# Service Description

## Core Data Discovery and Risk Insights Software-as-a-Service

## January 2026

opentext™

## Contents



This Service Description describes the components and services included in Core Data Discovery and Risk Insights (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.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

Core Data Discovery and Risk Insights SaaS is a subscription service that delivers data discovery capabilities that enrich data and expose value across our Customer's deep and rich data eco-systems. Core Data Discovery and Risk Insights is built to help **mitigate the risks associated with managing and preserving sensitive data** while containing the total cost of compliance – all from a single source in the cloud.

Core Data Discovery and Risk Insights provides **two** levels of service:

1. **Express Edition:** multi-tenant environment geared towards project-based discovery and risk assessments. Throughput can vary, but we benchmark approximately ~250GB indexed full content analysed per day*.
2. **Dedicated Edition:** this is a private, dedicated environment geared towards large, multi-national enterprises looking to have full analysis and cloud resources devoted for their project alone. Throughput can vary, but we benchmark in upwards of 2TB full content analysed per day* and dedicated cloud instance. A dedicated cloud setup fee is required for this edition.

Customers cannot move between service editions over the span of the subscription term.

*Throughput is dependent on many factors including the location of data (on-premises vs. cloud), the customer's internet pipe to the instance, the complexity of grammars (and in some cases the specific grammars in use), customer location in relation to the cloud hosting data center, and other resources allocated on the environment.

Within each edition the Customer has access to pay-per-use base services for metadata analysis, and storage services for building a data inventory index with optional pay-per-use services included for full-content file analysis and cloud-based data discovery (via an agentless service).

### Aviator

The CDDRI Aviator is a pop-up conversational dialog within the current user interface enabled through the Aviator icon on the toolbar. Use CDDRI Aviator to get answers to questions about using OpenText Core Data Discovery & Risk Insights. Smart Insight responses are compiled based on information in the Help Center.

CDDRI Aviator utilizes the Amazon Nova large language model using the AWS Bedrock service. Notwithstanding anything to the contrary in the SaaS Terms, the following terms apply:

- The terms and conditions that apply to use of Amazon Nova are: (i) the AWS Customer Agreement, (ii) the AWS Service Terms, (iii) the AWS Acceptable Use Policy, and (iv) the AWS Responsible AI Policy. Additionally, the AWS Privacy Notice governs use of personal information in AWS Services.
- Micro Focus does not guarantee the accuracy of AI-generated responses and/or rights to use them. It is Micro Focus' customer's responsibility to apply judgement and consider multiple sources before making any decisions.
- The SaaS may include and/or enable the use of predictive algorithms, generative artificial intelligence, and/or other components commonly referred to as artificial intelligence technologies

("AI Components"), all of which may be provided by third parties. By utilizing the Aviator feature, Customer agrees to the following:

- The AI Components may use or analyze Customer data based on parameters that have been determined, identified, and/or defined by Customer. Customer's choice of parameters and the types of Customer data which are Inputs into the relevant Products may include assumptions, biases and limitations which will affect the effectiveness, quality, relevance and accuracy of the outputs.
- The quality of the Outputs resulting from AI Components depends on the quality of the Inputs. The quality of the Inputs is the sole responsibility of Customer.
- Use of AI Components does not replace decision-making and judgement by natural individuals. The AI Components are intended to provide additional knowledge to support such decision making and judgement. Customer remains solely responsible for any decisions taken and judgements as a result of the Outputs. Customer agrees that Micro Focus shall have no liability resulting from (i) the creation and/or use of the Outputs, and/or (ii) any decisions resulting from the use of the Outputs. Unacceptable risk use (as defined in EU AI Act or per industry standards) is prohibited.
- For all AI Components that use large language models (including other technology affiliated with generative artificial intelligence), the nature of the technology may limit (i) the protection of privacy, (ii) rights to use, and/or (iii) the accuracy of the Outputs. Therefore, Micro Focus does not guarantee (i) the protection of privacy, (ii) rights to use, and/or (iii) the accuracy of the Outputs with regard to such AI Components and/ or use of such models and related technologies.
- Access to and use of any third-party products including and/or enabling AI Components may be subject to Customer agreeing to additional terms as notified to Customer or its user(s) at the time of order, installation, enablement, access or use of the relevant third-party service/product, and/or which may be as specified in paragraph 6 below, incorporated and made part of this Agreement.
- Applicable laws may provide for additional requirements concerning the use of AI Components in certain contexts, services or projects. Customer is solely responsible for identifying and complying with the requirements applicable to the implementation and use of the relevant services and products (including AI Components) in Customer's processes.
- Micro Focus shall be entitled to use, develop or share its experience and knowledge (including processes, ideas, statistical and other information) acquired by it in connection with the Products ("Services Statistics") provided that any such use of the Services Statistics by Micro Focus is in a manner or form whereby (i) the Customer is not identified as a source of any such Service Statistics; and (ii) any data arising from the Services Statistics is anonymized.

