IBM Master Data on Cloud Managed Service

This Service Description describes the Cloud Service IBM provides to Client. Client means the contracting party and its authorized users and recipients of the Cloud Service. The applicable Quotation and Proof of Entitlement (PoE) are provided as separate Transaction Documents.

1. Cloud Service

IBM Master Data Management ("MDM") on Cloud Managed service ("Cloud Service") manages master data for single or multiple domains – Clients, suppliers, locations, products, services offerings, accounts and more – for improving application and business process effectiveness. IBM manages the infrastructure (network, storage and compute resources), applies fixes to the application and maintains the IBM software, infrastructure and applicable security and privacy controls.

Several key features include:

a. A services-oriented architecture delivers functionality through intelligent, pre-packaged web services that can be used to integrate MDM into existing business processes and technical architectures.

b. Interfaces to the Cloud Service include HTTPS (for application access), Web Services and JMS over HTTPS (for on premises application to Cloud IS/MDM integration) and a secure file transport service for loading data into MDM.

c. The ability for Clients to deploy Client customized MDM and IS solutions and Extensions within the Cloud environment through a support ticket process.

d. Client's choice of integration method to Cloud Service to consume these services via an Application Programming Interface ("API"); Web Services or JMS.

e. Full auditing capabilities to record who requested access to what data and when.

f. Business process management capabilities enable Client to implement policies and coordinate multi-step / multi-role workflows for data stewardship and data governance.

g. Stewardship Center allows business users, data stewards, and IT teams to collaboratively improve master data quality by resolving possible duplicate master data records and creating master data in compliance with corporate governance policies.

h. Matching and search engine employ advanced statistical techniques to automatically resolve and manage data quality issues via probabilistic or deterministic options.

i. The Cloud Service is provisioned in select data centers in a VLAN based single-tenant environment.

j. IBM will provide application log files upon request through the support ticketing interface.

k. IBM will provide a Secure File Transport service in order to facilitate file transfers for loading and/or extracting data from MDM or Information Server.

1.1 IBM Master Data Management Available Configurations

Each Cloud Service configuration represents the capacity to process certain amounts of data volume and user operations in the specified time period as described below. The capacity descriptions are intended to be guidelines to help a Client select an appropriate configuration for intended workloads. Actual results may vary based on Client workload specifics.

1.1.1 IBM Master Data Management on Cloud Managed Small

- Rated for a scale of approximately 5 million party individual records and 35 Transactions Per Second ("TPS") in steady state usage.
- Provides 2TB of Object Storage; additional storage entitlement can be purchased under a separate statement of work.

1.1.2 IBM Master Data Management on Cloud Managed Medium

- Rated for a scale of approximately 30 million party individual records and 100 TPS in steady state usage.
- Provides 5TB of Object Storage; additional storage entitlement can be can be purchased under a separate statement of work.

1.1.3 IBM Master Data Management on Cloud Managed Large

- Rated for a scale of approximately 50 million party individual records and 250 TPS in steady state usage.
- Provides 10TB of Object Storage; additional storage entitlement can be purchased under a separate statement of work.

2. Content and Data Protection

The Data Processing and Protection data sheet (Data Sheet) provides information specific to the Cloud Service regarding the type of Content enabled to be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. Any details or clarifications and terms, including Client responsibilities, around use of the Cloud Service and data protection features, if any, are set forth in this section. There may be more than one Data Sheet applicable to Client's use of the Cloud Service based upon options selected by Client. The Data Sheet may only be available in English and not available in local language. Despite any practices of local law or custom, the parties agree that they understand English and it is an appropriate language regarding acquisition and use of the Cloud Services. The following Data Sheet(s) apply to the Cloud Service and its available options. Client acknowledges that i) IBM may modify Data Sheet(s) from time to time at IBM's sole discretion and ii) such modifications will supersede prior versions. The intent of any modification to Data Sheet(s) will be to i) improve or clarify existing commitments, ii) maintain alignment to current adopted standards and applicable laws, or iii) provide additional commitments. No modification to Data Sheet(s) will materially degrade the data protection of a Cloud Service.

Link(s) to the applicable Data Sheet(s):

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=3FC503E0646911E89B7C7F20C63AA31F

Client is responsible to take necessary actions to order, enable, or use available data protection features for a Cloud Service and accepts responsibility for use of the Cloud Services if Client fails to take such actions, including meeting any data protection or other legal requirements regarding Content.

