DATA SECURITY PROCESSES AND TERMS

1. DEFINITIONS.

(a) "Security Incident" means an event or series of events in which an unauthorized third party has accessed, compromised, misappropriated, destroyed, altered, received, or disclosed Customer Data.

(b) Capitalized terms not otherwise defined in this Data Security Addendum have the meaning ascribed to them in the Agreement.

2. SECURITY PROGRAM.

(a) **Generally.**

(i) OneStream has developed and implemented, and will maintain, monitor, and comply with, a comprehensive, written information security program that contains appropriate administrative, technical, and organizational safeguards designed to protect against Security Incidents. This program is based on NIST and ISO27001 requirements.

(ii) OneStream will review and, as appropriate, revise its information security program at least annually or whenever there is a material change in OneStream's business practices that can reasonably be expected to affect its security, confidentiality, availability, or integrity. During the Term, OneStream will not revise its information security program in a manner that could reasonably be expected to materially reduce protections of Customer Data.

(iii) OneStream will not alter or modify its information security program in a way that is materially likely to weaken or compromise the confidentiality, integrity, availability, or security of Customer Data.

(b) **Encryption.** Where the Service permits, OneStream will implement encryption as described in the Documentation, and will not, without Customer's consent, decrease any level of encryption with respect to Customer Data. Per the foregoing, OneStream currently uses TLS 1.2 for encryption in transit. Data at rest in Azure storage is protected by 256-bit AES encryption and Azure SQL Database is protected via transparent data encryption (TDE) that uses AES256.

(c) **Acceptable Use.** OneStream will implement rules for the acceptable use of information and assets consistent with the requirements of this Attachment. OneStream shall comply with all law with respect to privacy and data protection that applies to OneStream.

(d) **Security Awareness Training.** OneStream will, at least annually, conduct security awareness training for its personnel that is appropriate to the job functions of such personnel.

(e) **Control of Access Rights.** OneStream will disable user accounts and other access by its individual personnel to Customer Data within 24 hours after the termination of such individual's employment, contract, or agreement. OneStream will revise its individual personnel access to Customer Data within 24 hours after any change to such individual's role and privileges with respect to such Customer Data.

(f) **Screening.** Prior to an individual employee or agent of OneStream having access to Customer Data, OneStream will conduct a criminal background check and other screening appropriate to the role of the individual and any access to Customer Data.

(g) **Physical Security.**

(i) OneStream will restrict access to OneStream's facilities to personnel having actual need to have such access.

(ii) OneStream will implement and enforce clean-desk, clear-screen, and similar processes.

3. ASSESSMENTS AND AUDITS

(a) OneStream will, at least annually, cause an independent third-party provider to conduct penetration tests of the then-current release and version of the Service. OneStream will remediate any critical vulnerability revealed by such penetration test within 30 days after receipt of the report identifying such vulnerability, upon validation by OneStream.

(b) OneStream will, at least annually, cause a third party to perform an audit of OneStream's own systems used to process Customer Data, as contemplated by Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and produce a Service Organization Control 2 Type II report (each an "Audit Report") of such audit's findings.

(c) OneStream will make available to Customer each Audit Report upon request, subject to Customer's undertaking of such confidentiality obligations as the auditor requires.

(d) OneStream will promptly address any deficiency identified in an Audit Report.

(e) OneStream will make available to Customer such audit results and similar security information as OneStream is entitled to receive from its vendors and contracting parties that bear on the processing of Customer Data, including, but not limited to, such audit results as are available from its service providers. Where any such vendor or contracting party imposes confidentiality or non-use restrictions on such information, Customer will comply with such restrictions and will, if required, execute and deliver to such auditor any undertaking of confidentiality that the auditor requires.

(f) Customer may audit OneStream's own books, records, and facilities as follows:

(i) Any such audit will be subject to a mutually agreed written scope. No audit scope will include any matter covered by the then-current Audit Report unless that matter is subject to a finding by the auditor in the Audit Report of non-conformity with the management statements underlying the Audit Report.

(ii) Any such audit will take place with at least 10 business days' notice and be conducted in a manner reasonably calculated to avoid or minimize disruptions to OneStream's operations and the operations of OneStream's other customers.

(iii) Customer will bear all costs of such audits.

(iv) Customer may engage a qualified third party to conduct the audit, provided that the third party undertakes confidentiality obligations to OneStream that are at least as robust as those contained in this Agreement.

(v) OneStream will use commercially reasonable efforts to facilitate each audit and cooperate with Customer, including, within the agreed scope of the audit, access to equipment, applications, and systems used by OneStream and OneStream personnel.

4. COMMUNICATIONS AND OPERATIONS MANAGEMENT

(a) **Protections Against Malicious Code.** OneStream will implement detection, prevention, and recovery controls designed to protect against malicious code, including, but not limited to:

(i) Deploying malicious code detection and scanning on all systems commonly affected by malicious code (such as workstations and servers);

(ii) Installing security patches according to OneStream's evaluation of the threat level addressed by such patches; and

(iii) Maintaining a regular security patch process in accordance with industry standards.

