IBM Cloud Service Description: IBM Digital Data Exchange

The following is the Service Description for your Order:

1. Cloud Service

The Cloud Service offering, including the base offering and available optional features is described below and as selected in an Order Document. The Order Document will consist of the Quotation that is provided and the Proof of Entitlement (PoE) you will receive from IBM confirming the start date and term of the Cloud Services and when invoicing will commence.

1.1 IBM Digital Data Exchange

IBM Digital Data Exchange is a solution that provides you with a single interface for the configuration and deployment of website and mobile page tags.

IBM Digital Data Exchange enables you to manage IBM tags and IBM Business Partner tags to be deployed on your web or mobile site. The IBM Digital Data Exchange user interface provides direct control over the tagging process, giving users the ability to define page tags and page groups based on a set of rules to determine tag execution. Once you have purchased IBM Digital Data Exchange, you may manage current and previous deployment of IBM tags, IBM Business Partner tags and custom JavaScript or proprietary code to multiple environments.

2. Security Description

2.1 Security Policies

IBM maintains privacy and security policies that are published and communicated to IBM employees. IBM requires privacy and security education to individuals worldwide that support IBM data centers and we maintain a security team that is focused on information security. IBM security policies and standards are reviewed and re-evaluated annually. IBM security incidents are handled in accordance with a comprehensive incident response procedure.

2.2 Access Control

IBM maintains logical separation of client data. Client data resides in its own client-specific schema and is designed to be accessible through the Cloud Service or client-specified data export. Access to the Cloud Service and client data is controlled and managed by the client's designated administrator. IBM uses multi factor authentication and encrypted VPN tunnel technology when accessing client systems. Access is restricted to those individuals requiring access in order to maintain and administer the Cloud Service and associated hardware and software infrastructure in third party data center facilities. IBM uses WIFI (a/k/a 802.11) network traffic that is encrypted using WPA2 with the AES encryption algorithm option and provides for non-broadcast SSID and mutual authentication between the server and the end devices when accessing systems containing client data.

2.3 Service Integrity & Availability

Modifications to operating system resources (OSRs) and application software are governed by IBM's change management process. Hardware, software, access logs, read only access and encryption controls are used within the network infrastructure and on the workstations of individuals working in IBM data centers or with client data in IBM's data centers to help lessen the likelihood of the propagation and execution of computer viruses and other forms of known harmful code. IBM uses over-the-network encryption via standard SSL (https) connections and the IBM infrastructure employs technology solutions for end-to-end security, including firewall, intrusion prevention, and anti-malware technologies. Transmission Control Protocols/Internet Protocols (TCP/IP) vulnerability scanning is periodically conducted by authorized administrators to detect and resolve potential system security exposures. IBM warehouse data is copied to secondary storage in the IBM data center, and tertiary archival (tape) is encrypted and duplicated for storage at a 3rd party offsite disaster recovery facility.

2.4 Activity Logging

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. IBM maintains logs for recording i) successful and unsuccessful logon access attempts ii) successful and unsuccessful attempts

to gain access to the infrastructure from an external location, iii) update access attempts to OSRs and iv) activities performed using system or security administrative authority.

2.5 Physical Security

IBM restricts access to only IBM data center authorized personnel in IBM and IBM third party provided data centers. The IBM Cloud Service environment includes multi-factor authentication for physical access, involving a unique code and biometric scan, as well as 24 x 7 security personnel, manned security, and video surveillance. IBM prohibits unauthorized viewing, copying, alteration or removal of any media containing client data. Removable media on which client data are stored (including thumb drives, CDs, and DVDs) are encrypted using at least 256 bit AES (or equivalent). IBM issued laptops and workstations require implementation of whole disk encryption (PGP) where access privileges to sensitive or client data may be required. IBM destroys removable media and any mobile device (such as discs, USB drives, DVDs, back-up tapes, printers, and laptops) containing client data, or renders client data on such physical media unintelligible and not capable of reconstruction by any technical means prior to any reuse of the media. IBM shreds paper waste and disposes of it in a secure and confidential manner so as to render such paper waste unreadable.

2.6 Compliance

IBM certifies its privacy practices annually as consistent with the U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement. Industry standard audit SSAE 16 type (formerly SAS 70), or equivalent, is performed annually in our production data centers. IBM reviews security and privacy-related activities for compliance with IBM's business requirements. Assessments and audits are conducted regularly by IBM to confirm compliance with its information security policies. Security policies in place provide for security audits, the periodic application of security patches and password management and control. Workforce security education and awareness training is completed by IBM's employees and vendor employees on an annual basis. Personnel are reminded of their job objectives and their responsibility to meet ethical business conduct, confidentiality and IBM's security obligations on an annual basis.

3. Service Level Objectives

IBM endeavors to make the IBM SaaS available to Customer with an availability rate of 99%. The SLO is not a contractual commitment but rather a set of goals that IBM's Customer Support team strives to meet or exceed through its process, technology and people.

