



Service Description Guide

7.3.3 Release

Copyright © 2022 OneStream Software LLC. All rights reserved.

Any warranty with respect to the software or its functionality will be expressly given in the Subscription License Agreement or Software License and Services Agreement between OneStream and the warrantee. This document does not itself constitute a representation or warranty with respect to the software or any related matter.

OneStream Software, OneStream, Extensible Dimensionality and the OneStream logo are trademarks of OneStream Software LLC in the United States and other countries. Microsoft, Microsoft Azure, Microsoft Office, Windows, Windows Server, Excel, .NET Framework, Internet Information Services, Windows Communication Foundation and SQL Server are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. DevExpress is a registered trademark of Developer Express, Inc. Cisco is a registered trademark of Cisco Systems, Inc. Intel is a trademark of Intel Corporation. AMD64 is a trademark of Advanced Micro Devices, Inc. Other names may be trademarks of their respective owners.

Table of Contents

| | |
|---|---|
| Service Architecture | 1 |
| Overview | 1 |
| Cloud Instance Resources | 1 |
| Security | 2 |
| Overview | 2 |
| Data Encryption | 2 |
| Server Hardening | 2 |
| Network Security and Isolation | 3 |
| Isolated Management | 3 |
| Secure Secrets Storage Service | 3 |
| Privileged Identity Management (PIM) | 4 |
| Administrative Access Audits | 4 |
| Intrusion Detection | 4 |
| Datacenter Physical Security Controls | 5 |
| Service Operations | 6 |
| Change Requests | 6 |
| Authorized Personnel | 6 |
| Maintenance & Change Management | 6 |
| Physical Controls of OneStream Corporate Facilities | 7 |

Table of Contents

| | |
|---|----|
| Incident Response | 7 |
| Backup, Recovery, and Archive | 8 |
| Business Continuity and Disaster Recovery | 9 |
| Corporate Business Continuity | 9 |
| Disaster Recovery | 9 |
| Datacenter High Availability and Redundancy | 9 |
| Region Pair Replication | 10 |
| Recovery Objectives | 10 |
| Testing and Compliance | 10 |
| Information Security Governance and Risk Management | 10 |
| Governance Risk and Compliance Program (GRC) | 10 |
| Security Frameworks | 11 |
| Security Policy and Procedures | 11 |
| Service Organizational Controls – SOC Reporting | 11 |
| Security Vulnerability Assessment | 11 |
| Instance Types | 12 |
| Production Instance | 12 |
| Non-Production Instances | 12 |
| Partial Sandbox | 12 |
| Full Sandbox | 12 |

Table of Contents

Service Limits 13

 Database 13

Datacenter Locations 14

 Primary Data Center Locations 14

 Alternate Data Center Locations 14

Definitions 16

Revision History 17

Service Architecture

Overview

OneStream's Service is designed as a highly available and scalable offering utilizing datacenters located in geographically redundant regions globally. To deliver the Service, OneStream utilizes select third-party cloud service providers as identified in Appendix 1 of our Data Processing Agreement. The OneStream Service is provided via a collection of virtual computing resources (individually, a "Cloud Instance", and collectively, the "Service Environment") that are physically and logically isolated from the OneStream corporate network.

Cloud Instance Resources

A Cloud Instance is comprised of many different resources, including, but not limited to, virtual machines, containers, databases, virtual networks, and other related technologies. Each customer is provided a Cloud Instance that is logically isolated from other customers through a combination of network policies, access controls and resource separation with layered security mechanisms to provide a robust, scalable, and secure solution.

A customer's Cloud Instance will be provided with resources out of a primary datacenter with failover to a secondary datacenter located in the same physical region. For example, customers with their primary datacenter located in the Eastern United States would failover to a secondary datacenter in the Western United States while customers with their primary datacenter located in Western Europe would failover to a secondary datacenter in Northern Europe. OneStream's Service is offered in multiple regions to support geo-political boundaries and adhere to data residency laws and requirements.

