IBM Cloud Services Agreement

IBM Cloud Services Description: IBM WebSphere Cast Iron Live

The following is the Service Description for your Order:

1. **Cloud Service Description** for the following Cloud Service offerings that you may order. The offerings that you have ordered are specified in your Order Document. For the purpose of this Cloud Service, the Order Document will consist of the Quotation that IBM presents to you and the Proof of Entitlement (PoE) that you will receive from IBM confirming that the Cloud Service has been provisioned and setting forth the beginning and end date for the term of the Cloud Service.

   **A. IBM WebSphere Cast Iron Live**

   IBM WebSphere Cast Iron Live is a multi-tenant, cloud-based platform that provides tools and resources to integrate cloud and on-premise applications. Clients may choose from any supported cloud and on-premise applications.

   Standard Edition allows clients to configure, run, and manage certain common application integrations, including connectivity to cloud and supported standard on-premise applications, data synchronization and data migration scenarios. Standard Edition includes the ability to connect two applications, with an option to acquire additional application endpoints. Application Endpoints adds the authorization to integrate additional applications. Unrestricted Application Endpoints includes the authorization to integrate applications without a cap. Development Edition provides a complete, shared development environment for nonproduction use, and includes the authorization to integrate applications in the development environment without a cap.

   - IBM WebSphere Cast Iron Live Standard Edition with 2 Application Endpoints
   - IBM WebSphere Cast Iron Live Standard Edition Application Endpoints
   - IBM WebSphere Cast Iron Live Standard Edition Unrestricted Application Endpoints
   - IBM WebSphere Cast Iron Live Standard Development Edition

   Enterprise Edition includes everything in the Standard Edition, plus advanced capabilities, including the ability to connect supported enterprise on-premise applications, perform user interface mashups, use data quality features, develop reusable templates, and manage and monitor the solution remotely through management application programming interfaces (APIs). Enterprise Edition includes the same variations as described above for Standard Edition.

   - IBM WebSphere Cast Iron Live Enterprise Edition with 2 Application Endpoints
   - IBM WebSphere Cast Iron Live Enterprise Edition Application Endpoints
   - IBM WebSphere Cast Iron Live Enterprise Edition Unrestricted Application Endpoints
   - IBM WebSphere Cast Iron Live Enterprise Development Edition

   **B. IBM WebSphere Cast Iron Express**

   IBM WebSphere Cast Iron Express is a cloud-based platform that provides tools and resources to integrate information from supported Software as a Service (“SaaS”) applications with other data sources. Express Edition includes the ability to connect two applications, with an option to acquire additional application endpoints. Application Endpoints adds the authorization to integrate additional applications.

   - IBM WebSphere Cast Iron Express Edition with 2 Application Endpoints
   - IBM WebSphere Cast Iron Express Application Endpoints

2. **Security Description.** IBM implements and maintains the practices and procedures described in this section.

   **A. Security Policies**

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

B. Access Control
Access to client data is allowed only by authorized IBM support representatives according to principles of segregation duties. IBM support staff use authentication to an intermediate "gateway" management host. All connections use encrypted channels when accessing client data. All access to client data and transfer of data into or out of the hosting environment is logged. There is no usage of WIFI within the IBM data centers that support the Cloud Service.

C. Service Integrity & Availability
Modifications to operating system resources and application software are governed by IBM’s change management process. Changes to firewall rules are also governed by the change management process and are separately reviewed by the IBM security staff before implementation. IBM data resources are monitored through automatic alerts and by IBM staff. Internal and external vulnerability scanning is regularly conducted by authorized administrators or third party vendors to help detect and resolve potential system security exposures. Malware detection (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) systems are in place throughout all IBM data centers. IBM’s data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

D. 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. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time to central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to look for anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

E. Physical Security
IBM maintains physical security standards designed to restrict unauthorized physical access to data center resources. Only limited access points exist into the IBM data centers, which are controlled by two-factor authentication and monitored by surveillance cameras. Access is allowed only to authorized staff who have approved access. Operations staff verifies the approval and issues an access badge granting the necessary access. Employees issued such badges must surrender other access badges and can only possess the data center access badge for the duration of their activity. Usage of badges is logged. Non-IBM visitors are registered upon entering on premises and are escorted when they are on the premises. Physical protection measures against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster are applied. Delivery areas and loading docks and other points where unauthorized persons may enter the premises are controlled and isolated. Entry and removal of equipment is logged.

