Service Description

Micro Focus Digital Safe Foundations Software-as-a-Service

July 2021

V7.3

Contents

“This Service Description describes the components and services included in Micro Focus Digital Safe Foundations and above Software-as-a-Service (which also may be referred to as “SaaS”). Unless otherwise agreed to in writing this Service Description is subject to the Micro Focus Customer Terms for Software-as-a-Service or the applicable Micro Focus Pass-Through Terms and represents the only binding terms governing Micro Focus International plc and its affiliates (“Micro Focus”) respective obligations regarding its provision of this SaaS to the end-user customer. Any other descriptions of the features and functions of the SaaS, public statements, including advertisements, shall not be deemed as additional features or functionalities that Micro Focus is required to deliver. Updated March 2021”

Digital Safe Foundations SaaS Services Overview

High Level Summary

The Micro Focus Digital Safe Foundations is a SaaS Cloud Managed Service solution that provides secure write once read many (WORM) compliant archiving for a diverse set of modern electronic communications.

The Digital Safe Platform's capabilities are built on the compliance data lake platform as the foundation of unified search, surveillance, discovery, audit, analytics and end user email search.

Further details on Digital Safe Platform can be found here.

SaaS Service Components Offered

SaaS Service Components	
One SaaS Digital Safe Foundations Tenant*	✓
Digital Safe Supervision Foundation per Archived User	✓
Digital Safe Supervision Foundation per Monitored User	✓
End User Email Search per Archived User	✓
Message Compliance Manager 2021.1	**Optional for a Fee**
Social Media Governance Connectors	**Optional for a Fee**

✓ = Included

* Micro Focus Digital Safe Foundations 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.

SaaS Service Delivery Components

Digital Safe Foundations

Compliance Archiving
Micro Focus Digital Safe Foundations is a cloud-based, multi-tenanted solution which provides secure, WORM compliant archiving. Electronic communications are ingested with near synchronous, geo-remote replication of messages coupled with hourly geo-replicated index snapshots. This allows clients to know what message items (objects) have been received by the Digital Safe, what the objects' journey through the Digital Safe have been, reconcile the send and received objects and provide evidential proof that the integrity of the contents has been maintained. Electronic communications including email, social media, collaboration and audio are enriched and indexed for efficient search, audits, regulatory response and discovery. The offering provides a scalable, compliant query capability that enables the user to search the corpus of messages, metadata search, and compliant audit capability that enables user to perform highly complex searches on all indexed content and provides standard as well as premium advanced reporting capabilities.

Digital Safe Foundations Solution Specific Components	
Archiving – Compliance WORM • Data is retained at the file level for a specified duration, files cannot be deleted under retention or legal hold • Duration is based on regulatory requirements • Applies to all data within a domain • Document types enforced in data processing pipeline for ease of query • 2GB per archived user per year in primary and geo-replicated location included	✓
Continuance of Business • Replication of client data to a geo-redundant data center, includes: • Verification of stored items in the geo-redundant datacenter Hourly index snapshots stored in geo-redundant datacenter	✓
Deduplication of live stream data • Duplicate messages sent within 14 days of the original message will be de-duplicated out of the data set • Full duplicate fields: Date, message ID, Subject • Variant duplicate fields: To, CC, BCC	✓
Retention Management • Web-based application provides clients with the ability to set policy-based retention rules, establish legal holds and execute data deletion tasks • Highly scalable **retention objects** limits • Holds managed through Digital Safe functionality and user permissions across archive storage	✓
Digital Safe Search and Export • Web-based application used to search and preview data in the Digital Safe Solution	✓

• Enables search bulk export, bulk retrieval and export of data in multiple industry standard formats • 200GB of export monthly in individual containers of up to 20GB	
Connectivity • Support for up to two VPN connections or private leased line (Customer provided) – HTTPS/FTPS – Verisign SSL certificates – SSO Capability (SAML 2.0) • Encryption at rest for all live feed content • Encryption in flight from customer site to private cloud	✓
Metadata enrichment capabilities	✓
Internationalization with double byte character language support – option to turn on at setup	✓
Foundation Reports via Reporting Insights	✓
Archive capable of handling multiple content types including Email, Social, Collaboration, **File, Audio, Video archiving require optional setup**	✓ Optional setup
Modify or Customize Reports	**Optional for a Fee**
Data Feeds such as Bloomberg, Symphony, TRefinity (formerly Thomson Reuters)	**Optional for a Fee**
Social media and collaboration data feeds such as MS Teams, Slack, Salesforce Pardot	**Optional for a Fee**