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and DPA Exhibit(s) apply and are referenced in as part of the Agreement, if and to the extent the European General Data Protection Regulation (EU/2016/679) (GDPR) applies to personal data contained in Content. The applicable Data Sheet(s) for this Cloud Service will serve as the DPA Exhibit(s). If the DPA applies, IBM's obligation to provide notice of changes to Subprocessors and Client's right to object to such changes will apply as set out in DPA.

3. Service Level Agreement

IBM provides the following availability service level agreement ("SLA") for the Cloud Service as specified in a PoE. The SLA is not a warranty. The SLA is available only to Client and applies only to use in production environments.

3.1 Availability Credits

Client must log a Severity 1 support ticket with the IBM technical support help desk within 24 hours of first becoming aware that there is a critical business impact and the Cloud Service is not available. Client must reasonably assist IBM with any problem diagnosis and resolution.

A support ticket claim for failure to meet an SLA must be submitted within 3 business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the Cloud Service based on the duration of time during which production system processing for the Cloud Service is not available ("Downtime"). Downtime is measured from the time Client reports the event until the time the Cloud Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond IBM's control; problems with Client or third party content or

technology, designs or instructions; unsupported system configurations and platforms or other Client errors; or Client-caused security incident or Client security testing. IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service during each contracted month, as shown in the table below. The total compensation with respect to any contracted month cannot exceed 10 percent of one twelfth (1/12th) of the annual charge for the Cloud Service.

3.2 Service Levels

Availability of the Cloud Service during a contracted month

Availability during a contracted month	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
Less than 99.9%	2%
Less than 99%	5%
Less than 95%	10%

* If the Cloud Service was acquired from an IBM Business Partner, the monthly subscription fee will be calculated on the then-current list price for the Cloud Service in effect for the contracted month which is the subject of a claim, discounted at a rate of 50%. IBM will make a rebate directly available to Client.

Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month minus the total number of minutes of Downtime in a contracted month divided by the total number of minutes in the contracted month.

3.3 Additional Exclusions

In addition to the Downtime exclusions listed above, SLA credits are not eligible for disruption of the Cloud Service due to Client's actions, including problems with individual Cloud Service components that do not affect the overall availability of the Cloud Service; improper use of a Cloud Service API or functionality; issues caused by custom Extensions; disruption as a result of the VPN Services; Client's failure to allow an IBM-initiated update to be promoted into production.

4. Technical Support

Technical support for the Cloud Service is provided via email, online forums, and an online problem reporting system. IBM's software as a service support guide available at https://www-01.ibm.com/software/support/saas_support_guide.html provides technical support contact and other information and processes. Technical support is offered with the Cloud Service and is not available as a separate offering.

5. Entitlement and Billing Information

The Cloud Service is available under the charge metric specified in the Transaction Document:

- Instance is a unit of measure by which the Cloud Service can be obtained. An Instance is access to a specific configuration of the Cloud Service. Sufficient entitlements must be obtained for each Instance of the Cloud Service made available to access and use during the measurement period specified in Client's PoE or Transaction Document.

5.1 Billing Frequency

Based on selected billing frequency, IBM will invoice Client the charges due at the beginning of the billing frequency term, except for overage and usage type of charges which will be invoiced in arrears.

6. Term and Renewal Options

The term of the Cloud Service begins on the date IBM notifies Client of their access to the Cloud Service, as documented in the PoE at which time VPN setup will begin. The PoE will specify whether the Cloud Service renews automatically, proceeds on a continuous use basis, or terminates at the end of the term.

For automatic renewal, unless Client provides written notice not to renew at least 90 days prior to the term expiration date, the Cloud Service will automatically renew for the term specified in the PoE. In the event the automatic renewal is after receipt of an IBM notice of a withdrawal of the Cloud Service, the renewal term will end the earlier of the end of the current renewal term or the announced withdrawal date.

Renewals are subject to an annual price increase as specified in a quote. In the event the automatic renewal is after receipt of an IBM notice of a withdrawal of the Cloud Service, the renewal term will end the earlier of the end of the current renewal term or the announced withdrawal date.

For continuous use, the Cloud Service will continue to be available on a month to month basis until Client provides 90 days written notice of termination. The Cloud Service will remain available to the end of the calendar month after such 90 day period.

7. Additional Terms

7.1 General

Client agrees IBM may publicly refer to Client as a subscriber to the Cloud Services in a publicity or marketing communication.

Client may not use Cloud Services, alone or in combination with other services or products, in support of any of the following high-risk activities: design, construction, control, or maintenance of nuclear facilities, mass transit systems, air traffic control systems, automotive control systems, weapons systems, or aircraft navigation or communications, or any other activity where failure of the Cloud Service could give rise to a material threat of death or serious personal injury.