Security

Overview

OneStream utilizes a layered approach to security, in some cases referred to as a “defense in depth” strategy, to ensure that the Service and Customer Data remains secure. OneStream is committed to delivering a scalable, integrated, and highly performant solution with robust security measures that keep your data safe, and your business protected. OneStream understands that our customer’s data is one of its most valuable assets.

Data Encryption

OneStream’s Service utilizes industry standard encryption to protect all Customer Data while in-transit and at-rest. All data-in-transit between the Customer and the Service, using OneStream provided clients such as the OneStream Web Application for Windows and Excel add-in, is encrypted through the use of HTTPS/TLS 1.2 or greater. For data ingested from source systems, OneStream requires that the Customer provide an endpoint which supports industry-standard encryption protocols and cipher suites for connectivity.

Data-at-rest is stored using keys managed through the Secure Secrets Storage Service and is encrypted using an industry-standard cipher suite, such as AES-256. All data-at-rest is encrypted using a minimum key complexity of 256-bit for symmetric encryption keys.

Server Hardening

All compute images are built and configured with only the necessary services to operate the OneStream Service, and built to conform to the Center for Internet Security 1.1 Benchmark. All Cloud Instances are regularly patched and maintained in accordance with our policy noted under the section labeled “Maintenance & Change Management”.

Network Security and Isolation

OneStream follows industry-standard practices when configuring virtual networks and applying associated access controls. Our standard network access controls implement a policy of deny by default, allow by exception. Inbound network traffic is only permitted using specific network protocols and ports based on the minimum requirements to operate the Service. In addition, all applicable Cloud Instance resources, such as virtual machines, have firewalls enabled at the individual resource level.

By default, the OneStream Service is only accessible via a connection from the public internet. To the extent that a customer requests, OneStream will restrict access to the customer's Cloud Instances to only those connecting from a designated list of IP addresses. While OneStream will undertake reasonable security practices and precautions for connections originating from the customer's private network, customer is responsible for ensuring appropriate security policies are applied from within their internal network to such a connection.

Isolated Management

A customer's instance is accessible only to OneStream authorized personnel connecting through the OneStream corporate network. Administrative credentials, such as passwords, certificates, or cryptographic keys, for each customer's instance are stored in an isolated storage service dedicated to the specific customer. Access to this service is highly restricted and may only be accessed by authorized OneStream personnel when responding to a documented support request, during a maintenance event (both planned and unplanned), or other similar situations to ensure continuity of Service operations.

Secure Secrets Storage Service

Each customer is provisioned a dedicated instance of our secure secrets storage service which manages all administrative credentials, including passwords, certificates, API keys, and cryptographic keys. Each instance provides the following functionality and benefits:

- Advanced monitoring and logging
- Increased security with role-based access control policies and default encryption
- Automated administrative credential rotation and management

Only authorized OneStream personnel with documented approval via a support request, during a maintenance event (both planned and unplanned), or other similar situations to ensure continuity of Service operations may access this information. All administrative work performed in a customer's Cloud Instance is logged and can be traced to the specific authorization and team member(s) who performed the assigned work task. Prior to accessing the secrets storage service, authorized OneStream personnel must first authenticate against our corporate identity provider using their credentials and a multifactor authentication token.

Privileged Identity Management (PIM)

OneStream utilizes the principle of “least access” in designing its security architecture, to ensure that only authorized personnel have access to customer resources for approved requests. To facilitate this, OneStream utilizes PIM which temporarily allows access to a customer's Cloud Instance for approved tasks. Prior to accessing protected customer resources, authorized personnel must specify an approved support request number and time window for access. Use of PIM to access a customer's Cloud Instance is logged to provide a full audit history of any access to a specific customer's environment.

Administrative Access Audits

Privileged access to sensitive resources is restricted to defined users whose role requires the access and that are approved by the OneStream management. This access is reviewed on a periodic basis by the OneStream Compliance department. Audit logs are retained for a period of no less than twelve (12) months.

Intrusion Detection

To protect against online threats, OneStream provides anti-malware for Cloud Instance resources, such as virtual machines, containers, and select services. Our third-party cloud services providers also employ industry-standard intrusion detection, (distributed) denial-of-service (DDoS) attack prevention, regular penetration testing, data analytics, and machine learning tools to mitigate threats against the underlying infrastructure.