Micro Focus Digital Safe Foundations Supervision

Supervision functionality is delivered as a multi-tenanted cloud-based solution which enables customers to surveil, investigate, and analyze all electronic communications to meet the compliance and regulatory requirements of the SEC, FINRA, the IIROC as well as other global regulators. Providing automated import and organization of employees into risk-based groups facilitates comprehensive supervision and surveillance capabilities across multiple forms of electronic communication. This includes, but is not limited to email, instant messages, social media, collaboration and Bloomberg messaging. Electronic communications are sampled based on employee or group risk and communications channels, leveraging Micro Focus best practice risk-based policy filters.

Digital Safe Foundation Supervision Solution Specific Components

Access to the Digital Safe Foundations compliance archiving	✓
Customize surveillance of monitored users based on individual risk factors	✓
5 Default user roles with option to customize 2 additional roles	✓
Escalation and workflow management	✓
Reporting and trend analysis	✓
Executive web-based dashboards and system administration	✓
Policy management enrichment	✓
Automated display of reviewers' workload	✓
Message violation highlighting	✓
Best Practice policy filters for over 30 areas of risk	✓
Market Segment Policy Packages	**Optional for a Fee**
Audit Trails	✓

Best Practice Sampling up to 2500 messages per day includes • Communication channel • Message direction (inbound, outbound, or internal) • Entire groups or specific employees • Desired percentage and mix Random sampling • Policy filter alerts only • Policy filter alerts plus random percentage • Fixed amount with a mixed percentage of random and policy filter alerts	✓
Policy Selection Engine – Real-time policy-based monitoring	✓
Regular expressions searches	✓
Translation	Optional for a Fee
✓ **= Included**	

Micro Focus Foundations End User Mail Search

Foundations End User Mail Search allows end users to securely search and view their communications, calendar appointments and attachments directly (and exclusively). Like Outlook, users can be made 'delegates' to search and view their communications. The solution mirrors a user's own email system in many ways system – allowing them to search their mailbox or calendar or social media communications that have been stored in an immutable WORM archive.

Digital Safe Mail (DSMail) Solution Specific Components

Access to the Digital Safe Foundations archive Authenticated user has access to their sent or received electronic communications stored in compliant archive	✓
Access restricted to a user's identified communications / documents. Secure access to a single user's communications and archived documents. Communications and documents must be identified as belonging to specific user account	✓
Full Boolean search capabilities on the content a user has access to Authenticated users will have full search capabilities within their communications and documents, including Boolean search operators to construct complex queries.	✓
Access to explicitly identified delegated users' Any user may receive access to a 'delegated' user's mailbox / archived documents. If a delegate has been identified via LDIF or SCIM then an authenticated user will have the option to toggle between the accounts. Logging into a delegated account will function the same as logging into a personal account.	✓

Download selected document Authenticated users can, within the context of viewing a document, may opt to download that document locally. Please note that the format of the downloaded document, depending on the source material (e.g. social media) may be in HTML or other generic format.	✓
See / utilize past searches Authenticated users may save, access and then re-run past searches. This can be performed manually as a saved search or through search history which records recent searches.	✓
Determine favorite documents and default searches Users can manually (through the UI) designate favorite documents and default searches. Favorite documents may then be accessed at any later time – and the favorite status can be manually removed. Default searches is, also, a manual UI function, allowing a user to automatically run a search when they access their Inbox or Social Media (for examples.) Default searches may be removed or changed at any time and only controlled at the user level (not a default for all users)	✓
Web-based data preview capabilities – including email, calendars, social media, etc. Authenticated users will have the ability to see any selected communication or document. The rendering of the document will default to an HTML view of the selected document.	✓
Usage Reporting Those with appropriate permissions will have access to end user search system usage statistics, including the number of logins to the system.	✓
Custom product branding Clients may provide their own logo and color scheme throughout most of the main UI to provide their users with a more seamless corporate experience.	✓
✓ **= Included**	

Micro Focus Message Compliance Manager

The Micro Focus Message Compliance Manager is a solution that tracks all the messages that were ingested into Digital Safe and provides reconciliation and reporting. The product is built on top of Micro Focus Secure Messaging Gateway. Secure Messaging Gateway has many built-in features including anti-virus and anti-spam protection.