**Standard Subscription Licenses**

Core Data Discovery and Risk Insights provides monthly subscription terms (1-60 months) with a base subscription fee to run the service. Use of the service is licensed through flexible credits purchased upfront called Voltage Authorization Units (VAU). These VAUs are drawn down monthly based on utilization and VAUs that are purchased but not consumed prior to the expiration of the SaaS Term, shall be deemed to have expired and Customer shall have no rights to apply such VAUs or to receive a refund.

**For example, if you purchased 2,500 VAUs to run your sensitive data discovery project, and after month one you used 125 VAUs, you would have 2,375 VAUs remaining for the term.**

Service utilization is monitored and reported to show you (1) the amount of VAUs that have been consumed in the current month, (2) total consumption since the contract began, and (3) how many VAUs remain for the duration of the term.

Core Data Discovery and Risk Insights maps VAUs to the following services:

### Data Optimization (Metadata Only)

Data optimization is a critical stage in preparing data for clean-up, migration, and compliance related projects. Core Data Discovery and Risk Insights metadata analysis is the first step in the processing workflow and is included in all editions of Core Data Discovery and Risk Insights. This service can be used alone or in conjunction with the Standard or Enhanced data discovery processing services.

### Enhanced Data Discovery Processing (Analyzed)

Enhanced data discovery processing extracts the contents of documents being analysed and that full content is indexed in the application. Full content analysis helps identify PII, PCI, PHI etc. within the content of the files. Each repository you connect to the Core Data Discovery and Risk Insights can be configured to use various combinations of regionally and globally targeted grammars to identify sensitive data.

### Cloud Data Discovery (Source Cloud)

A Customer can use either an agentless data discovery or their on-premises connectors to collect data from a cloud-based source such as Office 365, SharePoint Online, and Google Drive. Cloud Data Discovery requires additional cloud resources to process and analyze this type of content.

### Structured Data Sources

Structured data discovery can be set up and configured within Core Data Discovery and Risk Insights to analyze structured data sources. Structured data adapters are provided through the on premise and cloud cluster agents.

### Data Inventory and Storage

Core Data Discovery and Risk Insights analyzes data in place without the need to collect the file itself. The results of that analysis are stored in the index and can include metadata, extracted text, enrichment tags, risk scores, and other metadata about processing and management activities. The index can be maintained for different purposes including:

- Search – full-text index for discovery and data management tasks
- Risk assessment – index maintains only classification tags for reporting and privacy impact assessment reporting

*Relates to any subsequent dataset scans after initial scan
**All rescanned table, changed or not

## Overview

| Core Data Discovery and Risk Insights | Express | Dedicated |
|---|---|---|
| **Tenant** | Multi-Tenant environment* | Dedicated environment* |
| **Database table analysis – throughput**** | 100 Tables/24hr | 500 Tables/24hr |
| **Full content analysis – throughput**** | ~250GB/24hr | ~2TB/24hr |
| **Data Optimization** | Pay upfront by unit***<br>Reported monthly | Pay upfront by unit***<br>Reported monthly |
| **Enhanced Data Discovery (Processing)** | Pay upfront by unit***<br>Reported monthly | Pay upfront by unit***<br>Reported monthly |
| **Cloud Data Discovery (Agentless analysis)** | Pay upfront by unit***<br>Reported monthly | Pay upfront by unit***<br>Reported monthly |
| **Metadata index, Data Inventory, legal hold** | Pay upfront by unit***<br>Reported monthly | Pay upfront by unit***<br>Reported monthly |

*Core Data Discovery and Risk Insights SaaS offering is provisioned using a single tenant within a multi-tenant environment. Each Customer has their data logically and securely segregated in such an architecture. Each Customer is called a tenant. A dedicated environment can be purchased as part of the Dedicated edition.
**Based on a Core Data Discovery and Risk Insights instance at full capacity where the SaaS resource pool is shared across 8-10 tenants with all analytical grammars selected.
***Unit of measure (UoM) for licensing is a unit (Voltage Authorization Units).

