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 anticipated threats or hazards to the confidentiality, integrity, or availability of Customer Data.

(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.

(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 Service.

(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 the Service. Per the foregoing, Transport Layer Security (TLS) 1.2 is used to encrypt data in transit. Data at rest is encrypted using AES-256.

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

(f) **Physical Security.** OneStream's physical locations are physically and logically separated from OneStream's Service. The OneStream Service is hosted via a cloud hosting service provider. OneStream performs a review of the cloud hosting service provider at least annually to ensure physical protections are met in accordance with industry standards.

3. ASSESSMENTS AND AUDITS

(a) OneStream will, at least annually, cause an independent third-party provider to conduct penetration tests on a similar environment of the then-current release and version of the Service.

(b) OneStream will cause a third party to perform a Standards for Attestation Engagements No. 18 (SSAE 18) audit, or any successor authoritative guidance for reporting on service organizations, at least once a year during the term of this Agreement, and will make available to Customer, at least annually, a copy of the reports OneStream receives related to compliance with SSAE 18 (e.g., SOC 1 Type II, SOC 2 Type II).

(c) During the term of the Agreement, OneStream shall endeavor to maintain its certificate of registration for International Organization for Standardization's standards: ISO/IEC 27001:2013 (or later version) – Information Security Management Systems.

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

(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) OneStream acknowledges that Customer may be required to conduct regular due diligence of its suppliers, and OneStream, in its role as a supplier, will use commercially reasonable efforts to cooperate with third-party assessments requested by Customer, with 30 days' written notice, as it relates to Service(s) performed. Any such audit will be subject to a mutually agreed upon 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. Customer will bear all costs of such audit.

4. COMMUNICATIONS AND OPERATIONS MANAGEMENT

(a) **Patch Management**. OneStream maintains a standard maintenance window to apply patches and other fixes. OneStream conducts regression testing of underlying patches in an OneStream test environment prior to introducing to the Service environment. If a critical update is necessary for security purposes, OneStream will notify Customer and take action to perform the updates as soon as possible irrespective of the standard maintenance window.

(b) **Protections Against Malicious Code.** OneStream will implement detection, prevention, and recovery controls designed to protect against malicious code, including, but not limited to deploying malicious code detection and scanning on systems commonly affected by malicious code (e.g., servers).

(c) **Boundary Protections.** OneStream has adopted a defense-in-depth approach to boundary protection, which includes network security groups (NSGs), load balancers, subnets, and a tiered architecture to ensure data flow is controlled and authorized in accordance with industry best practices. Inbound network traffic is only permitted using specific network protocols and ports based on the minimum requirements to operate the Service(s).

(d) **Logging & Monitoring.** OneStream will employ security controls and tools to monitor systems used to provide the Service(s) and log relevant information security events. OneStream will review anomalies from security and security related audit logs and resolve logged security problems in a timely manner. OneStream will maintain log information in a manner designed to prevent tampering and unauthorized access and for a period of at least one year.

5. ACCESS CONTROL, IDENTIFICATION, AND AUTHENTICATION

(a) OneStream will restrict access to systems used to provide the Service(s) to authorized OneStream personnel whose role requires such access and based on the principle of least privilege. The Customer is responsible for Service account management, including the creation, modification, enabling, disabling, and removal of user accounts to the Service.

(b) OneStream provisions named user accounts for all authorized OneStream personnel. OneStream requires passwords be of sufficient strength, minimally adhering to NIST SP 800-63B password guidelines. Multifactor authentication (MFA) is required for all individual OneStream user accounts. OneStream personnel do not control or manage Customer identification and/or authentication to their OneStream application. The Customer is responsible for configuring and managing their SSO provider or Customer may opt to use native authentication.

(c) OneStream performs periodic system access reviews to ensure OneStream personnel maintain appropriate access. OneStream will disable user accounts and other access by its individual personnel to OneStream systems used to provide the Service(s) within 24 hours after the termination of such individual's employment. OneStream will modify user access to OneStream systems used to provide the Service(s) within 24 hours after any change to such individual's role and privileges with respect to the Service.

6. VULNERABILITY MANAGEMENT

(a) OneStream has developed and maintained a threat and vulnerability management program responsible for identifying vulnerabilities and risks for the systems used to provide the Service(s) and ensuring the timely implementation of security updates, patches, and configuration changes to address the security concern. Vulnerabilities must be corrected either directly by solving the vulnerability, or by developing or applying compensatory controls to mitigate the risk. For security vulnerabilities with a risk or severity rating of critical, high, or moderate, OneStream will apply appropriate security patches or otherwise render the vulnerability not exploitable within documented commercially reasonable timeframes.

7. SECURITY INCIDENTS

(a) To ensure a consistent process for identifying, reporting, investigating, and closing Security Incidents, OneStream will develop, implement, document, maintain and comply with a Security Incident reporting process for the Service.

(b) OneStream requires its personnel to promptly notify management in the event it has a reasonable belief that a Security Incident has taken place. If Customer suspects a Security Incident, Customer must promptly report the Security Incident(s) to OneStream via a support ticket.

(c) On notice of any Security Incident, OneStream will:

(i) Contain and remedy the Security Incident or mitigate the impact of any Security Incident;

(ii) Take reasonable steps to prevent any further Security Incidents associated with current Security Incident;

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

(e) OneStream will 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.

8. 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.

9. BACK-UP AND RETENTION

(a) OneStream maintains a robust automatic backup system, ensuring continuity of the Service(s) in the event of unexpected failure or disaster. Databases are automatically backed up at the transaction level to allow for Point in Time Recovery (or "PITR") for the trailing seven (7) day period. In addition to PITR backups, databases also have weekly "snapshots" for long-term retention (or "LTR") for the trailing fifty-two (52) week period, subject to the Documentation.

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) OneStream maintains a vendor risk management program that is in line with industry best practices. On an annual basis, OneStream performs a review of critical vendors for the Service to validate the design and operating effectiveness of their controls.

12. 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.