The Message Compliance Manager ensures all messages have been properly retained into Digital Safe and acts as central hub to route messages into Digital Safe.

Message Compliance Manager can be installed on-premises or on the Micro Focus Cloud. For messages routed through Social Media Governance (SMG), the Message Compliance Manager can track messages between SMG and Digital Safe.

Message Compliance Manager Solution Specific Components	
Capturing of Messages • **Tracks all messages including email, and social media**	✓
Delivery of Messages • **Route messages to Digital Safe** • **Store and Forward of Messages**	✓
Reconciliation • **Automatic reconciliation of messages with Digital Safe**	✓
Foundation Reports • **Reconciliation Report** • **Message Capture Report**	✓
Archive capable of handling multiple content types including Email, Social, Collaboration, File, Audio	✓
Anti-virus protection	Optional for a Fee
Route messages to other destinations systems	Optional for a Fee
✓ **= Included**	

Social Media Governance

Micro Focus Social Media Governance addresses the need to compliantly archive social media content with added security. The solution connects to a wide range of social media and collaboration platforms including Twitter, LinkedIn, Facebook, MS Teams, Cisco Jabber and many others. Content including comments and posts, and attachments, are captured and archived.

Digital Safe Social Media Governance (SMG) Solution Specific Components	
Ingest of Social Media and Collaboration Channels to Digital Safe archive including	✓

• Role permissions/groups. SCIM is the preferred configuration methodology	
Single Archive Search including • Native viewing of social content • API integration with social channels • Endpoint management without an agent	✓
Supervision via Digital Safe Foundations supervision functionality	Requires Digital Safe Foundations Supervision
Analytics and Reporting • Dashboards • Report templates • Export options	✓
Data Processing and Formatting • Timestamps • Metadata preservation • Format/thread replication	✓
✓ **= Included** **O = Optional for a fee**	

Full Capabilities for Social Media Governance can be found here.
Data is stored in the Social Media Governance database for up to two weeks. Retention Management and Holds are managed from the archive.

SaaS Operational Services

Operational Services	
On-boarding Enablement	✓
External Integrations Support	Optional for a Fee
✓ **= Included**	

Architecture Components

Micro Focus deploys Micro Focus Digital Safe Foundations on SaaS Service using a shared infrastructure platform, monitors the system for 24x7 availability, and provides related 24x7 infrastructure support, including application version upgrades.
The Customer accesses Micro Focus Micro Focus Digital Safe Foundations on SaaS Service through the Internet (HTTPS).

Any required onsite components are installed and configured by the Customer or Customer contracted Consultants. Micro Focus does not operate onsite components or third-party integrations on behalf of the Customer and will not commit to any SLO for these components.

Client-Side Access

Micro Focus Digital Safe Foundations on SaaS Service access is provided as a web-based application accessible through a supported web browser as outlined in the product release notes.

Deployment method to the end users is the responsibility of Customer.

Service Components

The Customer may contact Micro Focus through a variety of methods such as online support tickets or telephone. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support.
Online support is available at: https://portal.digitalsafe.net/

Product support is available from the Micro Focus Micro Focus Digital Safe Community at: *portal.digitalsafe.net.* Micro Focus staffs and maintains a 24x7x365 Service Operations Center, which will be the single point of contact for all issues related to the support for Micro Focus Digital Safe on SaaS Service for the Customer. The customer will maintain a list of authorized users who may contact Micro Focus for support. The customer's authorized users may contact Micro Focus for support via the Web portal Monday through Friday, 6am Eastern to 11pm Eastern Time.

Support Services Guide

During the Term, Micro Focus will provide support services in the form of error corrections, updates, and email support (the "**Support Services**") to up to two (2) designated CUSTOMER technical contacts.

Description of Support Services.

