ONESTREAM XF CLOUD AGREEMENT

This OneStream XF Cloud Agreement (together with the Attachments to this OneStream XF Cloud Agreement, this "Agreement") is between the following parties and is effective as of the date of last signature below (the "Effective Date"). Any term in this Agreement that has initial capitals and isn't defined in this Agreement will have the meaning given to it by the Perpetual License Agreement or Subscription License Agreement, as applicable.

1. **DEFINED TERMS**.

(a) "Software" has the meaning given to that term by the Software License and Services Agreement or Subscription License Agreement between Customer and OneStream.

(b) "Cloud System" means the hardware, software, and systems (whether owned and operated by OneStream or otherwise) that OneStream uses to provide the functionality of the Software at the Demarcation Point.

(c) "Data Processing Terms" means the terms found at https://www.onestream.com/saas-terms-and-conditions/ with respect to OneStream's processing of "Personal Data" as defined in the Data Processing Terms.

(d) "Demarcation Point" means the outermost point on the Cloud System's firewall with the public Internet.

(e) "Cloud Services" means the provision by OneStream of the Software at the Demarcation Point, using the Cloud System, according to the service levels identified in Attachment C.

(f) "Customer Data" means information that Customer provides for (i) loading on the Cloud System and/or (ii) storage or processing using the Software on the Cloud System.

2. **CLOUD SERVICES**.

(a) OneStream will provide to Customer, and Customer will procure from OneStream, the Cloud Services for the purposes of running and accessing the Software. Customer may permit its Covered Entities to use the Cloud Services for the purpose of accessing and using the Software to the extent permitted by the Software License and Services Agreement or Subscription License Agreement.

(b) OneStream will provide the Cloud Services according to the service levels stated in Attachment C.

(c) OneStream will, within a commercially reasonable time, inform Customer of maintenance windows for the Cloud Services. OneStream may inform Customer of maintenance windows by posting to a customer portal or other means reasonably likely to give Customer actual notice of the maintenance windows. Without limiting the foregoing, OneStream will have timely informed Customer of a maintenance window if OneStream posts or makes such information available within 24 hours after the provider of the Cloud System makes available such information. During any such windows, the services levels in Attachment C will not apply. If Customer chooses to delay or decline a maintenance window, service levels will not apply until maintenance is performed.

(d) Customer will use the Cloud Services according to OneStream's then-current Acceptable Use Policy. The Acceptable Use Policy current as of the Effective Date is attached as Attachment D. The Acceptable Use Policy will automatically update if and when, and the same extent that, the provider of the Cloud System updates its acceptable use policy. OneStream may suspend or terminate Customer's access to the Cloud Services during any non-compliance by Customer with the Acceptable Use Policy. OneStream will use commercially reasonable efforts to afford Customer notice and an opportunity to cure its failure to comply with the Acceptable Use Policy but no such notice or opportunity to cure will apply where the provider of the Cloud System requires that OneStream suspend or terminate Customer's access to the Cloud Services, or the provider of the Cloud Services communicates to OneStream that Customer's acts or omissions jeopardize OneStream's ability to provide cloud services to OneStream's other customers. Fees for Cloud Services and Maintenance will continue unabated during any such suspension.

3. **MANAGEMENT SERVICES**.

(a) OneStream will provide the following services to manage the Software and the environment of the Cloud Services (the "Management Services"):

(i) Monitor and maintain Customer environmental health;
(ii) Perform monthly Windows Server updates;
(iii) Perform OneStream Software Upgrades;
(iv) Perform environment resizing (up/down if needed/ requested);
(v) Perform database optimization;
(vi) Create, copy, delete, and restore applications and/or databases, as applicable;
(vii) Notify Customer of any planned maintenance windows;
(viii) Configure a site-to-site VPN or express route connection;
(ix) Create, configure, and maintain OneStream environment;

(b) Customer must provide the following services to ensure proper functionality of the Software:

(i) Customer side configuration, facilitation, and connection of any required VPN connection to the Cloud Services.
(ii) Provisioning of and connection information for any required private circuit (Microsoft ExpressRoute, etc.).
(iii) Any required Customer specific encryption certificate information.
(iv) Distribution of Customer side Software, components, or add-ins of the Software to individual users.

(c) Customer is responsible for the following items:

(i) Approve all changes to environment
(ii) User ID management
(iii) Approve access to Customer's OneStream applications.
(iv) Testing of new releases in Customer environment
(v) Maintaining business rules (formulas)
(vi) Testing and production promotion of Customer data and business rule sets.
(vii) Declaration of network addressing schema
(viii) Ordering and installation of WAN circuit (if applicable)

4. **TERMINATION OF CLOUD SERVICES AND MANAGEMENT SERVICES**.

(a) Termination Generally. Customer may terminate Cloud Services and Management Services with at least 30 days' notice to OneStream and OneStream may terminate Cloud Services and Management Services with at least 180 days' notice to Customer.

(b) Transition Services; Notice. If Customer gives to OneStream notice at least 30 days prior to the effective date of termination of Cloud Services that Customer requires OneStream's assistance to transition from the Cloud Services to an alternative provider of cloud services or moving the Software to Customer's own internal systems (such notice being the "Transition Services Notice"), OneStream will, until the effective date of termination, use commercially reasonable efforts to assist with the transition ("Transition Services"). Customer may give the Transition Services Notice concurrently with the notice of termination of Cloud Services.

(i) Where such Transition Services include engineering or professional services by OneStream in excess of the ongoing Management Services associated with the relevant period, Customer will pay OneStream for such services at OneStream's then-current commercially reasonable professional services rates.

