
Service Description

Service Description

OpenText™ Core Endpoint Management

June 2026

opentext™

Copyright 2026 OpenText

Contents

Contents 2

Standard Service Features..... 3

Data Backup and Retention 7

SaaS Security 8

Audit 9

OpenText Security Policies..... 9

Security Incident Response 10

OpenText Employees and Subcontractors..... 10

Data Subject Requests 10

Scheduled Maintenance..... 10

Service Decommissioning..... 11

Service Level Objectives..... 11

Standard Service Requirements..... 14

This Service Description describes the components and services included in OpenText Core Endpoint Management (which also may be referred to as “SaaS”) and, unless otherwise agreed to in writing, is subject to the OpenText Customer Terms for Software-as-a-Service (“SaaS Terms”) found at <https://www.opentext.com/about/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 Core Endpoint Management is an OpenText cloud offering designed to offer OpenText customers a way to manage endpoint devices in their environment. It facilitates IT administrators of OpenText customers to easily distribute software applications, configurations, policies etc. to endpoint devices. It also supports deployment of operating system patches and applications patches on endpoint devices. All this can be done from an OpenText hosted centralized management console. OpenText oversees the deployment, infrastructure, operation, availability, security and data protection and support of the service. Some components like Endpoint Management agent need to be deployed by customers on their endpoint devices.

SaaS Delivery Components

SaaS Delivery Components

One OpenText Core Endpoint Management subscription	✓
Management Console for OpenText Core Endpoint Management Service	✓
Account management through OpenText Cloud Platform Admin Center	✓
✓ = Included	
O = Optional for a fee	

SaaS Operational Services

SaaS Operational Services

Onboarding	✓
Product Support	✓
✓ = Included	
O = Optional for a fee	

Architecture Components

OpenText Core Endpoint Management is used to manage endpoints, deploy applications and collect hardware and software information from these endpoints. It also supports deployment of operating systems and software application patches on these devices. OpenText Core Endpoint Management consists of these parts:

- Client Management Service: This is a cloud-based service running in secure OpenText Cloud Platform and is used to send commands, configurations etc. to endpoint devices
- Admin Management Service: This is cloud-based platform running in secure OpenText cloud platform providing capabilities to process data and orchestration capabilities

- **Patch Management Service:** This is cloud-based service running in OpenText Cloud Platform and is used to distribute and deploy operating systems and software application patches on endpoint devices
- **Endpoint Management Console:** This is cloud-based management console (part of Endpoint Management Service), accessible via a web UI through which Customer can manage different endpoints in their on-premise environment. This also has interactive dashboards for management and reporting.
- **Push Notification Service:** This is cloud-based service used to send notification to endpoint devices, so that they may contact back through Client Management Service
- **Endpoint Agent:** This is an endpoint agent available for download from Endpoint Management Console. This needs to be installed and configured on individual endpoints present on customer premises for endpoints to be managed from Endpoint Management Console.
- **Cloud Storage:** This is cloud-based storage from which an endpoint agent would download the content as instructed through client management service

OpenText deploys OpenText Core Endpoint Management Service using a shared infrastructure platform. The shared platform is monitored for 24x7 availability, and Open Text provides related 24x7 infrastructure support, including application version upgrades. Customer access to OpenText Core Endpoint Management is through the Internet over HTTPS.

OpenText does not install, deploy, or manage on-premises components that may be required to use OpenText Core Endpoint Management. Customer is responsible for installing, configuring, deploying, updating, and paying any additional fees (if required) for any additional on-premises components for its applications.

Core Endpoint Management Express

OpenText Core Endpoint Management is currently available as Core Endpoint Management Express. It is a suite of features of OpenText Core Endpoint Management comprising following set of offerings and capabilities

Offering	Capabilities Included
Core Endpoint Management Base (Express)	• Base endpoint management service providing enrolment and subsequent management of devices including collection of software inventory data
Core Endpoint Application Delivery (Express)	• Distribution and deployment of software applications on endpoint devices
Core Endpoint Patch Management (Express)	• Distribution and deployment of operating system patches and software application patches on endpoint devices

Above set of offerings are only available as part of Core Endpoint Management Express and can't be purchased separately.