1.1. Error Corrections. Micro Focus shall exercise commercially reasonable efforts to correct any error reported by CUSTOMER in the current unmodified release of the Digital Safe Solution or error reported by CUSTOMER with the hosted infrastructure in accordance with the priority level reasonably assigned to such error by Micro Focus. If a reported error has caused the Digital Safe Solution to be inoperable, or CUSTOMER' notice to Micro Focus states that the reported error is substantial and material with respect to CUSTOMER' use of the Digital Safe Solution, Micro Focus shall use its reasonable commercial efforts to correct expeditiously such error or to provide a software patch or bypass around such error. CUSTOMER acknowledges that all reported errors may not be corrected. Micro Focus shall have no obligation to support: (i) altered, damaged or modified Digital Safe Solution Services or any portion of thereof unless the Digital Safe Solution Services was altered, damaged, or modified by or on behalf of Micro Focus; or (ii) problems caused by CUSTOMER' negligence, abuse, misapplication or use of the Digital Safe Solution other than as specified in the documentation, or other causes beyond the reasonable control of Micro Focus. Micro Focus shall have no liability for changes in CUSTOMER' hardware necessary to use the Digital Safe Solution due to a workaround or maintenance release.

1.2. Updates. Updates and upgrades to Digital Safe Foundations shall be provided in accordance with Scheduled Maintenance and Upgrades section noted below. Micro Focus may, in its sole discretion, modify this Service Description and make available Updates to its customers which may add new and/or eliminate existing features, functions, operating environment and/or hardware platforms to the Subscription Service.

1.3. Support Options. Micro Focus Digital Safe customers can log support tickets by either, email, or logging an incident directly into our customer portal. The Micro Focus Operations team is staffed 24x7x365 to work on customer support incidents. Support email addresses may be found on Micro Focus's website. Micro Focus support personnel are also available to answer questions related to the Digital Safe Solution and provide assistance to CUSTOMER regarding accessing the Digital Safe Foundations Solution.

Priority Levels of Service Incidents - In the performance of Support Services, Micro Focus uses the impact and urgency of an issue to determine its relative priority.

2.1 Impact Categorization – Digital Safe Core Services

Impact	Archiving	Digital Safe UI	Compliant Search
Extensive/Widespread	Archiving performance severely impacted. (>75%) portals not archiving or no message archiving Mail queues building up on client side (SMTP) Batch fails archiving no messages (via API) Live stream archival only Portals are the landing point to process data	All users unable to access/utilize Application searches not completing/erroring	All users unable to access Audit/Exports failing in the following states have priority: *eSubmission *eQuery *eDelivery Or >50% audits failed

	being received by Digital Safe		
Significant/Large	Archiving performance impacted > 50% of portals not archiving for a given client (SMTP) Batch >50% fails to archive (API)	Multiple users unable to access application Multiple user unable to run search Search inconsistency	Multiple users unable to access No Audits/Exports progressing or are errored All audits/exports on a single CSD are filing (<50% and >25% of total audits)
Moderate/Limited	Archiving performance impacted > 25% of portals not archiving for a given client (SMTP) Batch >25% failures to archive (API)	Single user unable to access application Single user unable to run search Slow performance within SLA Individual user search inconsistent with DSUI	Multiple audits/exports failed (<25% but more than 1)
Minor/Localized	Single message failures, large message processing or single portal failures where <25% of customer traffic impacted	Cosmetic issue with search or applications	Cosmetic issues other usability problems or single audit/export failure

2.2 Impact Categorization – Digital Safe Applications

Impact	Supervisor	DSMail	Digital Safe eDiscovery
Extensive/Widespread	>50% of users unable to access application All searches failing archive/mailbox or body and attachment search	All users unable to access/run searches >50% of users unable to access application All searches failing	>50% of users unable to access application All searches failing

Significant/Large	Multiple users (25-50%) unable to access application or single app server failure Multiple users unable to run search Search inconsistency Other application performance concerns (e.g. message to message navigation)	Multiple users (25-50%) unable to access/run searches Searches failing for multiple users	Multiple users (25-50%) unable to access application Searches failing for multiple users
Moderate/Limited	Multiple users (<25%) unable to access application Single user unable to run search	Multiple users (<25%) unable to access/run searches Single user unable to run search Display issues for user in end user search	Multiple users (<25%) unable to access application Single user unable to run search Individual users search not consistent
Minor/Localized	Cosmetic issues and/or supervisor reports issues	Cosmetic issue and other usability issues	Cosmetic issue and other usability issues

2.3 Impact Categorization – Digital Safe Foundations

Urgency is the necessary speed of resolving and incident	
High	Imminent losses or exposure (Legal/Financial), or immediate but reducible impact with workarounds
Medium (Normal)	Potential/future (1 week or more) losses or exposure (legal/financial). Individual issue, where no manual workaround exists and which: • Makes performance or continued performance of any one or more system functions difficult. • The end user cannot circumvent or avoid on a temporary basis
Low	A non-critical issue where a workaround exists or that the end user is able to circumvent. User inconvenience

2.4 Impact Categorization – Message Compliance Manager

Impact	**Supervisor**
Extensive/Widespread	MCM services not able to receive messages MCM services not able to deliver messages to Digital Safe when there are no network outages. Reconciliation service is down for more than 12 hours.

