Service Description

OpenText Cloud to Cloud Backup Service

October 2024

opentext™

Contents

This Service Description describes the components and services included in OpenText Cloud to Cloud Backup (which also may be referred to as "SaaS") and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service ("SaaS Terms") found at https://www.microfocus.com/en-us/legal/software-licensing. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

High Level Summary

OpenText Cloud to Cloud Backup is a fully automated daily backup service for SaaS services keeping data in cloud storage. The service provides ability to quickly restore/export backed up data in case of data loss or corruption.

SaaS Delivery Components

SaaS Delivery Components	
Automated scheduled daily backups of MS365, Google Workspace, Box, Dropbox and Salesforce data to cloud storage	✓
High-frequency (3x daily) automated scheduled backups of data to cloud storage	O
Restore of backed up data back to the online service	✓
Export of backed up data for download/to cloud storage	✓
✓ **= Included**	
O = Optional for a fee	

SaaS Operational Services

Operational Services	
Initial onboarding support	✓
Operational training sessions	✓
Entire History Backup Data Export	**O**
✓ **= Included**	
O = Optional for a fee	

Architecture Components

OpenText Cloud to Cloud Backup is a cloud-based subscription service built on the AWS platform. No software installation is required, as the SaaS is browser-based. Customers can get access to the service at www.cloudally.com or via the AppRiver Portal if the service is being sold from the Secure Cloud platform.

OpenText Cloud to Cloud Backup includes web interface with access to backups management, recovery operations, billing/subscription and user management.

Backed up data is stored in vendor's AWS S3 by default; customers can connect to their own cloud storage repositories (AWS, GCP, Azure).

Application Administration

Customers have the following administration functions available in UI:

Backup Management
Customers can create, activate, pause and delete their backups.

Backup data and admins are managed by the Customer and can be deleted using features of the Cloud-to-Cloud Backup service. Application event logs, which include access attempts, are retained for up to twenty-four (24) months. Customer backup data is deleted from the system after a grace period of 5 days. After that the customers data is flushed from the environment and cannot be restored even by the SaaS.

Recovery Operations
Customers can restore backed up data back to the original service or export it for local download/cloud storage.

User Management
Customers can add and delete additional users with fine-grained access control to operations.

Security Management
Customers can set two-factor authentication, establish IP restrictions and optionally configure OKTA SAML integration.

Security and System Audit logs
Customers can see actions initiated by the system and other service users (within the same account).

Notifications/Alerts
Customers can configure multiple recipients for different types of system notifications and alerts.

Service Support

Customer can contact Cloud to Cloud Backup support 24x7x365 by phone, e-mail, chat or web ticket (embedded within the application).

Support Features:

Activity	
Customer Success Manager	✓
Onboarding Assistance	✓
24x7 Support via Chat, Phone, Email or Ticket	✓
Release Upgrades	✓
Training sessions on request	✓

99.9 % Availability SLA	✓
✓ **= Included**	
O = Optional for a fee	

Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability to SaaS and SaaS Data for Customer following an outage or similar loss of service for SaaS. OpenText Cloud to Cloud Backup periodically performs backup of the backed-up data from AWS S3 to AWS Glacier.

SaaS Data

The following types of SaaS Data reside in the SaaS environment:

- Application data backed up from the customer's SaaS service. This can include mail, calendar, contacts, tasks, documents, etc.
- Customer Billing Information. Note: Credit Card information, if provided, is handled by a PCI-compliant payment processor - the SaaS does not process or store any credit card information.

Cloud to Cloud Backup does not have access to or knowledge of the SaaS Data in any customer's account .

Micro Focus performs an internal backup of SaaS Data every quarter. Micro Focus retains each backup for the following three (3) months until the next quarterly backup.

Micro Focus's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of this data, despite any assistance or efforts provided by Micro Focus to recover or restore Customer's data. Customer may request via a service request for Micro Focus to attempt to restore such data from Micro Focus's most current backup. Micro Focus will be unable to restore any data not properly entered by Customer or lost or corrupted at the time of backup or if Customer´s request comes after the 7 days data retention time of such backup.