(ii) To the extent that the Cloud System consists of hardware, software, and/or systems of a third party and Customer desires that OneStream transfer to Customer such services, OneStream will use commercially reasonable efforts to assign or otherwise transfer to Customer the

contractual arrangements in place with the third-party systems provider with respect to the Cloud Services. In such a case:

(A) Customer will pay any charges required by the third-party systems provider for the transfer and any actual costs of accomplishing the transfer; and

(B) Customer understands that any volume discounts or similar arrangements (including, but not limited to, shared servers or other economies of scale) resulting from OneStream's provision of the Cloud Services might not transfer to, or benefit, Customer if Customer transfers from the Cloud Services under this Agreement. OneStream will, upon request by Customer, use commercially reasonable efforts to obtain, for Customer, fees and other estimates for transition of goods, services, and/or software.

(c) Where no Transition Services are Requested. For the avoidance of doubt, where Customer does not timely give the Transition Services Notice, OneStream need only provide the Cloud Services and Management Services through the effective date of termination of the Cloud Services and will have no further obligations to provide Cloud Services or Management Services thereafter.

(d) When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act) and FAR 52.233-1. During any dispute under the Disputes Clause, OneStream shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement

5. **INFORMATION SECURITY**.

(a) OneStream will carry out the processes, according to the terms, in Attachment B.

(b) OneStream will process Customer Data which contains Personal Data in accordance with the Data Processing Terms.

6. **FEES**.

(a) Cloud Services. OneStream will invoice monthly in arrears for Cloud Services and all such invoices are payable within 30 days of invoice date.

(b) Management Services. Customer will pay to OneStream the fees for Management Services as identified in the applicable Order Schedule in Attachment A or other document agreed upon by the parties. These fees will be billed on a monthly basis for the current month. All fees are due 30 days from the receipt of the invoice.

7. **INDEMNIFICATION.**

(a) OneStream will defend Customer against any claims made by an unaffiliated third party that the Cloud Services infringe its patent, copyright, or trademark or makes unlawful use of its trade secret. OneStream will pay the amount of any resulting adverse final judgment or approved settlement. This does not apply to claims or awards based on (i) information that Customer provides, (ii) Customer modifications to the Cloud Services or Management Services, (iii) Customer's combination of the Cloud Services or Management Services with (or damages based on the value of) a product, data, or business process not supplied by OneStream, or (iv) Customer's continued use of the Cloud Services or Management Services after being notified to stop due to a third-party claim.

(b) If OneStream reasonably believes that a claim under Section 7(a) may bar Customer's use of the Software, OneStream may attempt to: (i) obtain the right for Customer to keep using it; or (ii) modify or replace it with a functional equivalent. If these options are not commercially reasonable, OneStream may terminate Customer's rights to use the Cloud Services and Management Services and refund any advance payments for unused Cloud Services and Management Services.

(c) Customer must promptly notify OneStream of any claim of the kind described in Section 7(a) and:

(i) Give to OneStream sole control over the defense and settlement of the claim;

(ii) Give to OneStream reasonable help in defending the claim.

(d) In the case of such a claim, OneStream will (i) reimburse Customer for reasonable out-of-pocket expenses that Customer incurs in giving that help, and (ii) pay the amount of any resulting adverse final judgment (or settlement to which Customer consents, it being understood that Customer will not unreasonably withhold, delay, or condition any such consent).

(e) Customer's rights to defense and payment of judgments or settlements under this Section 7 are in lieu of any common law or statutory indemnification rights or analogous rights, and Customer waives any such common law rights.

(f) Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

8. **CONFIDENTIALITY**.

(a) "Confidential Information" Defined. "Confidential Information" of a party means any information belonging to, or held by, the party, whether fixed in a tangible medium or otherwise, that is:

(i) Not readily ascertainable by proper means by the public; and

(ii) The subject of commercially reasonable efforts by the party under the circumstances to keep it from becoming readily ascertainable by proper means by the public.

(b) Confidentiality and Use Generally. Each party, as a receiving party, will do the following things with regard to the Confidential Information of the other party.

(i) Prevent the disclosure of the Confidential Information by the receiving party and each of the receiving party's employees, agents, and/or professionals to any third-party other than as permitted under this Agreement.

(ii) Use, and permit the use of, the Confidential Information only for the purposes of providing, or enjoying the benefit of, the goods, services, and/or software provided for in this Agreement (the "Purpose").

(iii) Disclose the Confidential Information only to such of the receiving party's employees, agents, and professionals as have a bona fide need to possess or know the Confidential Information in the course of accomplishing, or advising the disclosing party with regard to, the Purpose.

(iv) Cause each employee, agent, or professional to whom the receiving party discloses the Confidential Information to be bound by an obligation of confidentiality that is at least as rigorous as the obligations contained in this Agreement. Each professional, such as a lawyer or an accountant, actually retained by the receiving party in a professional-client relationship will be deemed under an adequate obligation of confidentiality for the purposes of this Agreement so long as the law recognizes an obligation of confidence actionable by the receiving party under law without a separate contractual obligation.

(v) Return or destroy all written or other tangible copies of Confidential Information in the receiving party's possession or direct or indirect control, including all extracts and copies thereof, within a reasonable time after, and in accordance with, the disclosing party's request.

(c) Exceptions to Confidentiality and Use Restrictions. Nothing in this Agreement will prevent the receiving party from disclosing or using Confidential Information to the extent that:

(i) It is or becomes readily ascertainable by proper means by the public without any breach of a confidentiality obligation of the receiving party;

(ii) It is received from a third party that is not under an obligation of confidentiality of which the receiving party knew or had reason to know;

(iii) It was independently developed by the receiving party without use of the Confidential Information; or

(iv) It is required by law to be disclosed, provided that the receiving party provides to the disclosing party as much notice as is practicable under the circumstances of such requirement prior to disclosure and provides to the disclosing party, at the disclosing party's expense, such reasonable assistance as the disclosing party requests in seeking confidential treatment, protective orders, nondisclosure, and/or similar measures.