Significant/Large	Reconciliation process is very slow. For messages delivered into Digital Safe for more than one day, MCM is not able to provide confirmation. When delivering to third-party systems, MCM is not able to verify message delivery. Proper running of third-party systems cannot be verified by Micro Focus.
Moderate/Limited	Reconciliation process is very slow. For messages delivered into Digital Safe for more than two days, MCM is not able to provide confirmation. Reports are not getting delivered to customers
Minor/Localized	Cosmetic issues and/or MCM reports issues

2.4 Incident Ticket Priority

The JIRA Service Desk will then determine the appropriate **Incident Priority** using the Impact/Urgency combination:

Priority		URGENCY		
Calculation		High	Medium	Low
IMPACT	Extensive / Widespread	**Urgent**	High	High
	Significant / Large	High	High	Medium
	Moderate / Limited	High	Medium	Medium
	Minor / Localized	Medium	Medium	Low

3. Impact Categorization – Digital Safe Foundations

Notification Type	Major Incident*	High Priority	Medium Priority	Low Priority
First Technical Response (FTR)	1 hour	4 hours	24 hours	48 hours
Major Incident Notification (MINS) update frequency	4 hours	N/A	N/A	N/A
Status update frequency	Daily	24 hours	2 business days	Weekly
Internal Resolution Target	24 hours	72 hours	168 hours	720 hours

Recovery Point and Recovery Time Objectives:

Recovery Point Objectives: Data storage is recoverable to the point of failure. Restored indexes are up to date within two hours of the archived data.

Recovery Time Objectives: Index restoration is at the time services are restored and online – index restoration will complete based on the date range and size of the impacted index.

Hardware failures are typically resolved within 3 days. A catastrophic datacenter completely offline, except in case of act of god, will be restored in 7-10 business days.

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.

Solution Data Availability and Data Replication

The data availability, replication and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability and access to Customer of Digital Safe Foundations customer data, following an outage or similar loss of service.

Our Foundations compliance archive solution indexes and archives data in a primary Cloud, then replicates data to a geo-remote cloud near synchronously. A snapshot of the index is taken and is replicated to a geo-remote Cloud hourly. Our SaaS Operational Business Continuity Plan provides additional information.

Disaster Recovery

The Micro Focus Cloud Operations team continuously evaluates different risks that might impact the integrity and availability of Micro Focus Digital Safe Foundations. As part of this continuous evaluation, Micro Focus Cloud Operations team 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").

SaaS Security and Audit

Micro Focus Security Policies

Micro Focus purpose-built private cloud environments are SOC II compliant, we are re-audited annually for SOC II and we regularly re-evaluate and update our information and physical security program as the industry evolves, new technologies emerge or new threats are identified.

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability and integrity of Customer Personal Data and confidential information (the "Micro Focus Security Program").

Technical and Organizational Measures

This section describes Micro Focus´ standard technical and organizational measures, controls and procedures, which are intended to help protect the Customer-provided SaaS Data.

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

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS and include 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; securing equipment hosting Customer-provided SaaS Data in designated caged areas; and maintaining an audit trail of access.

Micro Focus Employees and Subcontractors

Micro Focus requests that all employees involved in the processing of Customer-provided SaaS Data are authorized personnel with a need to access the Customer-provided 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 Customer-provided 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.

Access Controls

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

- Secure user identification and authentication protocols;
- Customer provided 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;" and prohibition of shared accounts.

Availability Controls

Micro Focus´ business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus' 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.

Controls regarding disruption prevention include:

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

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 and content-based inspection in order to detect hostile activity in addition to monitoring the environment's health and availability.

Data Encryption

Micro Focus SaaS uses industry standard techniques to enforce encryption of all inbound and outbound data.