Datacenter Physical Security Controls

Datacenters managed by OneStream's third-party cloud service providers have extensive layers of protection including, but not limited to: access approval, at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. This layered approach reduces the risk of unauthorized users gaining physical access to data and the datacenter resources. In addition, our third-party cloud services providers are ISO 27001 compliant and regularly audited to ensure compliance with applicable standards, including SOC1 and SOC2 reporting standards.

Service Operations

Change Requests

Change requests (requests which impact confidentiality, integrity, availability, or cost) must be submitted in writing by a designated OneStream administrator through email or our support portal to manage the workflow of the requested change. 3rd parties, such as approved implementation partners and consultants, may submit requests on behalf of customers but require documented approval from a of a customer's designated administrators prior to being actioned.

Email: support@onestreamsoftware.com

Portal: <https://support.onestreamsoftware.com>

Authorized Personnel

OneStream performs extensive background checks prior to team consideration as well as during every year of employment. In addition, OneStream's third-party cloud services providers retain a full audit trail of any changes to a customer's Cloud Instance. All activities conducted within our Service Environment are auditable and track personnel actioning the change as well as the relevant support request(s). Audit logs and other related change management data is retained for a minimum period of twelve (12) months.

Maintenance & Change Management

Scheduled maintenance to a customer's Cloud Instance is coordinated by the OneStream Service Cloud Operations management team. A standard maintenance window is in place on the weekend following the industry's "Patch Tuesday" update releases and are mandatory events. OneStream conducts regression testing of all underlying patches in a OneStream test environment prior to introducing to the Service Environment. In the event a customer has scheduled activity, an alternate time within the next seven (7) calendar days following "Patch Tuesday" may be requested so long as the request is received at least three (3) calendar days prior to the maintenance window. If a critical update is necessary for security purposes, OneStream will notify the customers and take action to perform the updates as soon as possible irrespective of the standard maintenance window.

OneStream will coordinate separate scheduled maintenance windows with customers to perform upgrades to the software related to the functioning of the Service and other instance changes. OneStream will notify customer contacts at least three (3) calendar days before any maintenance window and again at least 24 hours prior.

Physical Controls of OneStream Corporate Facilities

OneStream deploys physical access devices (e.g. key fobs) to control entry to those offices with direct connectivity to OneStream's processing environment. Satellite offices are logically controlled by maintaining an internet connection and enforcing VPN access into the environment.

The electronic access logs are reviewed weekly, noting any anomalies. Special attention is paid to any unusual activity during the evenings and weekends, as well as monitoring the cleaning company's activities. If an issue is found, an incident report is created. OneStream employs security cameras and motion detectors to monitor activity. CCTV systems record continuously, and the recordings are retained for at least 60 days. Additionally, OneStream's offices have alarm systems that monitored and responded to by the local authorities.

All visitors must electronically sign-in, and sign-out of the visitor log located at the receptionist desk and be accompanied by the employee(s) that they are visiting for the duration of their stay.

Incident Response

OneStream takes any security incident very seriously. We practice prevention and preparedness through education. In the event of an incident, OneStream follows a process of Identification, Triage, Containment, Eradication, and Recovery. Following an incident, a full post-mortem review is conducted to close the loop on future education.

OneStream will notify customer without undue delay, which in no event shall be greater than 48 hours after the determination that a Security Incident has occurred or is likely to have occurred and provide to Customer, upon request, a reasonably detailed incident report. OneStream is committed to cooperate in good faith with Customer to remedy or mitigate the impact of any Security Incident.

Backup, Recovery, and Archive

OneStream maintains a robust automatic backup system, ensuring continuity of the Service Environment in the event of unexpected failure or disaster. Cloud Instance resources unique to a customer are automatically replicated to a secondary datacenter within the same region continuously. In addition, all 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. Additional periods of LTR for weekly “snapshots” may be procured for an additional fee, up to a maximum retention period of the trailing five-hundred and twenty (520) weeks. Both PITR and LTR enable a customer to roll back critical data elements (such as the database state) of a customer’s Cloud Instance to a specified point in time.