Disaster Recovery for SaaS

Business Continuity Plan
Micro Focus continuously evaluates different risks that might affect the integrity and availability of SaaS. As part of this continuous evaluation, Micro Focus develops policies, standards and processes that are implemented to reduce the probability of a continuous service disruption. Micro Focus documents its processes in a business continuity plan ("BCP") which includes a disaster recovery plan ("DRP"). Micro Focus utilizes the BCP to provide core SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that implements and tests SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

AWS Replication and Failover
As a SaaS service, the OpenText Cloud to Cloud backup service is implemented using a cloud-based technology service stack in a redundant mode over multiple availability zones. The failure of one zone will not impact the service availability as the system will automatically failover from the other zones.

SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability, and integrity of SaaS Data.

Technical and Organizational Measures

Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. No security measures are or can be completely effective against all security threats, present and future, known and unknown. The measures set forth in this section may be modified by Micro Focus but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

Physical Access Controls

The Cloud-to-Cloud Backup platform is built and runs on AWS infrastructure located in AWS data centers. As such, Micro Focus employees and subcontractors have no physical access capabilities to the data centers.

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make SaaS Data accessible only by authorized Micro Focus personnel who have a legitimate business need for such access:

- Secure user identification and authentication protocols
- Authentication of Micro Focus personnel in compliance with Micro Focus standards and in accordance with ISO27001 requirements for segregation of duties
- SaaS Data is accessible only by authorized Micro Focus personnel who have a legitimate business need for such access, with user authentication, sign-on and access controls
- Employment termination or role change is conducted in a controlled and secured manner
- Administrator accounts should only be used for the purpose of performing administrative activities
- Each account with administrative privileges must be traceable to a uniquely identifiable individual
- All access to computers and servers must be authenticated and within the scope of an employee's job function
- Collection of information that can link users to actions in the SaaS environment
- Collection and maintenance of log audits for the application, OS, DB, network and security devices according to the baseline requirements identified
- Restriction of access to log information based on user roles and the "need-to-know"
- Prohibition of shared accounts

Availability Controls

Micro Focus´s business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus's continuity plans cover operational shared infrastructure such as remote access, active directory, DNS services, and mail services. Monitoring systems are designed to generate automatic alerts that notify Micro Focus of events such as a server crash or disconnected network.

Data Segregation

SaaS environments are segregated logically by access control mechanisms. Internet-facing devices are configured with a set of access control lists (ACLs), which are designed to prevent unauthorized access to internal networks. Micro Focus uses security solutions on the perimeter level such as: firewalls, IPS/IDS, proxies and content-based inspection in order to detect hostile activity in addition to monitoring the environment's health and availability.

Data Encryption

Micro Focus uses industry standard techniques to encrypt SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted.

Audit

Micro Focus appoints an independent third party to conduct an annual ISO-27001 audit of the applicable policies used by Micro Focus to provide SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer's execution of Micro Focus's standard confidentiality agreement, Micro Focus agrees to respond to a reasonable industry standard information security questionnaire concerning its information and physical security program specific to SaaS no more than once per year. Such information security questionnaire will be considered Micro Focus confidential information.

Micro Focus Security Policies

Micro Focus regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge, or new threats are identified.

Customer initiated security testing is not permitted, which includes application penetration testing, vulnerability scanning, application code testing or any other attempt to breach the security or authentication measures of the SaaS.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure or alteration of SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to reasonably mitigate the impact of such Security Incident. Should Customer believe that there has been unauthorized use of Customer's account, credentials, or passwords, Customer must immediately notify Micro Focus Security Operations Center via SED@opentext.com.

Micro Focus Employees and Subcontractors

Micro Focus requires that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of customer data. Micro Focus requires that any affiliate or third-party subcontractor involved in processing SaaS Data enters into a written agreement with Micro Focus, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

Data Subject Requests

Micro Focus will refer to Customer any queries from data subjects in connection with SaaS Data.