### Additional License Components*

Optional Micro Focus products integrated with the Core Data Discovery and Risk Insights:

| Micro Focus Products | Use Case | Description |
|---|---|---|
| Content Manager | Data Preservation | Archive and manage business records for compliance purposes in Content Manager directly |
| IDOL Media Server | OCR/Rich Media | Extract sensitive data from scanned images and rich media with Media Server integration directly |
| Structured Data Manager | Database analysis | Extract sensitive data analysis from database sources with Structured Data Manager integration directly |

*Separate entitlements required

## SaaS Service Delivery Components

| SaaS Delivery Components | Core Data Discovery and Risk Insights |
|---|---|
| **1. Agent configuration** | **Optional for a Fee** |
| **2. Analytics Configuration** | **Optional for a Fee** |
| **3. LDAPS Directory Federation** | **Optional for a Fee** |
| **4. SAMLv2 Single Sign-On (SSO)** | **Optional for a Fee** |
| **5. Content Manager Integration *** | **Optional for a Fee** |
| **6. Custom adapters** | **Optional for a Fee** |
| **7. Media Server integration/configuration**** | **Optional for a Fee** |
| **8. Agentless, cloud-based file analysis - Office365 (OneDrive for Business, Exchange Online)** | **Optional for a Fee. Included in all editions.** |
| **9. Structured Data Manager** | **Optional for a Fee. Included in all editions.** |
| **10. Dedicated cloud instance of Core Data Discovery and Risk Insights** | **Set-up fee included in Dedicated Edition.** |

**Supported versions: Please refer to Support Matrix documentation on the Micro Focus documentation page for Core Data Discovery and Risk Insights*

## Architecture Components

Core Data Discovery and Risk Insights consists of two parts: (1) Native cloud-based micro services and management platform with file analysis capabilities along with interactive dashboard for management and reporting; and (2) a set of on-premises agents or cloud to cloud connectors, deployed from the application to connect to the data source(s) in real-time for the purposes of collecting, extracting data for analysis, and management. These data sources can be on-premises (Exchange, SharePoint, CIFS File shares, OpenText Documentum, OpenText Extended ECM, Content Manager*) or in the cloud (Office 365).

(*Please refer to Support Matrix documentation documentation page)

Deployment and management of following on-premises agents, connectors and integrated software components is a Customer responsibility:

1. Agent and custom adapters
2. IDOL Media Server
3. Content Manager
4. Structured Data Manager

## Application Administration

Core Data Discovery and Risk Insights service offering includes the following web-based applications:

- **Administration** provides administration of users, user groups, and roles and permissions
- **Connect** provides all the means to instantiate and configure agents and connect the SaaS solution to the various data sources (repositories) and data targets. In addition, Connect lets the Customer configure how the files are analyzed for the purpose of entity extraction (grammars) and classification (tagging)
- **Analyze** provides dashboards, reporting, and data discovery capabilities
- **Manage** provides deeper analysis on a subset of the data and management of the analyzed data (e.g., secure, delete, report)

New services will be released over time across Core Data Discovery and Risk Insights to support further data privacy, data security, and data protection use cases.

Core Data Discovery and Risk Insights supports collecting, indexing, and analyzing from Customers' Exchange, SharePoint, file system, OpenText Documentum, OpenText Extended ECM and Content Manager using on-premises agents. In addition, it supports connecting directly to M365, SharePoint Online, and Google Drive.