4. Entitlement and Billing Information

4.1 Charge Metrics

The Cloud Service is made available under one of the following charge metrics as specified in the Order Document:

a. Million Server Calls (MSCs) is a unit of measure by which the Cloud Service can be obtained. A Server Call is data passed to and processed by the Cloud Service as a result of a tagged event, initiated by a tracked visitor for one Entity ID. A Server Call processed by different Entity IDs will be counted as a unique Server Call for each unique Entity ID. An Entity ID separates and/or controls access rights to data in the Cloud Service which may encompass processed data from one or more of your web sites. Each MSC entitlement represents one Million Server Calls. Sufficient Million Server Call entitlements must be obtained to cover the number of Server Calls processed during the measurement period specified in the Order Document.

4.2 Charges and Billing

The amount payable for the Cloud Service is specified in the Order Document.

5. Term and Renewal Options

5.1 Term

The term of the Cloud Service begins on the date that IBM notifies you that you have access to the Cloud Service as described in the Order Document. The PoE portion of the Order Document will confirm the exact date of the start and end of the term. You are permitted to increase your level of use of the Cloud Service during the term by contacting IBM or an IBM Business Partner. We will confirm the increased level of usage in the Order Document.

5.2 Cloud Services Term Renewal Options

Your Order Document will set forth whether the Cloud Service will renew at the end of the term, by designating the term as one of the following:

5.2.1 Automatic Renewal

If your Order Document states that your renewal is automatic, you may terminate the expiring Cloud Service term by written request, at least ninety (90) days prior to the expiration date of the term that is set forth in the Order Document. If IBM or your IBM Business Partner does not receive such termination notice by the expiration date, the expiring term will be automatically renewed for either a one year term or the same duration as the original term as set forth in the PoE.

5.2.2 Continuous Billing

When the Order Document states that your billing is continuous, you will continue to have access to the Cloud Service and will be billed for the usage of the Cloud Service on a continuous basis. To discontinue use of the Cloud Service and stop the continuous billing process, you must provide IBM or your IBM Business Partner with ninety (90) days written notice requesting that your Cloud Service be cancelled. Upon cancellation of your access, you will be billed for any outstanding access charges through the month in which the cancellation took effect.

5.2.3 Renewal Required

When the Order Document states that your renewal type is “terminate”, the Cloud Service will terminate at the end of the term and your access to the Cloud Service will be removed. To continue to use of the Cloud Service beyond the end date, you must place an order with your IBM sales representative or IBM Business Partner to purchase a new subscription term.

6. Technical Support

Technical support is provided for the IBM SaaS offering and Enabling Software, as applicable, during the Subscription Period. Such technical support is included with the IBM SaaS and is not available as a separate offering.

Technical Support information can be found at the following URL: http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf

7. Enabling Software

a. This Cloud Service offering may include enabling software. You may use the enabling software only in association with your use of the Cloud Service, for the length of the term of the Cloud Service. To the extent that the enabling software contains sample code, you have the additional right to make derivative works of the sample code and use them consistent with this grant. The enabling software is provided subject to the SLA, if any, as a component of the Cloud Service, but is otherwise provided “AS IS”.

8. Additional Information

8.1 Entitlement Details

The subscription fee for IBM Digital Data Exchange includes the following:

a. You will be provided with a single instance of IBM Digital Data Exchange.

b. Standard enablement of up to five (5) hours of remotely delivered implementation services for your initial onboarding to IBM Digital Data Exchange. Services expire 90 days from date you are notified by IBM that their access to the Cloud Service is available regardless of whether all hours have been used.

8.2 Privacy Notice and Policy

You agree to (i) provide a clear and conspicuous link to your website terms of use and privacy policy which includes a link to IBM’s (http://www.ibm.com/software/marketing-solutions/privacy/index.html) and your data collection and use practices; (ii) provide notice that cookies and clear gifs/web beacons are being placed on the visitor's computer by IBM working on your behalf along with an explanation of the purpose and utilization of such technology; and (iii) to the extent required by law, obtain consent from website visitors prior to the placement of cookies and clear gifs/web beacons placed by you or IBM on your behalf on website visitor’s devices.

You are aware and agree that IBM may, as part of the normal operation and support of the Cloud Services, collect personal information from you (your employees and contractors) related to the use of the Cloud Services, through tracking and other technologies. IBM does so to gather usage statistics and information about effectiveness of our Cloud Services for the purpose of improving user experience and/or tailoring interactions with you. You confirm that you will obtain or have obtained consent to allow IBM to process the collected personal information for the above purpose within IBM, other IBM companies and their subcontractors, wherever we and our subcontractors do business, in compliance

with applicable law. IBM will comply with requests from your employees and contractors to access, update, correct or delete their collected personal information.

8.3 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) you identify as receiving benefit of the Cloud Services. IBM will apply taxes based upon the business address listed when ordering a Cloud Service as the primary benefit location unless you provide additional information to IBM. You are responsible for keeping such information current and providing any changes to IBM.