Scheduled Version Updates

SaaS Upgrades may or may not include new features or enhancements. Micro Focus determines whether and when to develop, release and apply any SaaS Upgrade. Customer is entitled to SaaS Upgrades during the applicable SaaS Order Term unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's SaaS. Unless Micro Focus anticipates a service interruption due to a SaaS Upgrade, Micro Focus may implement a SaaS Upgrade at any time without notice to Customer. Micro Focus aims to use the Scheduled Maintenance windows defined herein to apply SaaS Upgrades. Customer may be required to cooperate in achieving a SaaS Upgrade that Micro Focus determines in its discretion is critical for the availability, performance or security of SaaS.

Micro Focus will use the Scheduled Maintenance windows defined herein to apply the most recent service packs, hot fixes, and minor version updates to SaaS. To enable Customer to plan for scheduled major version updates by Micro Focus, Micro Focus will schedule major version updates at least two (2) weeks in advance. However, if Micro Focus does not receive Customer's cooperation in achieving the SaaS Upgrade in a timely manner, Micro Focus reserves the right to charge Customer additional fees that are related to Customer's SaaS instance remaining on a version that is beyond the "end of support" period. Customer also understands that this status may prevent the most recent patches from being applied to its SaaS solution, and that the availability, performance, and security of SaaS as described in this Service Description may be impacted as a result.

Support is available at https://support.cloudally.com/hc/en-us in the following tiers:

Support Tiers	Overview	Examples
First Line Support	Basic help desk resolution and front-line service desk delivery	• First call resolution • Triage of technical issues • Resolution of known issues • Identifying severity and escalating
Second Line Support	In-depth technical support with technicians who know the product and systems	• Symptom Identification • Provide Break-fix/Corrective support • Troubleshooting the product • System/Network Tuning
Third Line Support	Expert technical knowledge to support product and service problems	• In-depth technical resolution • Defect Detection and Analysis • Software Development • Testing and Releasing Patches

Service Request Classification and Support Time

Support may be provided by telephone, e-mail, or chat categorized according to the following:

Service Request Classification	SR Definition	Target Response Time*
Severity Level 1	Production system is down, or the or Software is functionally inoperable	2 hours (must be logged by phone)
Severity Level 2	A performance issue that has a significant impact on normal operations of the Services or Software or materially restricts Your use of the Services or Software (system is operational, but performance may be impacted)	4 hours
Severity Level 3 ***As a rule, Service Requests reported via email and/or for non-production systems are classified at this level.***	A performance issue that has a minor impact on normal operations of the Services or Software, or a minor defect in the functionality of the Services or Software that does not materially restrict Your use of the Services or Software.	24 hours
Severity Level 4	A performance issue that is a non-critical question or issue that does not affect the performance or functionality of the Services or Software.	48 hours

**Response Times are targets and not guaranteed. For the avoidance of doubt, the times listed are estimated times to respond and not times to resolve a SR.*

Responsibilities and Exclusions

- Micro Focus' ability to deliver Technical Support depends upon your full and timely cooperation as well as the accuracy and completeness of any information you provide.
- Your request will not be eligible for Technical Support if the situation was caused by:
  - Changes to Your operating system or environment that adversely affect the Services or Software
  - Your use of the Services or Software for any purpose other than as explicitly specified by Micro Focus
  - Your use of the Services or Software with equipment or software not recommended or supported by Micro Focus
  - Any alterations of, or additions to, the Services or Software made by anyone other than Micro Focus
  - Your violation of the underlying agreement for the applicable Services or Software

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to SaaS, and Customer shall promptly return to Micro Focus (or at Micro Focus's request destroy) any Micro Focus materials..

Micro Focus will make available to Customer any SaaS Data in Micro Focus' possession in the format generally provided by Micro Focus. The target timeframe is set forth below in Termination Data Retrieval Period SLO. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted in the ordinary course.