(d) Reserved.

(e) Duration of Confidentiality Obligations. The confidentiality obligations under this Agreement will continue after disclosure of each item of Confidential Information for the longer of:

(i) The time during which the Confidential Information remains a trade secret (as that term is defined in the Uniform Trade Secrets Act) of the disclosing party; or

(ii) Five years after the earlier of the termination of this Agreement or the effective date of the termination of Cloud Services and Management Services.

(f) This Section 8 will apply to Customer Data that is Customer's Confidential Information to the extent that OneStream actually accesses or processes the Customer Data outside of the Cloud System. Otherwise, Section 5 applies to such Customer Data.

(g) OneStream recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor

9. **LIMITATION OF OBLIGATIONS AND REMEDIES**.

(a) Limitations Generally. To the maximum extent permitted by law, except in the case of OneStream's gross negligence, willful misconduct, indemnification obligation, or breach of OneStream's obligations under Section 8, regardless of the basis of recovery claimed, whether in contract, tort, negligence, strict liability or other theory:

(i) ONESTREAM'S AGGREGATE LIABILITY WITH RESPECT TO THE SUBJECT MATTER OF THE AGREEMENT WILL BE LIMITED TO THE AMOUNT OF FEES PAID BY CUSTOMER FOR THE LAST 12 MONTHS OF SUBSCRIPTION FEES (OR, IF 12 MONTHS HAVE NOT BY THEN PASSED, THE AMOUNT THAT WOULD HAVE BEEN PAYABLE HAD THE TERM OF THE AGREEMENT RUN 12 MONTHS); and

(ii) ONESTREAM WILL NOT BE LIABLE FOR LOSS OF PROFITS, OR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES.

(b) The limitations of liability in this Section 9 will apply notwithstanding that OneStream knew, or should have known, of the possibility of any particular damages and notwithstanding that any limitation causes any remedy to fail of its essential purpose.

10. GENERAL.

(a) Choice of Law; Jurisdiction; Venue. The Agreement shall be governed by and construed under the Federal laws of the United States. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act are specifically excluded from application to this Agreement.

(b) Anti-Bribery; Anti-Corruption. Each party will, and will cause its subcontractors, employees, directors, and officers, to comply with all applicable laws, statutes, and regulations relating to bribery and corruption, including but not limited to, the U.S. Foreign Corrupt Practices Act and the UK Bribery Act 2010 (each an "Anti-Bribery Law"). The parties shall not engage in any activity, practice or conduct which would constitute an offense or could incur liability for the other party under Anti-Bribery Laws. Each party shall have, maintain and enforce, throughout the term of this Agreement, its own policies and procedures to ensure compliance with the Anti-Bribery Laws. For the avoidance of any doubt, any amounts paid by Customer pursuant to the terms of this Agreement will be for Cloud Services and Maintenance Services provided, and/or other fees incurred in accordance with the terms of this Agreement. Each party shall not, and shall ensure that its subcontractors, employees, officers and directors do not, accept bribes or kickbacks in any form. Each party, their subcontractors, employees, officers and directors shall be responsible for the observance and performance by such persons of the Anti-Bribery Laws and shall be directly liable to the other party for any breach by such persons of any of the Anti-Bribery Laws.

(c) Import/Export.

(i) Each Software, System and/or Service is subject to U.S. and international laws, restrictions, and regulations that may govern the import, export, and use of the Software, System and/or Service ("Export Laws"). Each party agrees to comply with Export Laws that apply to such party's use or provision of each Software, System and/or Service.

(ii) Customer represents and warrants that neither it nor any Permitted Entity or Authorized User is (A) an entity barred by the applicable Export Laws from participating in export activities (each a "Barred Entity") or (B) owned or controlled by a Barred Entity. A Barred Entity includes, but is not limited to, an entity located in any country subject to an embargo or other sanctions by the U.S. Government ("Embargoed Country"), which currently includes Cuba, Iran, North Korea, Russia, Syria, and Covered Regions of Ukraine (Crimea, Donetsk and Luhansk), or an entity designated on a "Denied Party List" maintained by the U.S. Government, including, but not limited to the U.S. Treasury Department's Specially Designated National's List administered by the Office of Foreign Assets Control and the U.S. Commerce Department's Entity List administered by the Bureau of Industry and Security.

(iii) Customer will not export, re- export, transfer, or otherwise use the export-controlled products in any Embargoed Country or allow any of its employees and affiliates to access any Software, System and/or Service from any Embargoed Country.

(iv) Customer will not export, re-export, or transfer, either directly or indirectly, any Software, System and/or Service to a Barred Entity or allow a Barred Entity to access any Software, System and/or Service.

(v) Customer will not use any Software, System and/or Service for any purpose prohibited by Export Laws, including, but not limited to, the design, development, or production of nuclear, chemical, or biological weapons, or rocket systems, space launch vehicles, sounding rockets, or unmanned air vehicle systems.

(d) Service Organization Control Reports (SOC). At least annually and at its expense, OneStream will have an independent certified public accounting firm (or similarly qualified person) conduct a review of OneStream's operations and procedures related to its information systems, and the other material aspects of control of the services and the system locations used to provide Services to Customer under this Agreement. OneStream will make available

to Customer the SOC 1 Type II report and/or SOC 2 Type II report on an annual basis.

(e) All notices must be in writing and shall be deemed delivered upon receipt when delivered personally or upon confirmation of receipt following delivery by (i) internationally-recognized overnight courier service or (ii) registered or certified mail, return receipt requested, postage prepaid, in each case addressed to the Legal Department at the receiving party's corporate headquarters or alternate notice address requested in writing.

(f) If a provision of this Agreement or portion thereof is invalid or unenforceable under applicable law, it shall be omitted from this Agreement without invalidating the remainder of this Agreement.