Definitions

Term	Definition
Service	Means the Core Endpoint Management Service made available by OpenText
Device	Means a physical or virtual endpoint, including but not limited to a desktop, laptop, mobile device, or other supported endpoint, that is capable of running the Endpoint Agent and being managed through the Service
Endpoint Agent	Means the software component provided by Licensor that is installed on a Device to enable monitoring, management, policy enforcement, and data exchange with the Service.

License Details for Core Endpoint Management Express

License Model

Core Endpoint Management Express is licensed on a per-Device, subscription basis. One (1) Device license is required for each Device enrolled in the Service.

Licensable Device

A Device is deemed licensable and consumes one (1) Device license when the Endpoint Agent is installed and enabled on such Device. Any Device meeting this condition is considered an active Device for license consumption purposes.

Device Retirement

The Licensee may designate a Device as retired so that it no longer requires an active license. To initiate retirement, the Licensee must permanently update the Device object attribute to “Retired” within the Service. A Device that remains continuously in the “Retired” state for one hundred and twenty (120) days shall be deemed fully retired. Upon completion of the 120-day retirement period, the Licensee is no longer required to maintain a subscription license to retain the retired Device record in the Service.

Device Deletion

As an alternative to retirement, the Licensee may permanently delete a Device from the Service. Upon deletion, the Device ceases to consume a license, and the corresponding license capacity is released.

Data Download Usage

Data downloaded from the Service under an active subscription is measured and counted against the applicable data download entitlement. Each licensed Device includes an entitlement of ten (10) gigabytes (GB) of data downloads per calendar month. The total data download entitlement is aggregated across all licensed Devices under the subscription and displayed as a cumulative available data download allowance. Data consumption against the data download metric is metered and made available to the Licensee for monitoring and reporting within the Service. The aggregated data download entitlement resets at the beginning of each calendar month. Unused data download entitlement does not roll over to subsequent months unless expressly stated otherwise in the applicable Order Form.

Service Support

Customer may contact OpenText through submitting online support tickets. The OpenText Support Team will either provide support to Customer directly or coordinate delivery of this support.

Support for SaaS is available at: <https://www.microfocus.com/en-us/support>

OpenText staffs and maintains a 24x7x365 Service Operations Center, which will be the single point of contact for all issues related to the support for SaaS. Customer will maintain a list of authorized users who may contact OpenText for support. Customer's authorized users may contact OpenText for support via the Web portal 24 hours a day, 7 days a week.

Support Features:

Activity	
Customer Manager	O
Welcome Package	✓
24x7 Phone and Email Access	✓
Version and Security Updates	
Major, minor, and hotfix version updates. Notification period according to notification timelines via email, release notes and help resources available	✓
Enhanced Technical Enablement	O
Remote mentoring and train-the-trainer sessions on selected product features	
99.5 % Availability SLO	✓
✓ = Included	
O = Optional for a fee	

Service Monitoring

OpenText monitors SaaS availability 24x7. OpenText uses a centralized notification system to deliver proactive communication about service changes, outages and scheduled maintenance. Alerts and notifications are sent to customer administrators via email.

Capacity and Performance Management

The architecture allows for scaling if better performance is needed through increasing compute.

Operational Change Management

OpenText follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and application, which enables beneficial changes to be made with minimal disruption to the service.

Data Backup and Retention

The data backup and retention described in this section are part of OpenText' 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.

SaaS Data

Customer is solely responsible for the data, text, audio, video, images, software, and other content input into a OpenText system or environment during Customer's (and its Affiliates' and/or Third Parties') access or use of OpenText SaaS ("SaaS Data"). The following types of SaaS Data reside in the SaaS environment:

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

- **User and Account Data:** This is data created by Customer that identifies users in their organization who have access to the application
- **Endpoint Data:** Data about software, hardware and use of application is collected from endpoint devices and is stored in Endpoint Management Service. This data can be accessed by customer through Endpoint Management Service
- **Activity Data:** Interaction with the SaaS creates activity data that will be logged which may include usernames and IP addresses

OpenText performs a backup of SaaS Data every one (1) day. OpenText retains each backup for the most recent seven (7) days.