Network Connections and Hardware; Customer Media

Customer will be solely responsible for procuring and maintaining the network connections that connect the Customer network to Micro Focus systems, as well as any firewalls, authentication methods, and encryption methods it deems appropriate. In addition, Customer will be solely responsible for procuring and maintaining any hardware located at a Customer site and utilized in connection with the Subscription Services.
In connection with any Subscription Services involving Customer's delivery of physical media containing Customer data, Customer will deliver to Micro Focus only copies of tangible media, not originals, or will create appropriate backups of the Customer Data contained on any original media that is delivered to Micro Focus.

Demarcation Point

The Demarcation Point shall be defined as the point at which Customer connects to Service Provider's data center. Customer will be solely responsible for procuring and maintaining the network connections that connect the Customer network to the point at which Customer connects to Service Provider's data center ("Demarcation Point") (inclusive of any firewalls, authentication methods, and encryption methods up to the Demarcation Point) which Customer deems appropriate.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure or alteration of Customer-provided 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 *softwaresoc@microfocus.com*.

Scheduled Maintenance and Updates

Scheduled Maintenance

Scheduled Maintenance is any Micro Focus planned activity which impacts the service to the client. Micro Focus reserves a weekly window outside of standard business hours, which are weekdays 6 a.m. Eastern Standard Time to 5 p.m. Eastern Standard Time. Micro Focus performs scheduled maintenance currently scheduled on a weekly basis between Friday at 10:00 p.m. Eastern Standard Time and Monday at 8:00 a.m. Eastern Standard Time. These windows will be used on an as-needed basis. Non-service disrupting changes can be applied at any time.

Version Updates

"SaaS Updates" are defined as both major version updates, minor version updates and binary patches applied by Micro Focus to Customer's Micro Focus Digital Safe Foundations on SaaS Service in production. These may or may not include new features or enhancements. Micro Focus determines whether and when to develop, release and apply any SaaS Update.
Customer is entitled to SaaS Updates as part of Micro Focus Digital Safe Foundations on SaaS Service unless the SaaS Update introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Multi-Tenant Shared Environment

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's Micro Focus Digital Safe Foundations. 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 will execute any service-impacting upgrades during non-business hours or off hours. MF may, at its sole discretion, change the times during which it performs such scheduled maintenance upon written notice to Customer. The Subscription Services and/or Customer data may be unavailable during a scheduled maintenance. 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 Micro Focus Digital Safe Foundations. Customer understands that patches will not be back-ported to non-current versions of the solution.

Service Decommissioning and Data Retention

Customer may cancel Micro Focus Digital Safe Foundations on SaaS service by providing Micro Focus with One Hundred and Twenty (120) days written notice prior to the expiration of the SaaS Order Term ("Cancellation"). Such Cancellation shall be effective upon the last day of the then current SaaS Order Term. Upon Cancellation, expiration, or termination of the SaaS Order Term, Micro Focus may disable all Customer access to Micro Focus Digital Safe Foundations on SaaS Service, and Customer shall promptly return to Micro Focus (or at Micro Focus' request destroy) any Micro Focus Materials.

Data Retention

Unless otherwise specified in an Order, Customer will be charged the applicable fees for the capture, indexing and/or archiving of Customer-provided Data from the period beginning on the date such Customer-provided Data is archived and ending on the date on which a specific set of Customer-provided SaaS Data is no longer retained (the "SaaS Order Term"). Where Customer-provided SaaS Data is archived beyond the expiration of the SaaS Order Term, the archiving of such Customer Data will automatically convert to extended archiving for consecutive one-year terms ("Extended Archiving") at the then-current rate and fees. Extended Archiving fees will be based on the volume of Customer-provided SaaS Data archived that has reached its Retention Period or Legal hold expiration date. Extended Archiving fees will appear as a separate line item on Customer's invoices.

Customer may at any time provide Micro Focus with written notice that it elects to discontinue Extended Archiving, provided that such notice must also contain an instruction to Micro Focus to either destroy or return Customer Data in lieu of Extended Archiving, and Customer will remain obligated for the payment of fees for Extended Archiving.

Return and Disposition of Customer Data

At any time during an applicable SaaS Order Term, Customer may request in writing that Micro Focus Services export a copy of any or all of its Customer-provided SaaS Data or **direct Micro Focus to delete and decommission its Customer-provided SaaS Data for a fee at the expiry of the SaaS Order Term, any Retention Period, or Legal Hold**.