(g) The waiver by either party of any default or breach of any provision of this Agreement shall not constitute a waiver of any other or subsequent default or breach.

(h) All materials provided by OneStream hereunder shall be delivered to Licensee on a F.O.B. shipping point basis, including electronic posting for download.

(i) The provisions of this Agreement shall be binding upon and inure to the benefit of the parties, their successors and permitted assigns.

(j) Except for actions for nonpayment or breach of OneStream's proprietary rights, no action, regardless of form, arising out of this Agreement may be brought by either party more than one year after a party knew or should have known of the claim.

(k) Excusable delays shall be governed by FAR 52.212-4(f).

(l) The Agreement, including all attachments and documents incorporated by reference, represents the entire agreement between the parties with respect to the subject matter of this Agreement, and this Agreement expressly supersedes any other agreements, whether oral or written, with respect to the subject matter of this Agreement. Each party acknowledges that it is not entering into this Agreement on the basis of any representations or warranties not expressly contained in this Agreement. Other than as specified in this Agreement, this Agreement may only be supplemented or modified by an amendment in a writing executed by the party against whom enforcement is sought. For the avoidance of doubt, this Agreement on the one hand and the Subscription License Agreement or other agreement executed and delivered by OneStream and Customer will, to the extent possible, be construed consistently one with the other. Where such construction is not possible, the provisions of this Agreement will control.

Attachment B

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.

(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) In an effort to maintain its FedRAMP authorization, OneStream will engage an accredited third-party assessment organization ("3PAO") at least annually to assess the security controls of the Service to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements per FedRAMP guidelines. OneStream will make available to Customer a copy of the security assessment report that documents the results of the assessment.

(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 virtual firewall appliances, 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 8 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 1 hour 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.

Attachment C

Service Level Agreement

Introduction

About this Document

This Service Level Agreement ("SLA") applies to the Cloud Services, but does not apply to separately-branded services made available with, or connected to, the Services or to any on-premise installation of the Software.

If OneStream does not achieve and maintain the Cloud Services as described in this SLA, then Customer may be eligible for a credit toward a portion of Customer's monthly service fees. OneStream will post any modification of this SLA in OneStream's customer portal or other appropriate place reasonably calculated to give Customer actual notice of the new SLA. Any adverse change to the SLA will not become effective until at least 90 days after OneStream gives notice of the new SLA or posts the new SLA in OneStream's customer portal or other appropriate place reasonably calculated to give Customer actual notice of the new SLA.

General Terms

Definitions

"**Applicable Monthly Period**" means, for a calendar month in which a Service Credit is owed, the number of days that you are a subscriber for a Service.

"**Applicable Monthly Service Fees**" means the total fees actually paid by you for a Service that are applied to the month in which a Service Credit is owed.

"**Downtime**" is defined for each Service in the Services Specific Terms below. Except for OneStream Azure Services, Downtime does not include Scheduled Downtime. Downtime does not include unavailability of a Service due to limitations described below and in the Services Specific Terms.

"**Error Code**" means an indication that an operation has failed, such as an HTTP status code in the 5xx range.

"**External Connectivity**" is bi-directional network traffic over supported protocols such as HTTP and HTTPS that can be sent and received from a public IP address.

"**Incident**" means (i) any single event, or (ii) any set of events, that result in Downtime.

"**Management Portal**" means the web interface, provided by OneStream, through which customers may manage the Service.

"**Scheduled Downtime**" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five days prior to the commencement of such Downtime.

"**Service Credit**" is the percentage of the Applicable Monthly Service Fees credited to you following OneStream's claim approval.

"**Service Level**" means the performance metric(s) set forth in this SLA that OneStream agrees to meet in the delivery of the Services.

"**Service Resource**" means an individual resource available for use within a Service.

"**Success Code**" means an indication that an operation has succeeded, such as an HTTP status code in the 2xx range.

"**Support Window**" refers to the period of time during which a Service feature or compatibility with a separate product or service is supported.

"**User Minutes**" means the total number of minutes in a month, less all Scheduled Downtime, multiplied by the total number of users.

Terms

Claims

In order for OneStream to consider a claim, Customer must submit the claim to customer support at OneStream including all information necessary for OneStream to validate the claim, including, but not limited to: (i) a detailed description of the Incident; (ii) information regarding the time and duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence.

OneStream must receive the claim by the end of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 15th, OneStream must receive the claim and all required information by March 31st.

OneStream will evaluate all information reasonably available to OneStream and make a good faith determination of whether a Service Credit is owed. OneStream will use commercially reasonable efforts to process claims during the subsequent month and within 45 days of receipt. Customer must be in compliance with the OneStream XF Cloud Agreement and all other agreements between Customer and OneStream in order to be eligible for a Service Credit. If OneStream determines that a Service Credit is owed to Customer, OneStream will apply the Service Credit to Customer's Applicable Monthly Service Fees.

In the event that more than one Service Level is not met because of the same Incident, Customer must choose only one Service Level under which to make a claim based on the Incident.

Service Credits

Service Credits are Customer's sole and exclusive remedy for any performance or availability issues for any service under the OneStream XF Cloud Agreement. Customer may not unilaterally offset Customer's Applicable Monthly Service Fees for any performance or availability issues.

In cases where Service Levels apply to individual Service Resources or to separate Service tiers, Service Credits apply only to fees paid for the affected Service Resource or Service tier, as applicable. The Service Credits awarded in any billing month for a particular Service or Service Resource will not, under any circumstance, exceed Customer's monthly Service fees for that Service or Service Resource, as applicable, in the billing month.

If Customer purchased Services as part of a suite or other single offer, the Applicable Monthly Service Fees and Service Credit for each Service will be pro-rated.

Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside OneStream's reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to OneStream's or its vendor's data centers, including at Customer's site or between Customer's site and OneStream's or its vendor's data center);
2. That result from the use of services, hardware, or software not provided by OneStream, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
3. Caused by Customer's use of the Cloud Services after OneStream advised Customer to modify Customer's use of the Service, if Customer did not modify Customer's use as advised;
4. During or with respect to preview, pre-release, beta or trial versions of a Service, feature or Software (as determined by us) or to purchases made using OneStream subscription credits;
5. That result from Customer's unauthorized action or lack of action when required, or from Customer's employees, agents, contractors, or vendors, or anyone gaining access to OneStream's network by means of Customer's passwords or equipment, or otherwise resulting from Customer's failure to follow appropriate security practices;
6. That result from Customer's failure to adhere to any required configurations, use supported platforms, follow any Acceptable Use Policies, or Customer's use of the Cloud Services in a manner inconsistent with the features and functionality of the Cloud Services (for example, attempts to perform operations that are not supported) or inconsistent with OneStream's published guidance;
7. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
8. That result from Customer's attempts to perform operations that exceed prescribed quotas or that resulted from OneStream's throttling of suspected abusive behavior;
9. Due to Customer's use of Cloud Service features that are outside of associated Support Windows; or
10. For licenses reserved, but not paid for, at the time of the Incident.

Specific Service Levels

AD Domain Services

Additional Definitions:
"Managed Domain" refers to an Active Directory domain that is provisioned and managed by Azure Active Directory Domain Services.
"Maximum Available Minutes" is the total number of minutes that a given Managed Domain has been deployed by Customer in Microsoft Azure during a billing month in a given Microsoft Azure subscription.
"Downtime" is the total accumulated minutes during a billing month for a given Microsoft Azure subscription during which a given Managed Domain is unavailable. A minute is considered unavailable if all requests for domain authentication of user accounts belonging to the Managed Domain, LDAP bind to the root DSE, or DNS lookup of records, made from within the virtual network where the Managed Domain is enabled, either return an Error Code or fail to return a Success Code within 30 seconds.
"Monthly Uptime Percentage" is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Levels and Service Credits are applicable to Customer's use of Azure Active Directory Domain Services:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Azure Monitor

Additional Definitions:
"**Action Group**" is a collection of actions deployed by Customer in a given OneStream Azure subscription which defines preferred notification delivery methods.
"**Deployment Minutes**" is the total number of minutes that a given Action Group has been deployed by Customer in OneStream Azure subscription during a billing month.
"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Action Groups deployed by Customer in a given OneStream Azure subscription during a billing month.
"Downtime" is the total accumulated Deployment Minutes, across all Action Groups, during which the Action Group is unavailable. A minute is considered unavailable for a given Action Group if all continuous attempts to send alerts or perform registration management operations with respect to the Action Group throughout the minute either return an Error Code or do not result in a Success Code within five minutes.
"Monthly Uptime Percentage" is calculated as Maximum Available Minutes less Downtime divided by Maximum Available Minutes in a billing month for a given OneStream Azure subscription. Monthly Uptime Percentage is represented by the following formula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Levels and Service Credits:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Azure Security Center

Additional Definitions:
"**Protected Node**" is a OneStream Azure resource, counted as a node for billing purposes that is configured for the Azure Security Center Standard Tier

"**Security Monitoring**" is the assessment of a Protected Node resulting in potential findings such as security health status, recommendations, and security alerts, exposed in Azure Security Center.

"**Maximum Available Minutes**" is the total number of minutes during a billing month that a given Protected Node has been deployed and configured for Security Monitoring.

"**Downtime**" is the total accumulated minutes during a billing month for which Security Monitoring information of a given Protected Node is unavailable. A minute is considered unavailable for a given Protected Node if all continuous attempts to retrieve Security Monitoring information throughout the minute result in either an Error Code or do not return a Success Code within two minutes.

"Monthly Uptime Percentage" is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Backup Service

Additional Definitions:

"**Backup**" or "**Back Up**" is the process of copying computer data from a registered server to a Backup Vault.

"**Backup Agent**" refers to the software installed on a registered server that enables the registered server to Back Up or Restore one or more Protected Items.

"**Backup Vault**" refers to a container in which Customer may register one or more Protected Items for Backup.

"**Deployment Minutes**" is the total number of minutes during which a Protected Item has been scheduled for Backup to a Backup Vault.

"**Failure**" means that either the Backup Agent or the Service fails to fully complete a properly configured Backup or Recovery operation due to unavailability of the Backup Service.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Protected Items for a given OneStream Azure subscription during a billing month.

"**Protected Item**" refers to a collection of data, such as a volume, database, or virtual machine that has been scheduled for Backup to the Backup Service such that it is enumerated as a Protected Item in the Protected Items tab in the Recovery Services section of the Management Portal.

"**Recovery**" or "**Restore**" is the process of restoring computer data from a Backup Vault to a registered server.

"Downtime" The total accumulated Deployment Minutes across all Protected Items scheduled for Backup by Customer in a given OneStream Azure subscription during which the Backup Service is unavailable for the Protected Item. The Backup Service is considered unavailable for a given Protected Item from the first Failure to Back Up or Restore the Protected Item until the initiation of a successful Backup or Recovery of a Protected Item, provided that retries are continually attempted no less frequently than once every 30 minutes.

"Monthly Uptime Percentage" is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

ExpressRoute

Additional Definitions:

"**Dedicated Circuit**" means a logical representation of connectivity offered through the ExpressRoute Service between your premises and Microsoft Azure through an ExpressRoute connectivity provider, where such connectivity does not traverse the public Internet.

"**Maximum Available Minutes**" is the total number of minutes that a given Dedicated Circuit is linked to one or more Virtual Networks in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

"**Virtual Network**" refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within Microsoft Azure.