OpenText' standard storage and backup measures are OpenText' only responsibility regarding the retention of the SaaS Data, despite any assistance or efforts provided by OpenText to recover or restore the SaaS Data. Customer may request via a service request for OpenText to attempt to restore SaaS Data from OpenText' most current backup. OpenText 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

OpenText continuously evaluates different risks that might affect the integrity and availability of SaaS. As part of this continuous evaluation, OpenText develops policies, standards and processes that are implemented to reduce the probability of a continuous service disruption. OpenText documents its processes in a business continuity plan ("BCP") which includes a disaster recovery plan ("DRP"). OpenText 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.

OpenText Core Endpoint Management disaster recovery is implemented and based on the RPO and RTO of the software redundancy committed to by GCP services.

Backups

OpenText performs both on-site and off-site backups with a 24 hours recovery point objective (RPO). Backup cycle occurs daily where a local copy of production data is replicated on-site between two physically separated storage instances. The backup includes a snapshot of production data along with an export file of the production database. The production data is then backed up at a remote site. OpenText uses storage and database replication for its remote site backup process. The integrity of backups is validated by (1) real time monitoring of the storage snapshot process for system errors, and (2) annual restoration of production data from an alternate site to validate both data and restore flows integrity.

SaaS Security

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

Technical and Organizational Measures

OpenText 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 OpenText but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

Physical Access Controls

OpenText maintains physical security standards designed to prohibit unauthorized physical access to the OpenText equipment and facilities used to provide SaaS and include OpenText data centers and data centers operated by third parties. This is accomplished through the following practices:

- Presence of on-site security personnel on a 24x7 basis
- Use of intrusion detection systems
- Use of video cameras on access points and along perimeter
- OpenText employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises
- Monitoring access to OpenText facilities, including restricted areas and equipment within facilities
- Maintaining an audit trail of access

Access Controls

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

- Secure user identification and authentication protocols
- Authentication of OpenText personnel in compliance with OpenText standards and in accordance with ISO27001 requirements for segregation of duties
- SaaS Data is accessible only by authorized OpenText 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

OpenText’s business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. OpenText’ 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 OpenText of events such as a server crash or disconnected network.

Controls regarding disruption prevention include:

- Uninterruptible power supplies (UPS) and backup power generators
- At least two independent power supplies in the building
- Robust external network connectivity infrastructure

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. OpenText 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

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

Audit

OpenText appoints an independent third party to conduct an annual audit of the applicable policies used by OpenText to provide SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer’s execution of OpenText’ standard confidentiality agreement, OpenText 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 OpenText confidential information.

OpenText Security Policies

OpenText 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 OpenText confirms a security incident resulted in the loss, unauthorized disclosure or alteration of SaaS Data ("Security Incident"), OpenText 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 OpenText Security Operations Center via SED@opentext.com.

OpenText Employees and Subcontractors

OpenText 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 SaaS Data. OpenText requires that any affiliate or third-party subcontractor involved in processing SaaS Data enters into a written agreement with OpenText, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

Data Subject Requests

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

Scheduled Maintenance

To enable Customer to plan for scheduled maintenance by OpenText, OpenText reserves predefined timeframes to be used on an as-needed basis. OpenText reserves a weekly two (2) hours window (Sunday 00:00 to 02:00 Pacific Standard Time) and one (1) monthly four (4) hour window (Sunday in the 00:00 to 08:00 Pacific Standard Time block). These windows will be used on an as-needed basis.

Planned windows will be scheduled at least two (2) weeks in advance when Customer action is required, or at least four (4) days in advance otherwise.

Scheduled Version Updates

"SaaS Upgrades" are defined as major version updates, minor version updates, and binary patches applied by OpenText to Customer's SaaS in production. These may or may not include new features or enhancements. OpenText 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 OpenText offers on an optional basis for an additional fee.

