.2.2. Require use of authentication as part of accessing Customer Data, such as user IDs, passwords, and/or multi-factor authentication;
1.2.3. Require internet connections to have commercially reasonable controls to help detect and terminate unauthorized activity;
1.2.4. Internal audits designed to assist in identifying security threats and vulnerabilities;
1.2.5. Require performance of periodic vulnerability assessments;
1.2.6. Require use of anti-malware and patch management controls to help protect against virus or malware infection;
1.2.7. Define access control requirements in accordance with confidentiality, availability and integrity goals, including, but not limited to:
1.2.7.1. user access management;
1.2.7.2. user responsibilities;
1.2.7.3. network access control;
1.2.7.4. operating system access control;
1.2.7.5. application access control;
1.2.7.6. monitoring systems, including employing system event logs to securely gather and store relevant security logs in applicable systems; and
1.2.7.7. mobile computing and remote working.
1.2.8. Define appropriate physical security, including physical entry controls, physical security perimeters, securing offices, rooms, facilities, and equipment.
1.2.9. Establish, where appropriate, minimum encryption standards, both at rest and in transit, for information CUBE reasonably deems sensitive. CUBE's minimum encryption standards shall reasonably meet then-current industry standards, which for illustrative purposes, may include the Triple Data Encryption Standard (3DES), the Advanced Encryption Standard (128 or higher), or similar. CUBE may reasonably utilize acceptable mitigating and/or compensating controls, in lieu of encryption, upon approval by appropriate CUBE personnel.

1.3. CUBE Personnel Security Compliance Training. CUBE will maintain policies, procedures, and/or processes designed to:
1.3.1. Require periodic training of CUBE personnel regarding CUBE's information security practices;
1.3.2. Require CUBE personnel to report any observed or suspected information security threats, vulnerabilities, or incidents to CUBE information security personnel; and
1.3.3. Ensure CUBE information security personnel will be made aware of reported information security threats, vulnerabilities, or incidents.
1.3.4. CUBE shall be responsible for its personnel's acts and omissions resulting in a breach of CUBE's obligations under this Agreement.

1.4. Security Incident. Subject to CUBE's obligations under the Information Privacy Exhibit regarding Personal Data:
1.4.1. CUBE will maintain a formal incident response policy designed to promptly respond to suspected or confirmed breaches of Customer Data in accordance with Applicable Law, including providing to Customer any notice and/or information as required under Applicable Law regarding a confirmed security incident.

1.4.2. CUBE shall provide notice to Customer promptly, but in no scenario any longer than 72 hours of, CUBE's confirmation of a security incident resulting in the unauthorized access to Customer Data.
1.4.3. Upon Customer's request following a security incident, CUBE shall endeavour to provide documentation related to the security incident as it relates to Customer Data, including a summary of the cause of the security incident, the type of Customer Data believed to be impacted, and steps taken to remedy the security incident and to prevent any, as applicable, reoccurrence.
1.4.4. CUBE shall promptly take commercially reasonable actions designed to remedy or mitigate the impact of such security incident, including performing a root cause analysis to identify the cause of such security incident.
1.4.5. Upon Customer's request following a security incident, CUBE shall reasonably cooperate with Customer's investigation into the security incident.
1.4.6. CUBE agrees that it will not inform any third party of any security incident naming Customer without first obtaining Customer's prior written consent, except if and to the extent otherwise required under Applicable Law, or such disclosure is in furtherance of CUBE's investigation or resulting response plan.

1.5. Personnel Authentication. CUBE will maintain policies, procedures, and/or processes regarding CUBE personnel accessing CUBE systems, including, but not limited to:
1.5.1. Requiring unique account identifiers or user IDs;
1.5.2. Requiring passwords of sufficient complexity and length;
1.5.3. Prohibiting the sharing of user IDs and passwords;
1.5.4. Requiring password changes at periodic intervals; and
1.5.5. Requiring multi-factor authentication (MFA) across all CUBE systems.

1.6. Updates to Information Security Program. CUBE shall review and evaluate its information security program from time to time, including via ongoing testing, monitoring and risk assessments, and other material changes or impacts to CUBE and/or the CUBE Services. Accordingly, CUBE may make changes to its information security program from time to time provided such change does not materially, detrimentally impact the safeguarding of Customer Data.