"**VPN Gateway**" refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

"Downtime" is the total accumulated minutes during a billing month for a given Microsoft Azure subscription during which the Dedicated Circuit is unavailable. A minute is considered unavailable for a given Dedicated Circuit if all attempts by you within the minute to establish IP-level connectivity to the VPN Gateway associated with the Virtual Network fail for longer than 30 seconds.

"Monthly Uptime Percentage" is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit The following Service Levels and Service Credits are applicable to Customer's use of each Dedicated Circuit within the ExpressRoute Service.

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

SQL Database Service (Basic, Standard and Premium Tiers)

Additional Definitions:

"**Availability Zone**" is a fault-isolated area within an Azure region, providing redundant power, cooling, and networking.

"**Database**" means any Microsoft Azure SQL Database created in any of the Service tiers and deployed either as a single database or in an Elastic Pool or Managed Instance.

"**Zone Redundant Deployment**" is a Database that includes multiple synchronized replicas provisioned in different Availability Zones.

"**Primary**" means any Database or managed instance that has active geo-replication relationship with a Database or managed instance in other Azure regions. Primary can process read and write requests from the application.

"**Secondary**" means any Database or managed instance that maintains asynchronous geo-replication relationship with Primary in another Azure region and can be used as a failover target. Secondary can process read-only requests from the application.

"**Compliant Secondary**" means any Secondary that is created with the same size and in the same service tier as the Primary. If the Secondary is created in an elastic pool, it is considered Compliant if both Primary and Secondary are created in elastic pools with matching configurations and with density not exceeding 250 databases.

"**Deployment Minutes**" is the total number of minutes that a given Database has been operational in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes for a given Microsoft Azure subscription during a billing month.

"**Downtime**" is the total accumulated Deployment Minutes across all Databases in a given Microsoft Azure subscription during which the Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts by Customer to establish a connection to the Database within the minute fail.

"**Monthly Uptime Percentage**" for a given Database is calculated as Maximum Available Minutes less Downtime divided by Maximum Available Minutes in a billing month for a given Microsoft Azure subscription. Monthly Uptime Percentage is represented by the following formula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

The following Service Levels and Service Credits are applicable to Customer's use of the Business critical or Premium tiers of the SQL Database Service configured for Zone Redundant Deployments:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.995%	10%
< 99%	25%
< 95%	100%

The following Service Levels and Service Credits are applicable to Customer's use of the Business critical or Premium tiers of the SQL Database Service not configured for Zone Redundant Deployments:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.99%	10%
< 99%	25%
< 95%	100%

The following Service Levels and Service Credits are applicable to Customer's use of the General purpose, Standard or Basic tiers of the SQL Database Service:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.99%	10%
< 99%	25%
< 95%	100%

The following Service Levels and Service Credits are applicable to Customer's use of the Hyperscale tier of the SQL Database Service.

PROVISIONED REPLICAS	MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
0	< 99.9%	10%
	< 99%	25%
1	< 99.95%	10%
	< 99%	25%
2+	< 99.99%	10%
	< 99%	25%
	< 95%	100%

Storage Service

Additional Definitions:

"**Average Error Rate**" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"Blob Storage Account" is a storage account specialized for storing data as blobs and provides the ability to specify an access tier indicating how frequently the data in that account is accessed.

"Cool Access Tier" is an attribute of a Blob Storage Account indicating that the data in the account is infrequently accessed and has a lower availability service level than data in other access tiers.

"**Excluded Transactions**" are storage transactions that do not count toward either Total Storage Transactions or Failed Storage Transactions. Excluded Transactions include pre-authentication failures; authentication failures; attempted transactions for storage accounts over their prescribed quotas; creation or deletion of containers, file shares, tables, or queues; clearing of queues; and copying blobs or files between storage accounts.

"**Error Rate**" is the total number of Failed Storage Transactions divided by the Total Storage Transactions during a set time interval (currently set at one hour). If the Total Storage Transactions in a given one hour interval is 0, the error rate for that interval is 0%.

"**Failed Storage Transactions**" is the set of all storage transactions within Total Storage Transactions that are not completed within the Maximum Processing Time associated with their respective transaction type, as specified in the table below. Maximum Processing Time includes only the time spent processing a transaction request within the Storage Service and does not include any time spent transferring the request to or from the Storage Service.

Request Types	Maximum Processing Time
PutBlob and GetBlob (includes blocks and pages) Get Valid Page Blob Ranges	Two seconds multiplied by the number of MBs transferred in the course of processing the request
PutFile and GetFile	Two seconds multiplied by the number of MBs transferred in the course of processing the request
Copy Blob	90 seconds (where the source and destination blobs are within the same storage account)
CopyFile	90 seconds (where the source and destination files are within the same storage account)
PutBlockList GetBlockList	60 seconds
Table Query List Operations	10 seconds (to complete processing or return a continuation)
Batch Table Operations	30 seconds
All Single Entity Table Operations All other Blob, File, and Message Operations	Two seconds

These figures represent maximum processing times. Actual and average times are expected to be much lower.

Failed Storage Transactions do not include:

1. Transaction requests that are throttled by the Storage Service due to a failure to obey appropriate back-off principles.
2. Transaction requests having timeouts set lower than the respective Maximum Processing Times specified above.
3. Read transactions requests to RA-GRS Accounts for which Customer did not attempt to execute the request against Secondary Region associated with the storage account if the request to the Primary Region was not successful.
4. Read transaction requests to RA-GRS Accounts that fail due to Geo-Replication Lag.

"**Geo Replication Lag**" for GRS and RA-GRS Accounts is the time it takes for data stored in the Primary Region of the storage account to replicate to the Secondary Region of the storage account. Because GRS and RA-GRS Accounts are replicated asynchronously to the Secondary Region, data written to the Primary Region of the storage account will not be immediately available in the Secondary Region. You can query the Geo Replication Lag for a storage account, but OneStream does not provide any guarantees as to the length of any Geo Replication Lag under this SLA.