Micro Focus will comply with such request, except (a) to the extent prohibited by applicable law, (b) with respect to Customer-provided SaaS Data that has not yet reached its Retention Period or Legal Hold expiration date, and (c)
in the event Customer has not paid in full all fees due and owing hereunder through the date of such request.

Unless otherwise specified on an Order, any Customer-provided SaaS Data that is deleted will be deleted from the storage cell and/or raid configured disk, using standard deletion methods. Unless otherwise specified in an Order, the fees for data export services and/or data deletion services will be based on Micro Focus' then-current rates for such services.

Within thirty (30) days following the expiration of a SaaS Order Term, Customer will send written notice to Micro Focus instructing it to export or delete/erase all Customer Data. In the absence of such written instruction, Micro Focus may export all Customer-provided SaaS Data to Customer on a medium and in a format of Micro Focus' choice, and Customer shall be obligated for the payment of fees associated with such return.

Notwithstanding the foregoing, Customer's directions, or anything else to the contrary Customer agrees that in the event that any SaaS Order Term expires and Customer has not requested that a copy of its Customer-provided SaaS Data be exported or preserved through Extended Archiving within (120 days), Micro Focus may securely delete or destroy the Customer-provided SaaS Data without any liability, and Micro Focus will have no responsibility or obligation for any Customer-provided SaaS Data that remains in the Micro Focus SaaS environment after such (120 day) period.

Service Level Commitments

Service Level Agreement

Micro Focus provides clear, detailed, and specific Service Level Agreements (SLAs) for the services that the SaaS Managed Service provides to its customers. These SLAs are targets used by Micro Focus to deliver the service and are provided as guidelines.
Micro Focus will provide self-service access to Customer to the Service Level measurements and Service Level Objectives data online at https://portal.digitalsafe.net/

1. **Solution Object Receipt SLA**
   Solution Object Receipt SLA addresses compliant object receipt. Object Receipt Uptime is defined by Micro Focus as the ability to receive objects from the customer into the portal cluster. Micro Focus guarantees Object Receipt Uptime specific to objects sent to the portal directly by Customer, exclusive of 3rd party connectors, on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9%.

2. **Solution UI Availability SLA**
   Micro Focus will provide Customer access to the Micro Focus Digital Safe SaaS Managed Service production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5% ("Solution UI Availability").

3. **Measurement Methods**
   Solution Object Receipt Uptime shall be measured by Micro Focus through DREAM monitoring of portal/system availability. DREAM is web-based front-end application that services monitoring data from Digital Safe. Dream consists of a number of dashboards that represent different facets of the monitoring platform. Unavailability of the full portal cluster constitutes an outage. On a monthly basis, Solution Object Receipt Uptime will be measured using the measurable minutes in the month (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. "Availability", expressed as a percentage, means the period of time, as measured monthly, during which the Application is Available for Object Receipt, and is calculated in accordance with the following formula:

   Availability % = 100% x (Total Minutes per Month – Outage Minutes Per Month) ÷ (Total Minutes Per Month)
   *Outage Minutes accrue from the moment of report until the moment of restoration or workaround.

   Solution UI Availability shall be measured by Micro Focus through DREAM monitoring of portal/system availability. On a monthly basis, Solution UI Availability will be measured using the measurable minutes in the month (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator.
   "Availability", expressed as a percentage, means the period of time, as measured monthly, during which the Solution UI is Available, and is calculated in accordance with the following formula:

Availability % = 100% x (Total Minutes per Month – Outage Minutes Per Month) ÷ (Total Minutes Per Month)
*Outage Minutes accrue from the moment of report until the moment of restoration or workaround.

An “Outage” is defined as two consecutive monitor failures within a five minute period where UI is unavailable for user access, lasting until the condition has cleared. Closed sessions do not constitute an outage.

Boundaries and Exclusions
Solution Uptime shall not apply to any of the following exceptions:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of the SaaS agreement
- Actions or omissions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Failure in any hardware, software, system or network external to the Micro Focus Digital Safe Foundations SaaS service and not owned, operated or under the control of Micro Focus (by way of subcontract or otherwise);
- Scheduled Maintenance
- Scheduled Version Updates

Reporting
Micro Focus will provide self-service access to Customer at https://portal.digitalsafe.net/
In addition Micro Focus will make available at https://portal.digitalsafe.net/ a SaaS Service Uptime Metric Report (“Uptime Metric Report”) on the portal on the fifth business day of each month. If the Customer does not agree with the Uptime Metric Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the Uptime Metric Report.