2. Annual Audit of Controls. CUBE shall cause third-party assessment, certification, audit or similar to be performed annually with respect to the Services provided to Customer, which may include a SOC 2, Type 2 audit. Upon Customer's request, CUBE shall up to once per calendar year provide such assessment, certification, audit or similar to Customer, however, Customer acknowledges that certain sensitive, non-determinative information may be reasonably redacted, the disclosure shall be treated at all times as CUBE Confidential Information, and shall be used by Customer solely for its due diligence purposes and for no other purposes whatsoever.

3. Ongoing Penetration Testing and Vulnerability Scanning. CUBE shall implement processes and/or a written policy to cause, either by CUBE or an appointed third party, periodic (1) penetration testing, (2) both internal and external vulnerability scans, and (3) monitoring for security threats, system configurations, and vulnerabilities, of CUBE systems which provide to Customer the Services or otherwise store or process Customer Data. Upon written request, to occur no more than one per calendar year unless as otherwise agreed between parties, CUBE shall provide the results or an executive summary of such testing. Customer acknowledges that certain sensitive, non-determinative information may be reasonably redacted, the disclosure shall be treated at all times as CUBE Confidential Information, and shall be used by Customer solely for its due diligence purposes and for no other purposes whatsoever.

4. Annual Requests. Customer may request in writing, no more than once per calendar year, relevant and supporting policies and/or documentation necessary to demonstrate CUBE's compliance with its obligations in the Agreement, including the protection of any Customer Data. If the foregoing does not fully demonstrate CUBE's compliance with its obligations in the Agreement, Customer may request in writing, and CUBE shall use commercially reasonable efforts to provide, such information through a service audit engagement to occur no more frequently than once per calendar year. Any information disclosed to Customer by CUBE shall be treated as CUBE Confidential Information. Customer is responsible for ensuring appropriate confidentiality terms to protect such CUBE Confidential Information with any third-party due diligence service provider the Customer utilizes for processing such CUBE Confidential Information. Any information disclosed by CUBE in response to such service audit engagement shall be utilized solely for due diligence purposes and no other purposes whatsoever.

5. Virus/Malware. Each party agrees to implement and configure industry-standard anti-virus and malware anti-protection on systems (i) holding or processing the other party's information, or (ii) accessing the other party's systems or interfaces. Customer acknowledges and agrees that the CUBE Services are accessible via the Internet, which CUBE does not control, and accordingly, notwithstanding anything to the contrary in the Agreement, CUBE shall not be liable for viruses or malware which originate from the Internet.

6. Business Continuity/Disaster Recovery. CUBE will maintain a written business continuity and disaster recovery plan designed to limit interruptions in the event of a major failure. Such policy shall:
6.1. Review and address risks at CUBE's operation offices, loss of staff, loss of vendors, and loss of CUBE datacentres and/or cloud providers, as applicable, including, where reasonably necessary:
6.1.1. Establishing multiple working capabilities, including remote work;
6.1.2. Reducing key personnel dependencies and providing "follow-the-sun" availability models for Customer dependencies;
6.1.3. Establishing commercially reasonable steps designed to provide resiliency for key CUBE vendors, such as utilization of multiple datacentres and/or cloud providers, as applicable, with redundant links for access to, and between multiple sites;
6.2. Be reviewed and updated regularly by appropriate CUBE personnel;

6.3. Establish resilience and availability of CUBE's critical systems and data by setting the following:
6.3.1. Recovery Point Objective in the event of a disruption; and
6.3.2. Recovery Time Objective to restore CUBE systems in the event of a system outage or failure.
6.3.3. Establish a process for observing a critical failure or event, invoking the applicable process, operate during disaster recovery, then returning to business as usual. Such process shall include notice to CUBE customers;
6.3.4. Establish key personnel for roles and responsibilities under such policy; and
6.3.5. Perform regular testing of disaster recovery capabilities, including operational tests and full tests.

Customer may request no more than once per year, and CUBE shall provide, a summary of CUBE's disaster recovery testing results.

7. Vendor Risk Management. CUBE will maintain policies, procedures, and/or processes regarding CUBE vendors and suppliers, including the requirement for CUBE to perform certain reviews and/or validations, including, but not limited to:
7.1. Conducting searches across sanction and watch lists;
7.2. Performing checks to assess vendors' financial health;
7.3. Requiring vendor to complete code of conduct declaration;
7.4. Conducting review of adverse media;
7.5. Re-perform certain reviews and/or validations on a periodic basis; and
7.6. As reasonably determined by CUBE, conduct regular service review meetings.