Service Level Objectives

Micro Focus provides clear, detailed, and specific Service Level Objectives (SLOs) for SaaS. These SLOs are targets used by Micro Focus to deliver the service and are provided as guidelines. They in no way create a legal requirement or obligation for Micro Focus to meet these objectives.

Solution Provisioning Time SLO
Solution Provisioning is defined as SaaS being available for access over the internet. Micro Focus targets to make SaaS available within one (1) business day of Customer's Order for SaaS being booked within the Micro Focus order management system.

Customer is responsible for installing, configuring, deploying, updating and paying any additional fees (if required) for any additional on-premise components for its applications. Any on-premise components of the solution are not in scope of the Solution Provisioning Time SLO.

Additionally, the import of Customer data into the application is not in scope of the Solution Provisioning Time SLO.

Solution Availability SLO
Solution Availability is defined as the SaaS production application being available for access and use by Customer over the Internet. Micro Focus will provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9 % ("Solution Uptime").

Measurement Method
Solution Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing.

On a quarterly basis, Solution Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9% availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

Boundaries and Exclusions
Solution Uptime shall not apply to or include any time during which SaaS is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events
- Actions or omissions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance
- Scheduled SaaS upgrades

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9% ("Online Support Uptime").

Measurement Method
Online Support Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing. On a quarterly basis, Online Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

Boundaries and Exclusions
Online Support Uptime shall not apply to or include any time during which the SaaS support portal is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events
- Actions or inactions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance
- Scheduled SaaS upgrades

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the support described herein. It is defined as the acknowledgment of the receipt of Customer's request and the assignment of a case number for tracking purposes. Initial SaaS Response will come as an email to the requester and include the case number and links to track it using Micro Focus online customer portal. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the Initial SaaS Response no more than one hour after the successful submission of Customer's request.

SaaS Support SLOs

There are two types of SaaS Support SLOs: Service Request and Support Request SLOs.

- The Service Request SLO applies to the majority of routine system requests. This includes functional system requests (product add/move/change), informational, and administrative requests.
- The Support Request SLO applies to issues that are not part of the standard operation of the service and which causes, or may cause, an interruption to or a reduction in the quality of that service.

The Response and Resolution Targets are provided as guidelines and represent typical request processing by Micro Focus SaaS support teams. They in no way create a legal requirement or obligation for Micro Focus to respond in the stated time.

Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which Customer can retrieve a copy of their SaaS Data from Micro Focus. Micro Focus targets to make available such data for download in the format generally provided by Micro Focus for 30 days following the termination of the SaaS Order Term.

Service Level Commitments

Micro Focus provides the following Service Level Commitments for the purpose of further measuring the quality of service that Micro Focus is delivering to the Customer.

SaaS Availability SLA
SaaS availability is the SaaS production application being available for access and use by Customer over the Internet. Micro Focus will provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9 % ("Target Service Availability" or "TSA").

Measurement Method
TSA shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing. On a quarterly basis, the TSA will be measured using the measurable hours in the quarter (total time minus Downtime Exclusions) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

Downtime Exclusions

The TSA shall not apply to or include any time during which SaaS is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Third party service (including, without limitation, Amazon Web Services) outages or other causes beyond Micro Focus' reasonable control
- Configuration, maintenance or correction of third-party software, hardware or communications facilities
- Scheduled maintenance, or emergency maintenance
- Your use of an unsupported version of the Services
- Force Majeure
- Your use of the Services other than in accordance with the Cloud Terms and Conditions
- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks Outages caused by disruptions attributable to force majeure events (i.e., unforeseeable events outside of Micro Focus' reasonable control and unavoidable even by the exercise of reasonable care
- Customer-caused outages or disruptions
- Outages not caused by Micro Focus or not within the control of Micro Focus (i.e. unavailability due to problems with the Internet), unless caused by Micro Focus' service providers
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance activities
- Scheduled SaaS upgrades
- Customer exceeding the service restrictions, limitations or parameters listed in this Service Description and/or the Order
- Unavailability due to customizations made to the Micro Focus SaaS which are not validated, reviewed and approved in writing by both parties
- System downtime requested by Customer
- Suspensions of the Micro Focus SaaS by Micro Focus as a result of Customer's breach of the SaaS Terms

Reporting

The Customer gets backup summary reports on daily basis, unless changed or disabled in SaaS settings. The Customer also gets reports on recovery operations and notifications on backup issues.