Online Support Availability SLO

Online Support Availability is defined as the Micro Focus SaaS support portal https://portal.digitalsafe.net/ being available for access and use by Customer and its Authorized Users over the Internet. Micro Focus targets to provide Customer access to the Micro Focus SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5% (“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 (2,189 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

Online Support Uptime shall not apply to any of the following exceptions:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of agreement
- 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

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the Service Support described herein. It is defined as the acknowledgment of the receipt of a customer 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 a customer 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 always 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://portal.digitalsafe.net/

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to the Micro Focus Digital Safe Foundations on SaaS service. Customer acknowledges that Micro Focus utilizes storage technology that does not employ optical disk technology for the storage of Customer-provided SaaS Data. In the event Customer is subject to Rule 17a-4 promulgated under the Securities Exchange Act of 1934, as amended (“Rule 17a-4”), then Customer will be solely responsible for determining which letters it must file with certain governmental authority(ies) (each a "Governmental Authority") pursuant to Rule 17a-4 ("Rule 17a-4 Letters"), which letters may include letters filed under Rule 17a-4(f)(2)(i), Rule 17a-4(f)(3)(vii) and Rule 17a-4(f)(3)(i), and for filing or causing such letters to be filed. 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 • Owns the business relationship with the range of departments and organizations using Micro Focus Digital Safe Foundations SaaS Service • Manages contract issues
Administrator/Project Manager	• Serves as the first point of contact for Micro Focus Digital Safe Foundations on SaaS Service end users for problem isolation • Performs Micro Focus Digital Safe Foundations on SaaS Service administration • Provides tier-1 support and works with Micro Focus to provide tier-2 support • Coordinates end-user testing as required • Leads ongoing solution validation • Coordinates infrastructure-related activities at the customer site • Coordinates network connection to the demarcation line • Defines Sources of message ingest • Interface between the MF project team and the Customer departments • Administering Change Authorization procedures with the Micro Focus Contact • Obtaining and providing information, data, decisions and approvals as reasonably requested by MF • Facilitating the reasonable cooperation of Customer contractors whose cooperation is needed to fulfill the obligations under this agreement ensuring appropriate Customer personnel take the MF-provided training

	• Escalating issues within the Customer organization, as required • Coordinating data access approvals within the Customer
Compliance Sponsor	• Principally responsible for approving decisions related to compliance aspects of Customer data. • Determines any change to the six year default retention period • Responsible for determining that the solution meets their regulatory needs
Customer Executive Sponsor	• Ultimate decision maker on behalf of Customer for the Solution.
Technical Sponsor	• Principally responsible for providing technical input and information to assist in establishing and providing the technical environment required to complete the Solution
Legal Sponsor	• Principally responsible for approving decisions related to legal aspects of the Customer Data

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Services Operations Center	• Performs system-related tasks such as provisioning of networking and hardware, on-going maintenance, setup and configuration of the Software and restoring instances according to Micro Focus' standard practices • Provides 24x7 SaaS infrastructure support • 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 Micro Focus Digital Safe Foundations on SaaS Service • Monitors the Micro Focus systems and Micro Focus Digital Safe Foundations on SaaS Service for availability

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 this Micro Focus Digital Safe Foundations on SaaS Service.
- Micro Focus Digital Safe Foundations on SaaS 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 purchase order (PO) is booked within the Micro Focus order management system.
- The import of Customer data into the Micro Focus Digital Safe Foundations on SaaS service during the implementation requires that the information is made available to Micro Focus at the appropriate step of the solution implementation and in the Micro Focus designated format.
- 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.
- Performance of the Digital Safe Foundations on SaaS service is dependent on being on a version no more than two minor releases older than the current release. Any additional performance constraints can be found here

Furthermore this Micro Focus Digital Safe Suite on SaaS Service is provided based on the assumption that Customer will implement and maintain the following controls in its use of Micro Focus Digital Safe Foundations on SaaS Service:

- Configuring end user browsers and other clients to interact with Micro Focus Digital Safe Foundations on SaaS Service
- Configuring Customer's network devices to access Micro Focus Digital Safe Foundations on SaaS Service
- Appointing authorized users
- Configuring its Micro Focus Digital Safe Foundations on SaaS Service accounts 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 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.