7.2 Cloud Service Environment Updates

Maintenance

Cloud Service Major and Minor updates and/or patches will be evaluated for installation within a monthly maintenance window. Two weeks prior to the maintenance window, IBM will publish the list of Major and Minor updates being applied along with a brief description of the updates. The Cloud Service will not be available to Client during this maintenance window. Maintenance windows may last up to 8 hours and are typically the last Saturday of each month.

Client is responsible for testing and compatibility of all Client Extensions and Client specific use of the Cloud Service with proposed updates.

Client may provide a request to delay Major and Minor updates once notified. IBM will use commercially reasonable efforts to coordinate the implementation of the update with the Client. Requests for Major update delays must be provided within 30 days of original notification and requests for Minor update delays must be provided within 7 days of original notification. Client acknowledges and agrees that IBM will deploy Major updates within 6 months of the original notification and will deploy Minor updates within 45 days of notification. In the event of Client's failure to allow an IBM-initiated update to be promoted into the Cloud Service, additional monthly charges could occur.

Emergency Maintenance

In addition to Major and Minor updates, IBM may determine that an emergency environment update is required to address significant vulnerabilities or regulatory requirements and cannot wait for a scheduled maintenance window. In this situation, IBM may update the environment at any point in time with no advance notice to the Client.

7.3 LDAP Directory

A standalone LDAP configuration is included as part of the Cloud Service. Additionally, IBM provides the ability to integrate with Clients' on-premises Active Directory. The following on-premises Active Directory synchronization options can be implemented on request after provisioning has been completed and the environment has been turned over to Client:

a. Authentication to the Cloud Service LDAP Server replicating back to on-premise Client LDAP:
   (1) Support for one (1) Active Directory server
   (2) Provide a (Read Only) domain controller in the Cloud Service that is in the Client domain
   (3) Client manages all end user access to the cloud environment (groups, IDs, access)
   (4) Full admin rights to Client;

b. Authenticate to the Cloud Service LDAP server where the Client manages the users (not in the Client domain);

c. Point to on-premise Client domain controller for authentication

(1) Possible performance implications

(2) Authenticates for the life of the session;

(3) Provide SAML authentication if required

Other configurations (e.g. manual or scripted excerpts of LDAP file directory to the Cloud Service; federation options including MS Federation Services or others) quoted separately.

7.4 Backup and Restore

Routine scheduled file system backups (recommended files) and periodic (daily / weekly / monthly) data base backups are provided. Periodically, backup files will be archived to IBM Cloud Object Storage and retained for up to 28 days. Client will be able to perform 2 backup restores per month. Additional restores or increased system backup frequency greater than on a daily basis can be performed under a separate Statement of Work for an additional charge. Snapshot Backup is not provided.

7.5 Virtual Private Network (VPN)

Client may select to utilize a software VPN connection for securely connecting to the Cloud Service.

a. Configuration of one (1) VPN endpoint (gateway) is provided as part of this Cloud Service. Additional endpoints may be quoted separately and can be added through an additional services agreement.

b. The IBM Cloud Integrated Analytics VPN Connectivity service uses Site-to-Site IPsec VPN technology.

7.6 Third Party Website and / or Other Services

The Cloud Service may contain integrations with, links to or be used to access Third Party Services. Access to Third Party Services is provided "AS-IS", **with no warranty of any kind, express or implied, including the warranaty of title, non-infringement or noninterference and the implied warranties and conditions of merchantability and fitness for a particular purpose**.

Client is responsible for entering into and complying with separate agreements with the third parties for the access to, or use of, such Third Party Services. IBM does not provide these Third Party Services under this offering in the Cloud Service. Except to extent that Client may separately acquire such Third Party Services from IBM in a separate transaction, IBM is not a party to any such separate agreements, and as an express condition of the Agreement, Client agrees to comply with the terms of such separate agreements to the extent that it wishes to use them in conjunction with the Cloud Service. If Client on behalf of itself, any Cloud Service user or any end user, consents to the transmission of Content to such third party service that is linked to or made accessible by the Cloud Service, Client, the Cloud Service user, and end user provide IBM with the consent to enable any such transmission of content, but such interaction shall be deemed to be solely between Client and the third party offering the Third Party Service.

Inbound connections from external third parties will not be allowed.