Customers retain ownership of, and are expected to maintain, all data in their Cloud Instance. OneStream requires that the Customer ensure that all data uploaded to the Cloud Instance, including but not limited to personally identifiable information, is in compliance with applicable legislation and regulations. For the avoidance of doubt, OneStream does not purge or obfuscate data on customers behalf.

Business Continuity and Disaster Recovery

OneStream's Corporate Business Continuity Plan (or "BCP") is maintained, tested, and reviewed annually or as needed based on business changes to support OneStream's corporate environment. An event in OneStream's corporate environment could occur with little or no impact on the ability to provide full-service availability to our customers.

OneStream's Service Disaster Recovery (or "DR") plan is specific to the Service Environment, including customer Cloud Instances, and is maintained, tested, and reviewed annually or as needed based on business changes to support OneStream's Service for our customers.

Corporate Business Continuity

OneStream's Business Continuity process covers its functional offices and is a distinct operating procedure from its management of the Service. The BCP has been developed as a component of our Governance Risk and Compliance (or "GRC") Program including Business Impact Assessments (or "BIA") to understand the impact of the loss of any given systems or locations.

Disaster Recovery

Datacenter High Availability and Redundancy

OneStream's Service is provided to each customer out of a primary datacenter region, with automatic replication and backup to a secondary datacenter region as a failover. The primary and secondary datacenter regions will be automatically selected from OneStream's default regions as noted in "Datacenter Locations", unless a customer has specific data residency requirements and specifically requests an alternate datacenter region from our list of "Alternate Datacenter Locations". These datacenters have several layers of high availability built into them. While the probability of a failure is low, redundancies and backups are employed in strategic ways to ensure that, in the event of a failure, services are restored at a secondary data center in a timely manner. In the unlikely event that an entire datacenter is rendered off-line unexpectedly, Cloud Instances in the impacted datacenter will failover to the secondary datacenter region. Note that this overview and the following information regarding DR is applicable only to Cloud Instances designated as "Production".

Region Pair Replication

The OneStream Service includes the replication of customer data to a secondary datacenter region. Each datacenter region is paired with another datacenter region within the same geography (such as the United States, Europe, or Asia). This approach allows for the replication of resources across a geography reducing the likelihood of natural disasters, civil unrest, power outages, or physical network outages. Additional advantages of region pairs include:

- In the event of a wider data center outage, one region is prioritized out of every pair to help reduce the time to restore for applications
- Planned data center updates are rolled out to paired regions one at a time to minimize downtime and risk of application outage

Recovery Objectives

In the event of a catastrophic data center failure, OneStream has defined a Recovery Point Objective of one (1) hour and a Recovery Time Objective of twenty-four (24) hours.

Testing and Compliance

OneStream formally tests our disaster recovery process as either a live or tabletop exercise annually as a component of our Governance Risk and Compliance Program. Additional non-formal testing also occurs as business conditions dictate.

Information Security Governance and Risk Management

Governance Risk and Compliance Program (GRC)

OneStream maintains a comprehensive risk management program, inclusive of the following governance, risk, and compliance elements:

- Third- and Fourth-Party Vendor Risk Management
- Risk and Controls Framework Management
- Business and Application Risk Assessments

- Business Continuity, Disaster Recovery Program Management
- Audit, Compliance Program Management
- Capability Maturity Model Assessments and Continuous Improvements

Prospects and customers may request the "GRC Program - Customer Due Diligence Package" for an overview of our GRC Program Framework inclusive of cadence and artifact inventory.

Security Frameworks

The OneStream Service is aligned with NIST 800-53 and ISO 27001 operational and security controls. These frameworks include a comprehensive set of security controls that are used as a baseline for the operational and security controls utilized to manage and secure the OneStream Service.

Security Policy and Procedures

OneStream's Service Policies and Plans are controlled subject matter and are not distributed. Prospects and customers may request the "GRC Program - Customer Due Diligence Package" for an overview of our policy and controls framework.