"**Geographically Redundant Storage (GRS) Account**" is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You cannot directly read data from or write data to the Secondary Region associated with GRS Accounts.

"**Locally Redundant Storage (LRS) Account**" is a storage account for which data is replicated synchronously only within a Primary Region.

"**Primary Region**" is a geographical region in which data within a storage account is located, as selected by Customer when creating the storage account. You may execute write requests only against data stored within the Primary Region associated with storage accounts.

"**Read Access Geographically Redundant Storage (RA-GRS) Account**" is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You can directly read data from, but cannot write data to, the Secondary Region associated with RA-GRS Accounts.

"**Secondary Region**" is a geographical region in which data within a GRS or RA-GRS Account is replicated and stored, as assigned by OneStream Azure based on the Primary Region associated with the storage account. You cannot specify the Secondary Region associated with storage accounts.

"**Total Storage Transactions**" is the set of all storage transactions, other than Excluded Transactions, attempted within a one hour interval across all storage accounts in the Storage Service in a given subscription.

"**Zone Redundant Storage (ZRS) Account**" is a storage account for which data is replicated across multiple facilities. These facilities may be within the same geographical region or across two geographical regions.

"Monthly Uptime Percentage" is calculated using the following formula:

$$100\% - Average\ Error\ Rate$$

Service Credit – LRS, ZRS, GRS and RA-GRS (write requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Credit – RA-GRS (read requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

Service Credit – LRS, GRS and RA-GRS (write requests) Blob Storage Accounts (Cool Access Tier):

Monthly Uptime Percentage	Service Credit
< 99%	10%
< 98%	25%

Service Credit – RA-GRS (read requests) Blob Storage Accounts (Cool Access Tier):

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 98%	25%

Virtual Machines

Additional Definitions:
"Availability Set" refers to two or more Virtual Machines deployed across different Fault Domains to avoid a single point of failure.
"**Availability Zone**" is a fault-isolated area within an Azure region, providing redundant power, cooling, and networking.
"**Azure Dedicated Host**" provides physical servers that host one or more Azure virtual machines with the (default) setting of autoReplaceOnFailure required for any SLA.
"**Data Disk**" is a persistent virtual hard disk, attached to a Virtual Machine, used to store application data.
"**Dedicated Host Group**" is a collection of Azure Dedicated Hosts deployed within an Azure region across different Fault Domains to avoid a single point of failure.
"**Fault Domain**" is a collection of servers that share common resources such as power and network connectivity.
"**Operating System Disk**" is a persistent virtual hard disk, attached to a Virtual Machine, used to store the Virtual Machine's operating system.
"**Single Instance**" is defined as any single Microsoft Azure Virtual Machine that either is not deployed in an Availability Set or has only one instance deployed in an Availability Set.
"**Virtual Machine**" refers to persistent instance types that can be deployed individually, as part of an Availability Set or using a Dedicated Host Group. A virtual machine can be deployed in a multi-tenant environment in Azure or in an isolated, single-tenant environment using Azure Dedicated Hosts.
"**Virtual Machine Connectivity**" is bi-directional network traffic between the Virtual Machine and other IP addresses using TCP or UDP network protocols in which the Virtual Machine is configured for allowed traffic. The IP addresses can be IP addresses in the same Cloud Service as the Virtual Machine, IP addresses within the same virtual network as the Virtual Machine or public, routable IP addresses.
Monthly Uptime Calculation and Service Levels for Virtual Machines in Availability Zones
"**Maximum Available Minutes**" is the total accumulated minutes during a billing month that have two or more instances deployed across two or more Availability Zones in the same region. Maximum Available Minutes is measured from when at least two Virtual Machines across two Availability Zones in the same region have both been started resultant from action initiated by Customer to the time Customer has initiated an action that would result in stopping or deleting the Virtual Machines.

"**Downtime**" is the total accumulated minutes that are part of Maximum Available Minutes that have no Virtual Machine Connectivity in the region.
"**Monthly Uptime Percentage**" for Virtual Machines in Availability Zones is calculated as Maximum Available Minutes less Downtime divided by Maximum Available Minutes in a billing month for a given Microsoft Azure subscription. Monthly Uptime Percentage is represented by the following formula:

$$Monthly\ Uptime\ \% = \frac{(Maximum\ Available\ Minutes - Downtime)}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines, deployed across two or more Availability Zones in the same region:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.99%	10%
< 99%	25%
< 95%	100%

Monthly Uptime Calculation and Service Levels for Virtual Machines in an Availability Set, or in the same Dedicated Host Group

"**Maximum Available Minutes**" is the total accumulated minutes during a billing month for all Virtual Machines that have two or more instances deployed in the same Availability Set, or in the same Dedicated Host Group. Maximum Available Minutes is measured from when at least two Virtual Machines in the same Availability Set, or same Dedicated Host Group, have both been started resultant from action initiated by Customer to the time Customer has initiated an action that would result in stopping or deleting the Virtual Machines.

"**Downtime**" is the total accumulated minutes that are part of Maximum Available Minutes that have no Virtual Machine Connectivity.