(b) **Monitoring.**

(i) OneStream will employ security controls and tools to monitor systems used to provide the Service(s) and log user activities, exceptions, unauthorized information processing activities, suspicious activities, and information security events.

(ii) OneStream will maintain facilities and log information:

(A) In a manner designed to prevent tampering and unauthorized access; and

(B) For a period of at least 90 days.

(iii) OneStream will synchronize the clocks of all relevant information processing systems using an authoritative national or international time source.

5. ACCESS CONTROL

(a) **User Access Management.** OneStream will:

(i) Employ formal procedures for granting and revoking access to OneStream's systems used to provide the Services;

(ii) Employ a formal password management process in accordance with industry standards; and

(iii) Perform recurring reviews of users' access rights.

(b) **User Responsibilities.** OneStream will:

(i) Restrict access to systems and applications storing or transmitting Customer Data by OneStream to only those individuals whose role requires such access based on need-to-know and need-to-access;

(ii) Require screen timeout, screen locking, and other industry-standard measures to be used with respect to OneStream workstations used to access or process Customer Data;

(iii) Submit a written request for the access to Customer Data and receive consent for the access; and

(iv) Implement policies prohibiting OneStream personnel from sending, uploading, removing on portable media, or otherwise transferring Customer Data to a non-OneStream system (other than a system used by OneStream under contract to provide storage and computing resources) except where Customer directs, or consents to, such activity.

(c) **Operating System Access Control.** OneStream will:

(i) Require secure login procedures to access operating systems;

(ii) Require that users use unique user IDs

(iii) Restrict the use of utility programs that can override system and application controls to circumstances where such use is required; and

(iv) Shut down inactive sessions after a defined period of inactivity.

6. SECURITY INCIDENTS

(a) OneStream will:

(i) Implement a process to report Security Incidents through appropriate management channels as soon as possible;

(ii) Train all personnel and users of information systems and services how to report any observed or suspected Security Incidents;

(iii) Notify Customer without undue delay which in no event shall be greater than 48 hours of determination that a Security Incident has occurred or is likely to have occurred and provide to Customer, upon request, a reasonably detailed incident report;

(iv) Cooperate in good faith with Customer to remedy or mitigate the impact of any Security Incident and retain for at least the period required by applicable law all information in OneStream's possession or control that reasonably relates to each Security Incident; and

(v) Log all Security Incidents.

(b) Customer must report Security Incidents to OneStream promptly on becoming aware of it by opening a support ticket.

7. DISASTER RECOVERY

(a) OneStream will maintain appropriate business-continuity and disaster-recovery procedures and systems to maintain the availability, integrity, confidentiality, and security of the systems used to provide the Service(s). During the Term, OneStream will not revise its business-continuity and disaster-recovery procedures in a manner that could reasonably be expected to materially degrade OneStream's ability to resume operations in the case of a disaster.

8. THIRD-PARTY DEMANDS

(a) To the extent not prohibited by law:

(i) OneStream will notify Customer of any warrant, subpoena, or other third-party demand made on OneStream regarding any Customer Data promptly after receipt; and

(ii) OneStream will comply with any preservation requests by Customer regarding Customer Data and will provide support for Customer's efforts to comply with third party requests if Customer cannot otherwise reasonably obtain such information.

(b) If the services required to comply with this Section 8 are not otherwise included in the Service(s), Customer will pay to OneStream OneStream's then-current (but in any case, commercially reasonable) rates for such services.

9. BACK-UP AND RETENTION

(a) OneStream will:
  (i) Conduct incremental daily and full weekly backups of user and system-level information contained in the information system, as well as information system documentation and security related documentation;
  (ii) Backup Customer Data, utilizing Microsoft Azure SQL platform databases;
  (iii) Back-up transactions to the minute within the Customer's primary Microsoft Azure datacenter. These are replicated to a sister datacenter automatically; and
  (iv) Conduct, once per week, full backups to the secondary Microsoft Azure datacenter.

(b) Weekly full backups are retained for 52 weeks.

10. DATA RETURN

(a) Per the timelines and terms as specified in Section 10.(c)(ii) of the Agreement, upon expiration or termination of the Applicable Term, Customer may request the return of Customer Data and OneStream shall provide a backup of the database file(s).

11. VENDOR RISK MANAGEMENT

(a) Management of third-party vendors and service providers is addressed through the vendor management policy and procedures.

(b) On an annual basis, OneStream performs a review of critical 3rd and 4th party vendors to validate the design and operating effectiveness of their controls.

(c) OneStream will advise customers of any significant and material changes to key suppliers that may have an impact on customer data and implementation.

(d) Vendor Management practices are in line with industry best practices.