## Data Usage Events Summary

Data usage is tracked within the application under the Administration tab. The table below shows possible actions taken inside the service and how consumption is tracked over time.

| Action | Action parameters | | | Triggered Events | | | |
|---|---|---|---|---|---|---|---|
| | Object | Through Cloud Agent | Store Content as Text | Metadata-Only (metric: source doc size) | Analyzed (metric: source doc size) | Source Cloud (metric: source doc size) | Structured Data (metric: table count) |
| **Ingest/Scan** | Metadata-Only Document | Yes | - | X | | X | |
| **Ingest/Scan** | Metadata-Only Document | No | - | X | | | |
| **Ingest/Scan** | Full/Smart Scan (Analyzed) | Yes | Yes | | X | X | |
| **Ingest/Scan** | Full/Smart Scan (Analyzed) | No | Yes | | X | | |
| **Ingest/Scan** | Full/Smart Scan (Analyzed) | Yes | No | | X | X | |
| **Ingest/Scan** | Full/Smart Scan (Analyzed) | No | No | | X | | |
| **Ingest/Scan** | Database table/View Smart/Full Scan | Yes | - | | Sample file size | Sample file size | X |
| **Ingest/Scan** | Database table/View Smart/Full Scan | No | - | | Sample file size | | X |
| **WB: Analyze** | Metadata-Only Document | Yes | Yes | | X | X | |
| **WB: Analyze** | Metadata-Only Document | No | Yes | | X | | |
| **WB: Analyze** | Metadata-Only Document | Yes | No | | X | X | |
| **WB: Analyze** | Metadata-Only Document | No | No | | X | | |
| **WB: Analyze** | Analyzed Document content already stored | no consumption event | | | | | |
| **WB: Analyze** | Analyzed Document content NOT stored | Yes | - | | X | X | |
| **WB: Analyze** | Analyzed Document content NOT stored | No | - | | X | | |
| **Change Tags** | - | no consumption event | | | | | |
| **Change dataset grammars** | Metadata-Only Document | no consumption event | | | | | |
| **Change dataset grammars** | Analyzed Document content already stored | no consumption event | | | | | |
| **Change dataset grammars** | Analyzed Document content NOT stored | Yes | - | | X | X | |
| **Change dataset grammars** | Analyzed Document content NOT stored | No | | | X | | |
| **Change grammar sets and "re-analyze"** | Analyzed Document content already stored | no consumption event | | | | | |
| **Change grammar sets and "re-analyze"** | Analyzed Document content NOT stored | Yes | - | | X | X | |
| **Change grammar sets and "re-analyze"** | Analyzed Document content NOT stored | No | | | X | | |
| **Re-scan*** | Metadata-Only Document | Yes | - | new & updated documents | | new & updated documents | |
| **Re-scan*** | Metadata-Only Document | No | - | new & updated documents | | | |
| **Re-scan*** | Full/Smart Scan (Analyzed) | Yes | Yes | | new & updated documents | new & updated documents | |
| **Re-scan*** | Full/Smart Scan (Analyzed) | No | Yes | | new & updated documents | | |
| **Re-scan*** | Full/Smart Scan (Analyzed) | Yes | No | | new & updated documents | new & updated documents | |
| **Re-scan*** | Full/Smart Scan (Analyzed) | No | No | | new & updated documents | | |
| **Re-scan*** | Database table/View Smart/Full Scan | Yes | - | | Sample file size | Sample file size | rescanned table** |
| **Re-scan*** | Database table/View Smart/Full Scan | No | - | | Sample file size | | rescanned table** |
| **WB: Collect** | Metadata-Only Document | Yes | - | | X | X | |
| **WB: Collect** | Metadata-Only Document | No | - | | X | | |
| **WB: Collect** | Full/Smart Scan (Analyzed) | Yes | - | | | | |
| **WB: Collect** | Full/Smart Scan (Analyzed) | No | - | | | | |

## Service Support

Customer may contact Micro Focus through submitting online support tickets or by telephone. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support.

Online support for SaaS is available at: https://support.cyberreshelp.com

Email at: MFI-Cyberressupport@opentext.com

Micro Focus staffs and maintains a 24x5x52 weeks Service Operations Center with on-call coverage on weekends and holidays for Severity 1 issues 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 Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal or telephone 24 hours a day, 7 days a week.

| Severity Level | Technical Response | Update Frequency | Target For Resolution | What Qualifies? |
|---|---|---|---|---|
| 1 | Immediate | Hourly | 4 hours | Total or substantial failure of service. Known or suspected security events |
| 2 | 30 mins | Every 2 hours | 8 hours | Significant degradation of service, major feature inability |
| 3 | 4 hours | Every 8 hours | 24 business hours | Performance issues outside the norm but not substantial enough to prevent usability of a feature. Issues with reports generated from within the Customer's Tenant |
| 4 | As available | As available | Determined by the Customer impact or LOE | Bugs in deployed products not substantial enough to prevent required Customer functionality from being accessible but requiring development time to resolve |