"**Monthly Uptime Percentage**" for Virtual Machines is calculated as Maximum Available Minutes less Downtime divided by Maximum Available Minutes in a billing month for a given Microsoft Azure subscription. Monthly Uptime Percentage is represented by the following formula:

$$Monthly\ Uptime\ \% = \frac{(Maximum\ Available\ Minutes - Downtime)}{Maximum\ Available\ Minutes}\ x\ 100$$

The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines in an Availability Set, or same Dedicated Host Group:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.95%	10%
< 99%	25%
< 95%	100%

Monthly Uptime Calculation and Service Levels for Single-Instance Virtual Machines

"**Minutes in the Month**" is the total number of minutes in a given month.
"**Downtime**" is the total accumulated minutes that are part of Minutes in the Month that have no Virtual Machine Connectivity.
"**Monthly Uptime Percentage**" is calculated by the percentage of Minutes in the Month in which any Single Instance Virtual Machine using Premium SSD or Ultra Disk for all Operating System Disks and Data Disks had Downtime.

$$Monthly\ Uptime\ \% = \frac{(Minutes\ in\ the\ Month - Downtime)}{Minutes\ in\ the\ month}\ x\ 100$$

The following Service Levels and Service Credits are applicable to Customer's use of Single-Instance Virtual Machines:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.9%	10%
< 99%	25%
< 95%	100%

VPN Gateway

Additional Definitions:
"**Maximum Available Minutes**" is the total accumulated minutes during a billing month which a given VPN Gateway has been deployed in a OneStream Azure subscription.

"**Virtual Network**" refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within OneStream Azure.

"**VPN Gateway**" refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

"Downtime" is the total accumulated Maximum Available Minutes during which a VPN Gateway is unavailable. A minute is considered unavailable if all attempts to connect to the VPN Gateway within a 30 second window within the minute are unsuccessful.

"Monthly Uptime Percentage" for a given VPN Gateway is calculated as Maximum Available Minutes less Downtime dived by the Maximum Available Minutes in a billing month for the VPN Gateway. The Uptime Percentage is represented by the following formula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

The following Service Levels and Service Credits are applicable to Customer's use of each VPN Gateway:

Basic Gateway for VPN or ExpressRoute Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Standard, High Performance, VpnGw1, VpnGw2, Gateway for VPN / Standard, High Performance, Ultra Performance Gateway for ExpressRoute Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Azure Active Directory Basic

"Downtime" is any period of time when users are not able to log in to the service, log in to the Access Panel, access applications on the Access Panel and reset passwords; or any period of time IT administrators are not able to create, read, write and delete entries in the directory and/or provision/de-provision users to applications in the directory.

"Monthly Uptime Percentage" is calculated using the following formula:

$$\frac{User\ Minutes\ -\ Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Azure Active Directory Premium

"Downtime" is any period of time when users are not able to log in to the service, log in to the Access Panel, access applications on the Access Panel and reset passwords; or any period of time IT administrators are not able to create, read, write and delete entries in the directory and/or provision/de-provision users to applications in the directory.

"Monthly Uptime Percentage" is calculated using the following formula:

$$\frac{User\ Minutes\ -\ Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Key Vault

Additional Definitions:
"**Deployment Minutes**" is the total number of minutes that a given key vault has been deployed in Microsoft Azure during a billing month.

"**Excluded Transactions**" are transactions for creating, updating, or deleting key vaults, keys, or secrets.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Key Vaults deployed by you in a given Microsoft Azure subscription during a billing month.

"Downtime" is the total accumulated Deployment Minutes, across all key vaults deployed by Customer in a given Microsoft Azure subscription, during which the key vault is unavailable. A minute is considered unavailable for a given key vault if all continuous attempts to perform transactions, other than Excluded Transactions, on the key vault throughout the minute either return an Error Code or do not result in a Success Code within five seconds from Microsoft's receipt of the request.

"Monthly Uptime Percentage" is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\text{-}Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Attachment D

Acceptable Use Policy for Cloud Services

This Acceptable Use Policy identifies activities that you are prohibited from engaging in when using Cloud Services.

Please report violations of this Acceptable Use Policy to OneStream Customer Support, include the words "Acceptable Use Policy" in the subject.

When using Cloud Services, you may not:

1. Use the Cloud Services in a way that is against applicable law, including:
    a. Illegal activity such as child pornography; gambling; piracy; violating copyright, trademark or other intellectual property laws.
    b. Accessing or authorizing anyone to access the service from an embargoed country.
    c. Threatening, stalking, defaming, defrauding, degrading, victimizing or intimidating anyone for any reason.
    d. Invading anyone's privacy by attempting to harvest, collect, store, or publish private or personally identifiable information, such as passwords, account information, credit card numbers, addresses, or other contact information without their knowledge and consent.
2. Use the Cloud Services in a way that could harm them or impair anyone else's use of them, including:
    a. Any attempt to gain unauthorized access to a Cloud Service, acting to deny others access to a Cloud Service, or authorizing any third party to access or use the Cloud Services on your behalf (such as anyone without a license or revealing to anyone your username and password).
    b. Use the Cloud Services to try to gain unauthorized access to any other service, data, account or network by any means.
    c. Use any automated process or service to access or use the Cloud Services such as a bot, a spider or periodic caching of information stored by OneStream.
    d. Intending to harm or exploit minors in any way, or collecting personally identifiable information of, any minor.
3. Falsify any email header information or in any way misrepresent your identity, including misrepresenting the source of anything you post or upload or impersonating another individual or entity, such as with "spoofing".
4. Use the Cloud Services to transmit, distribute, or deliver any unsolicited bulk or unsolicited commercial e-mail (i.e., spam).
5. Remove, modify, or tamper with any regulatory or legal notice or link that is incorporated into the Cloud Services, including providing or creating links to external sites that violate this Acceptable Use Policy or other legal agreements OneStream provides, and any use of the Cloud Services to distribute any offering or link designed to violate these terms (e.g., enable sending of spam, enable denial of service attacks, etc.)

Additionally:

OneStream is not responsible for the content of any user-created posting, listing or message. The decision to view content or engage with others is yours. We advise you to use your judgment.

You are responsible for protecting your computer against interference, spyware or viruses that may be encountered for downloaded items from the service. We recommend you install a virus protection program on your computer and keep it up to date.