Service Organizational Controls – SOC Reporting

As a component of the OneStream GRC Program, OneStream submits to twice annual SOC 1 and SOC 2 audit as well as Bridge Letters to cover any additional customer audit cadence. Prospects may request SOC reports for their review as a component of their due diligence process. Existing customers may download SOC reports from OneStream MarketPlace at any time as needed to support their internal audit program.

Security Vulnerability Assessment

OneStream conducts a security assessment of our Service at least annually. This testing is conducted against a standard OneStream Cloud Instance by a third-party service provider. OneStream Software engages with an outside provider to perform a security assessment to enumerate possible attack vectors, evaluate existing security controls, and provide recommendations for improvement. Providers assess the security posture and perform an authenticated black-box review of OneStream's Service. This "web application" penetration test focuses on the Open Web Application Security Project's (OWASP's) Top 10 Flaws of Insecure Software, a broad consensus of the most critical web application security flaws aimed to help fight root cause, as well as the SANS Top 25 vulnerability list as current to the project engagement.

Instance Types

Production Instance

By default, OneStream's Service only includes a production instance. The production instance is configured based on the customer's user count to provide optimal performance for the estimated size of the unified data model.

Non-Production Instances

In addition to the production instance, customers may add additional non-production instances for development and testing purposes. All non-production instances are isolated from the customer's production cloud instance resources to ensure that no performance degradation occurs as a result of development and testing activities.

Partial Sandbox

A partial sandbox is intended to be used as a testing environment. The partial sandbox allows customers to load their metadata, business rules, and other application configuration elements, along with source system data, to test their unified data model, workflows, and related items. Note that the partial sandbox prioritizes a production like experience for the data model, with limited user concurrency. You can use a partial sandbox for quality assurance tasks such as data model verification, user acceptance testing, integration testing, and similar activities.

Full Sandbox

A full sandbox is intended to be used as a testing environment. In addition to the feature functionality provided by a partial sandbox, a full sandbox allows for performance / load testing on a like-for-like basis with the customer's production Cloud Instance.

Service Limits

Database

Storage – Database storage space included with the Service is the greater of 512 gigabytes or 4 gigabytes per named user, up to a Service maximum limit of 4 terabytes. Additional storage capacity can be provisioned, up to the Service maximum limit.

Datacenter Locations

The OneStream Service and associated Cloud Instance resources are operated out of several global datacenters. By default, a customer's region will be automatically selected on their behalf based on the Base Location as denoted on the Order Schedule. Please note that only primary datacenter locations will be included in the default selection criteria pool, as alternate datacenter locations are only available by customer request. A customer with a documented data residency requirement may request a different region by specific request on an Order Schedule. Alternate datacenter locations may have specific considerations – please consult your account manager for additional information.

Primary Data Center Locations

| Base Location | Primary Region | Secondary Region |
|-----------------------------|-----------------------|-----------------------|
| Americas | Eastern United States | Western United States |
| Europe, Middle East, Africa | Western Europe | Northern Europe |
| Asia-Pacific | Southeast Asia | East Asia |

Alternate Data Center Locations

| Base Location | Primary Region | Secondary Region |
|------------------------------|--------------------------|------------------------|
| Canada | Central Canada | Eastern Canada |
| United Kingdom | Southern United Kingdom | Western United Kingdom |
| Asia-Pacific (Secondary) | Australia East | Australia Southeast |
| Middle East | UAE North | UAE Central |
| U.S. Government ¹ | U.S. Government Virginia | U.S. Government Texas |

Datacenter Locations

¹ U.S. Government region only available to qualified entities. Contact your account manager for the qualification requirements associated with entities eligible for the denoted data center regions.

Definitions

“Recovery Point Objective” or “RPO” means the maximum amount of data loss measured in time between data restoration and an unexpected failure or disaster.

“Recovery Time Objective” or “RTO” means the maximum length of time allowed between an unexpected failure or disaster and the resumption of normal operations.

Revision History

| Revision Number | Date | Description |
|-----------------|-----------------|--------------------------------|
| 7.2 | September, 2022 | Updated copyright notice. |
| 7.2.1 | October, 2022 | Updated for release number. |
| 7.2.1 | November, 2022 | Updated for storage history. |
| 7.2.2 | November, 2022 | Updated Data Center locations. |