## Service Monitoring

Micro Focus monitors Core Data Discovery and Risk Insights solution components 24x7 availability. Micro Focus uses a notification system to deliver proactive communications about application changes, outages, and scheduled maintenance. Alerts and notifications are available to Customer online at: https://support.cyberreshelp.com

### Capacity and Performance Management

The architecture allows for addition of capacity to applications, databases, and storage. Additional agents can be added to increase collection and extraction rates. Setup of these additional agent machines are the responsibility of the customer.

### Operational Change Management

Micro Focus 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 Micro Focus's overall business continuity management practices designed to attempt to recover availability to Customer of Micro Focus and access to the Customer data, following an outage or similar loss of service.

### SaaS Data

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

When objects are captured by the Core Data Discovery and Risk Insights processing agent, the extracted content and relevant metadata is transmitted to the back office for further enrichment. The end results are then held in index storage within the back office.

Optionally, you may elect to also collect data (either by choice or to enforce a hold). In this case, a copy of the original data object is then also transmitted to the back office, which will be held in object storage within the back office.

Individual tenant data is stored in separate indexes and object storage locations.

All incoming communication (from web users, on-premises agents, FTP clients, and so on) is transmitted exclusively via TLS 1.2+ using only high strength cipher suites (Encryption in Transit).

Object and volume storage containing non-ephemeral data is encrypted using the industry standard AES-256 algorithm (Encryption at Rest).

Industry standard Principle of least privilege (PoLP) is consistently applied. This is applied within the application, as well as within the back office (governing access to infrastructure resources, limiting intra-back-office communications, and so on).

Micro Focus performs a backup of SaaS Data Daily. Micro Focus retains each backup for the most recent fourteen (14) days.

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.

**Backups**

Micro Focus SaaS utilizes cloud-native functions such as replication between primary and secondary availability zones to ensure data availability and recoverability. All replicas reside within the same governmental compliance boundary to ensure adherence to all applicable data residency regulations. Real-time replication is used between primary and standby nodes to facilitate an RPO of 2 hours (Real-time replication is used between nodes). No removable media is used at any time to ensure the protection of customer data.

### Disaster Recovery

**Business Continuity Plan**

Micro Focus SaaS continuously evaluates different risks that might affect the integrity and availability of Micro Focus SaaS. As part of this continuous evaluation, Micro Focus SaaS 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 Micro Focus SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that Micro Focus SaaS implements and tests Micro Focus SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

**High Availability and Durability**

Micro Focus SaaS utilizes cloud-native functions such as replication between primary and secondary availability zones to ensure data availability and recoverability. All replicas reside within the same governmental compliance boundary to ensure adherence to all applicable data residency regulations. Real-time replication is used between nodes. No removable media is used at any time to ensure the protection of Customer data.

## 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 may be modified by Micro Focus but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

## Physical Access Controls

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS, including Micro Focus 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
- Micro Focus employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on-premises
- Monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities
- Maintaining an audit trail of access

## 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 Micro Focus 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 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

Micro Focus SaaS environments are segregated logically by Micro Focus SaaS 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 to detect hostile activity, and monitoring the environment's health and availability.

### Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted. Data in the relational database, index, and object storage (data at rest) is also encrypted.

## Audit

Micro Focus appoints an independent third party to conduct an annual 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 conducts annual reviews of its policies around the delivery of SaaS against ISO 27001. 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.

## 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 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 MFI-Cyberressupport

## Micro Focus Employees and Subcontractors

Micro Focus requests 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 requests 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 Maintenance

To enable Customers to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis.

A twenty-four-hour period once a quarter starting at 00:00 Saturday, in the local data center region, and ending at 00:00 Sunday.

- This window is considered an optional placeholder for major releases and events that could be significantly service impactful. If the window is to be exercised, and a major disruption expected, all Customers should be notified no later than ten business days before.

A two-hour maintenance window once a month starting Tuesday at 00:00, in the local data center region.

- This is for patching of environments. Patching should be done in a non-service disrupting fashion; however, some elements may require a brief outage to update properly. Customers will be notified at least five business days in advance if any actual service disruption is expected.