7.7 Use Restrictions and Limitations

The Cloud Service is limited regarding LDAP, MDM, Business Process Manager ("BPM") and Information Server programmatic and client user interfaces as follows:

a. User Interface functionality is limited to HTTPS access to LDAP, Information Server, MDM and BPM user functionality;

b. IBM is not providing access or interfaces to any of the MDM, BPM and Information Server development tooling as part of this Cloud Service. IBM will provide Client with the ability to deploy MDM, BPM and Information Server customizations, including development artifacts, into the managed environment through the support ticking service;

c. IBM is not providing direct access to the individual servers, OS level, or application admin consoles for MDM, WebSphere Application Server, BPM, Information Server, LDAP or DB2;

d. Inbound and outbound JMS interfaces access is limited to running over an HTTPS protocol for both MDM and Information Server. Support for other protocols, interfaces or connectors can be evaluated but will require an additional services agreement;

e. MDM Web Services interfaces are limited to running over an HTTPS protocol;

7.7.2 Business Process Manager

The Cloud Service includes IBM Business Process Manager functionality. Use of IBM Process Server and IBM Process Center is limited to Master Data Governance and Stewardship Processes only. A Master Data Governance and Stewardship Process may only pass these master data quality decisions to other systems for the purpose of master data synchronization.

7.7.3 Information Server

The Cloud Service includes the functionality of IBM Information Server. Use of Information Server in the Cloud Service is limited to supporting Master Data Management processes and Master Data Management related data. Additionally, Information Server services provided are limited in use to Data Stage, Information Governance Catalog and Quality Stage functionality.

7.8 Disaster Recovery

The disaster recovery objective to restore Client's production data is 14 calendar days.

7.9 Client Obligations

a. Client will provide a single technical point of contact knowledgeable in the client enterprise network, VPN and security requirements.

b. Client will complete the Virtual Private Network ("VPN") questionnaire and return it to IBM for review no later than 60 days from the date the order is placed ("Order Date"). If Client has not provided IBM with the required VPN questionnaire within 60 days of the Order Date, IBM will continue to engage Client to obtain the VPN questionnaire information. Once the VPN questionnaire has been completed and provided to IBM, IBM will notify Client with provisioning details upon completion of the environment VPN configuration, which may take several days.

c. Client will ensure that a security and network administrator is/are available during the configuration and validation phase of the VPN configuration to work with IBM to complete VPN setup.

d. Client is responsible for all administration, maintenance, modification, configuration and testing of hardware and software at the Client site used for the VPN.

e. Client is responsible for user acceptance testing to validate the VPN configuration during implementation.

f. Client will notify via the online problem reporting system of any changes required to VPN configuration.

g. Client is responsible for the definition, setup and maintenance of all LDAP users and groups as they relate to any MDM application solutions deployed by the Client

7.10 Client-Provided Materials

To the extent Client provides IBM with Client or third party drivers, jar files, license files, configuration files, CBA's and other materials or assets that Client asks IBM to use in the Client's Cloud Service environment (collectively "Client-Provided Materials"): Client hereby grants IBM a fully-paid, non-exclusive, non-transferable, worldwide, limited license (without the right to sublicense), under Client's applicable intellectual property rights to use the Client-Provided Materials for the sole purpose of providing the Cloud Service to Client. IBM has sole discretion whether to use such Client-Provided Materials and may cease using Client-Provided Materials at its sole discretion at any time for any reason. Client represents and warrants on an ongoing basis that (a) it has the necessary rights to give Client-Provided Materials to IBM, (b) IBM may lawfully use the Client-Provided Materials in providing the Cloud Service to Client, and (c) the Client-Provided Materials do not contain harmful code. Client must promptly inform IBM if Client loses the right to allow IBM to use the Client-Provided Materials or Client learns it contains harmful code.

Client acknowledges that (a) IBM does not warrant the functionality of Client-Provided Materials within the Cloud Service, and (b) IBM is not responsible or liable to Client to the extent the Client-Provided Materials impairs IBM's ability to meet IBM's: (1) representations and warranties regarding the Cloud Service, and/or (2) the Cloud Service's Service Level Agreement (SLA).

7.11 Extensions

Extensions permit the Client to configure the Cloud Service to meet Client's business requirements by creating software extensions to the Cloud Service application. Extensions are content provided in the use of the Cloud Service and are not part of the Cloud Service. Client is responsible for the development, management, maintenance and support of all Extensions. Client may contract separately with IBM or a third party contractor specifically authorized in writing by IBM to create Extensions. Client is responsible for ensuring that any such third party contractor complies with these terms.

a. Client-created Extensions are subject to the following additional terms and conditions:

(1) IBM will have the right to review and approve or reject the design documents, testing plans, test results and object code for Extensions for compliance with the terms of the Agreement.

(2) IBM may require Client to perform performance tests specified by IBM. Client shall provide such design documents, testing plans and results, and object code to IBM for review a reasonable time in advance of the Cloud Service going live and shall co-operate with IBM in resolving issues identified by IBM.