OpenText determines whether and when to apply a SaaS Upgrade to Customer's SaaS. Unless OpenText anticipates a service interruption due to a SaaS Upgrade, OpenText may implement a SaaS Upgrade at any time without notice to Customer. OpenText 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 OpenText determines in its discretion is critical for the availability, performance or security of SaaS.

Service Decommissioning

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

Upon decommissioning, Customer shall un-install / remove Endpoint Agent from all its endpoints enrolled into Endpoint Management.

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

Service Level Objectives

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

SaaS Provisioning Time SLO

SaaS Provisioning Time is defined as SaaS being available for access over the internet. OpenText targets to make SaaS available within five (5) business days of Customer's Order for SaaS being booked within the OpenText 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 are not in scope of the SaaS Provisioning Time SLO.

Additionally, the import of SaaS Data into the application is not in scope of the SaaS Provisioning Time SLO.

SaaS Availability SLO

SaaS Availability is defined as the SaaS production application being available for access and use by Customer over the Internet. OpenText will provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5 % ("SaaS Uptime").

Measurement Method

SaaS Uptime shall be measured by OpenText using OpenText monitoring software running from a minimum of four global locations with staggered timing.

On a quarterly basis, SaaS 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 = 99.5% availability).

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

Boundaries and Exclusions

SaaS 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
- Outages caused by disruptions attributable to force majeure events (i.e., unforeseeable events outside of OpenText' reasonable control and unavoidable even by the exercise of reasonable care)
- Actions or omissions of Customer (unless undertaken at the express direction of OpenText) or third parties beyond the control of OpenText
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of OpenText
- Scheduled maintenance
- 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 OpenText SaaS which are not validated, reviewed, and approved in writing by both parties
- System downtime requested by Customer
- Suspensions of the OpenText SaaS by OpenText as a result of Customer's breach of the SaaS Terms

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal <https://www.microfocus.com/en-us/support> being available for access and use by Customer over the Internet. OpenText 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 OpenText using OpenText 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 OpenText) or third parties beyond the control of OpenText
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of OpenText
- 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 OpenText online customer portal. The Initial SaaS Response Time covers both service request and support requests. OpenText 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 OpenText SaaS support teams. They in no way create a legal requirement or obligation for OpenText to respond in the stated time. The Response and Resolution Targets, including their scope and determining factors (such as impact and urgency), are further described at <https://home.saas.microfocus.com/myaccount/slo/>.

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 OpenText. OpenText targets to make available such data for download in the format generally provided by OpenText for 30 days following the termination of the SaaS Order Term.

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and OpenText responsibilities relative to SaaS. OpenText' 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
Business Owner	• Owns the business relationship between the customer and OpenText • Owns the business relationship with the range of departments and organizations using SaaS • Manages contract issues
Project Manager	• Coordinates customer resources as necessary • Serves as the point of contact between the customer and OpenText • Drives communication from the customer side • Serves as the point of escalation for issue resolution and service-related issues
Administrator	• Serves as the first point of contact for SaaS end users for problem isolation • Performs SaaS administration • Provides tier-1 support and works with OpenText to provide tier-2 support • Coordinates end-user testing as required • Leads ongoing SaaS validation • Trains the end-user community • Coordinates infrastructure-related activities at the customer site • Owns any customization
Subject Matter Expert	• Leverages the product functionality designed by Customer's SaaS administrators. • Provides periodic feedback to the SaaS Administrator

OpenText Roles and Responsibilities

OpenText 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 OpenText systems and SaaS for availability • Performs system-related tasks such as backups, archiving, and restoring instances according to OpenText' 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 OpenText:

- Customer must have internet connectivity to access SaaS
- SaaS will be delivered remotely in English only
- A SaaS Order Term is valid for a single application deployment, which cannot be changed during the SaaS Order Term
- The service commencement date is the date on which Customer's Order is booked within the OpenText order management system
- The import of SaaS Data into SaaS during the implementation requires that the information is made available to OpenText at the appropriate step of the solution implementation and in the OpenText designated format
- Customer must ensure that its administrators maintain accurate contact information with OpenText
- 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 OpenText'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 OpenText. 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 OpenText in performing its obligations under this Service Description, OpenText will not be liable for such failure or delay.