A four-hour maintenance window once a month starting Saturday, midnight in the local data center region.

- This time is set aside for system updates and product releases that cannot be performed without a visible Customer impact. Use of this window is optional, and Customers should be notified at least ten business days in advance if any outage is expected.

In case of any holiday conflicts, the regularly scheduled window will automatically fall to the following week on the same day of the week.

Micro Focus determines whether and when to apply a SaaS Upgrade for Customer's Core Data Discovery and Risk Insights. 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 Core Data Discovery and Risk Insights.

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

### Tenant Off Boarding SLO

Micro Focus guarantees a tenant off boarding time of two days from the time in which the Customer submits the formal written request. If a formal written request to delete Customer data is not submitted, off boarding of Customer data will take place as set forth below in Termination Data Retrieval Period SLO.

### User Removal SLO

Micro Focus guarantees that after the completion of this request, analytical results about the removed user will no longer be stored or available within the application.

### SaaS Availability SLO

SaaS availability is defined as the Core Data Discovery and Risk Insights production application being available for access and use by Customer and its Authorized Users over the Internet. Micro Focus will provide Customer access to the Core Data Discovery and Risk Insights production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5%.

### 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.

## Standard Service Requirements

### Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to the Core Data Discovery and Risk Insights service. 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 |
|---|---|
| **Business Owner** | • Owns the business relationship between the Customer and Micro Focus<br>• Owns the business relationship with the range of departments and organizations using Core Data Discovery and Risk Insights Service<br>• Manages contract issues. |
| **Project Manager** | • Coordinates Customer resources as necessary<br>• Serves as the point of contact between the Customer and Micro Focus<br>• Drives communication from the Customer side<br>• Serves as the point of escalation for issue resolution and service-related issues |

| | |
|---|---|
| **Administrator** | • Serves as the first point of contact for Core Data Discovery and Risk Insights Service end users for problem isolation<br>• Performs Core Data Discovery and Risk Insights Service administration<br>• Provides tier-1 support and works with Micro Focus to provide tier-2 support<br>• Coordinates end-user testing as required<br>• Leads ongoing solution validation<br>• Trains the end-user community<br>• Coordinates infrastructure-related activities at the customer site<br>• Owns any customization |
| **Subject Matter Expert** | • Leverages the product functionality designed by Customer's Core Data Discovery and Risk Insights Service administrators<br>• Provides periodic feedback to the Core Data Discovery and Risk Insights Service Administrator |

## Micro Focus Roles and Responsibilities

| Micro Focus Role | Responsibilities |
|---|---|
| **Customer Success Manager (CSM)** | • Serves as the Customer liaison to Micro Focus<br>• Coordinates Micro Focus resources including system and process experts as necessary<br>• Facilitates ongoing mentoring<br>• Coordinates with the Customer during required and periodic maintenance<br>• Oversees the Customer onboarding process |
| **Service Operations Center Staff (SOC)** | • 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 the Core Data Discovery and Risk Insights Service<br>• Provides 24x7 application support<br>• Provides 24x7 SaaS infrastructure support |
| **Operations Staff (Ops)** | • Monitors the Micro Focus systems and Core Data Discovery and Risk Insights Service for availability<br>• Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices |

## 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 (ports 9000-9999 range) to access this Core Data Discovery and Risk Insights Service
- Core Data Discovery and Risk Insights Service will be performed remotely and delivered 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 Micro Focus order management system
- The Customer data indexed during the ingestion process requires the data location information be made available to Micro Focus to analyze the data
- Customer must ensure that its administrators maintain accurate contact information with Micro Focus SaaS
- 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, this Core Data Discovery and Risk Insights Service is provided based on the assumption that Customer will implement and maintain the following controls in its use of Core Data Discovery and Risk Insights Service:

- Configuring Customer's browser and other clients to interact with Core Data Discovery and Risk Insights Service
- Configuring Customer's network devices to access Core Data Discovery and Risk Insights Service
- Appointing authorized users
- Configuring its Core Data Discovery and Risk Insights Service account to require that end user passwords be sufficiently strong and properly managed
- Procedures for access approvals, modifications, and terminations

## Good Faith Cooperation

Customer acknowledges that Micro Focus's ability to perform the 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.