(3) Client agrees to have in place and maintain a program to prevent malware, including viruses, Trojan horses, denial-of-service and other disruptive and covert technologies from being included in the Extensions.

(4) IBM may monitor and scan Extensions for security vulnerabilities and/or malware. IBM may remove the Extensions from any Cloud Service environment or suspend the Cloud Service until the security vulnerability or malware issue is resolved.

(5) Extensions will not include or add any third party commercial or packaged software product that operates independently of the Cloud Service, and the addition of any such third party commercial or packaged software is prohibited.

(6) Client is responsible to train and maintain staff with an appropriate knowledge and skill level to work with the Cloud Service and Extensions during the term of the subscription. Any training or educational assistance that is required is at the Client's expense. Should it be determined by IBM that the Client is not able to perform its required tasks with reasonable assistance, IBM, at its sole discretion, may require that Client engage in hands-on knowledge transfer activities with IBM professional services personnel. Such knowledge transfer activities shall be, unless between IBM and its affiliates, at the Client's expense. IBM will provide such training to Client upon Client's request for an additional charge.

(7) Client, or their licensors retain all right, title, and interest or license in and to the Extensions provided to IBM for hosting with the Cloud Service. Client represents and warrants to IBM that Client has all rights necessary to provide the Client Extensions to IBM for the purpose of hosting with the Cloud Service and that neither the Client Extensions nor the hosting by IBM with the Cloud Service violate any third party patent or copyright.

(8) Client grants to IBM, on a world-wide, royalty-free, fully-paid, revocable, sub-licensable basis, all rights and licenses to, and agrees to promptly obtain and keep in effect Required Consents for all Extensions, necessary for IBM and its subcontractors to host the Extensions and otherwise perform its obligations. Upon request, Client will provide to IBM evidence of any such rights, licenses, or Required Consents. IBM will be relieved of its obligations to the extent that they are affected by Client's failure to promptly obtain and provide to IBM any such rights, licenses, or Required Consents. In this paragraph, "Required Consents" means any consents, licenses or approvals required to give IBM and its subcontractors the right or license to access, use and/or modify in electronic form and in other forms solely as necessary to perform under this Service Description, including making derivative works, the Extensions, without infringing the ownership or intellectual property rights of the providers, licensors, or owners of such Extensions.

(9) Client will ensure code, data and other artifacts introduced by Client through the Extensions, do not increase the security risk, or require additional certification requirements unless expressly agreed to by IBM through an amendment or addendum to this Service Description. Without limiting any of the foregoing, Client will: (a) perform web application and static code vulnerability scans on all Extensions to identify any security exposures; and (b) disclose to IBM in writing the existence of any exposures that were identified by a vulnerability scan that are included in or is provided in connection with the Extensions.

b. Client is responsible for testing Extensions in all environments.

c. Any additional work to be performed by IBM in support of Extensions, such as creation of Extensions or activation of other integrated components, may be described in a separate statement of work between IBM and Client, and will be subject to separate fees invoiced in accordance with the terms and fees contained in such a statement of work.

7.12 Performance Testing

Client accepts that the Cloud Service is modified by Extensions and integrates with Third Party Services and Client's other applications. As a result, performance and response times cannot be guaranteed by and are not the sole responsibility of IBM. Client is responsible for performing any and all performance tests before and after activation of the Cloud Service Environment for use by the Client for normal business activities and/or use by the Client in servicing, in anyway, their customers and/or use by the Client in support of revenue generation. IBM will provide reasonable assistance to Client in the resolution of any performance as part of support services.

7.13 Definitions

a. **Extensions** – are the software artifacts and configuration provided by the Client, or their authorized third party, to extend the Cloud Service by implementing the Client's business process flow, manage specific data needs, and provide Client specific integration processing, in support of the Client's business requirements. This can be, but not limited to, software code, database extensions, scripts or files created to customize Client's utilization of the Cloud Service, including integrations to Third Party Services or data sources. Extensions are the responsibility of the Client.

b. **Third Party Services** – are third party data services, databases, web services, web sites, software, or other third party content accessed via the Cloud Service.

c. **Major** – is defined as a maintenance update that IBM reasonably determines does require Client Extension and/or data remediation in order to insure compatibility. Examples might include major operating system or MDM/BPM/IS/IS version upgrades.

d. **Minor** – is defined as a maintenance update that IBM reasonably determines does not require Client Extension and/or data remediation in order to insure compatibility. Examples might include minor operating system or MDM/BPM/IS/IS product patches.