Remedies for Breach of Service Levels

i. **Sole remedy.** Customer's rights described in this section state Customer's sole and exclusive remedy for any failure by Micro Focus to meet the agreed service levels.
ii. **Escalation.** Quarterly ASA below 98% shall be escalated by both parties to the Vice President (or equivalent).
iii. **Credit.** Subject to the terms herein, Micro Focus will issue a credit reflecting the difference between the measured ASA for a quarter is less than the TSA. ("**Remedy Percent**"). For clarity, several example calculations using this formula are illustrated in the table below:

Target Service Availability (TSA)	Actual Service Availability	Result	Remedy Percent
99.9 %	99.9%		Not Applicable
99.9%	94.9%	5% missed	5%
99.9%	90.9%	9% missed	9%

Customer must request credits in writing to Micro Focus within ninety (90) days of receipt of the ASA Report resulting in such credit and identify the support requests relating to the period where the SaaS production application was not available for access and use by the Customer over the internet. Micro Focus shall apply the requested credits on a quarterly basis.

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to SaaS. Micro Focus's ability to fulfill its responsibilities relative to SaaS is dependent upon Customer fulfilling the responsibilities described below and elsewhere herein:

Customer Roles and Responsibilities

Customer Role	Responsibilities
Primary Administrator	• Owns the business relationship between the customer and Micro Focus • Manages subscription and payments • Recovers organizational data upon a need or request • Serves as the first point of contact for SaaS end users for problem isolation • Performs SaaS administration • Coordinates end-user testing as required • Leads ongoing solution validation • Trains the end-user community • Coordinates infrastructure-related activities at the customer site
Secondary Administrator (Optional)	• Manages subscription and payments • Recovers organizational data upon a need or request • Serves as the first point of contact for SaaS end users for problem isolation • Performs SaaS administration • Coordinates end-user testing as required

	• Leads ongoing solution validation • Trains the end-user community • Coordinates infrastructure-related activities at the customer site
End User (MS)	• Recovers own Microsoft Exchange data

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Customer Service Centre (CSC)	• Primary point of contact for service requests. The customer can contact the Service Operations Center for all services such as support and maintenance, or issues regarding availability of SaaS • Provides 24x7 application support
Operations Staff (Ops)	• Monitors the Micro Focus systems and SaaS for availability • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices • Provides 24x7 SaaS infrastructure support

Assumptions and Dependencies

This Service Description is based upon the following assumptions and dependencies between the Customer and Micro Focus:

- Customer must have internet connectivity to access SaaS
- SaaS will be delivered remotely in English only
- The service commencement date is the date on which Customer´s Order is booked within the Micro Focus order management system
- Customer must ensure that its administrators maintain accurate contact information with Micro Focus
- Customer has determined, selected, and will use options in the Customer environment that are appropriate to meet its requirements, including information security controls, connectivity options, and business continuity, backup and archival options
- Customer will establish and follow secure practices for individual account-based access for accountability and traceability.

Furthermore, SaaS is provided based on the assumption that Customer will implement and maintain the following controls in its use of SaaS:

- Configuring Customer's browser and other clients to interact with SaaS
- Configuring Customer's network devices to access SaaS
- Appointing authorized users

- Configuring its SaaS account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications, and terminations

Good Faith Cooperation

Customer acknowledges that Micro Focus's ability to provide SaaS and related services depends upon Customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Micro Focus. Where this Service Description requires agreement, approval, acceptance, consent or similar action by either party, such action will not be unreasonably delayed or withheld. Customer agrees that to the extent its failure to meet its responsibilities results in a failure or delay by Micro Focus in performing its obligations under this Service Description, Micro Focus will not be liable for such failure or delay.