F. Compliance
IBM reviews its privacy practices annually to confirm that they are 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 SAS 70 Type II now SSAE 16, or equivalent is performed annually in our production data centers. IBM’s team reviews security and privacy-related activities for compliance with IBM’s business activities. The Cloud Service is not designed to comply with HIPAA and may not be used for the transmission or storage of any Personal Health Information. Assessments and audits are conducted regularly by IBM’s team to confirm compliance with its information security policies. 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 Commitment. IBM provides the following service level commitment (“SLA”) for the Cloud Service. The component to which the SLA applies will be known as the “Service” throughout this section that describes the SLA.
A. Definitions
i. "Authorized Contact" means the individual you have specified to IBM who is authorized to submit Claims under this SLA.

ii. "Availability Credit" means the remedy IBM will provide for a validated Claim. The Availability Credit will be applied in the form of a credit or discount against a future invoice of subscription charges for the Service.

iii. "Claim" means a claim submitted by your Authorized Contact to IBM pursuant to this SLA that a Service Level has not been met during a Contracted Month.

iv. "Contracted Month" means each full month during the term of the Service measured from 12:00 a.m. EST on the first day of the month through 11:59 p.m. EST on the last day of the month.

v. "Client" means an entity subscribing for the Service directly from IBM which is not in default of any material obligations, including payment obligations, under its contract with IBM for the Service.

vi. "Downtime" means a period of time during which production system processing for the Service is unavailable, as measured in sub-section C “Service Level Monitoring Methodology” below. Downtime does not include the period of time when the Service is not available as a result of:
   ● Planned System Downtime.
   ● Force Majeure.
   ● Problems with Client or third party applications, equipment or data.
   ● Client or third party acts or omissions (including anyone gaining access to the Service by means of your passwords or equipment).
   ● Failure to adhere to required system configurations and supported platforms for accessing the Service.

vii. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.

viii. "Force Majeure" means acts of God, terrorism, labor action, fire, flood, earthquake, riot, war, governmental acts, orders or restrictions, viruses, denial of service attacks and other malicious conduct, utility and network connectivity failures, or any other cause of Service unavailability that was outside IBM’s reasonable control.

ix. "Planned System Downtime" means a scheduled outage of the Service for the purpose of service maintenance.

x. "Service" means the IBM WebSphere Cast Iron Live service(s) that you have ordered as specified in the Order Document. This SLA applies to each Service individually and not in combination. This SLA does not apply to Development Edition components of the Service.

xi. "Service Level" means the standard set forth below by which IBM measures the level of service it provides in this SLA.

B. Availability Credits
i. In order to submit a Claim, you must log a Severity 1 support ticket for each Event with the IBM client support help desk, within twenty-four (24) hours of your first becoming aware that the Event has impacted your use of the Service. You must provide all necessary detailed information about the Event and reasonably assist IBM with the diagnosis and resolution of the Event.

ii. You must submit your Claim for an Availability Credit no later than three (3) business days after the end of the Contracted Month which is the subject of the Claim.

iii. Availability Credits will be based on the duration of Downtime measured from the time you report that you were first impacted by the Downtime. For each valid Claim, IBM will apply the highest applicable Availability Credit based on the achieved Service Level during each Contracted Month, as shown in the
table below. IBM will not be liable for multiple Availability Credits for the same Event in the same Contracted Month.

iv. If you purchased a subscription to the Service from a valid IBM reseller in a remarketing transaction in which IBM maintains primary responsibility for fulfilling the Service and SLA commitments, then the Availability Credit will be based on the then-current published Relationship Suggested Value Price (RSVP) for the Service in effect for the Contracted Month which is subject to a Claim, discounted at a rate equal to the lower of (a) fifty percent (50%) and (b) for special bid sales, the special bid discount percentage.

v. The total Availability Credits awarded with respect to any Contracted Month shall not, under any circumstance, exceed 100 percent (100%) of one twelfth (1/12) of the annual charge paid by you to IBM for the Service.

C. Service Level Monitoring Methodology
The following methodology will be employed to measure the Downtime that is used in determining the Achieved Service Level:

i. IBM uses a test program that simulates an end user logging into the Service to test the availability of the web management console.

ii. IBM runs the test at approximately five (5) minute intervals.

iii. Downtime is determined as the number of minutes between the time of a failed test and the time of the next successful test.

D. Service Levels – Availability of Service during a Contracted Month

<table>
<thead>
<tr>
<th>Availability during a Contracted Month</th>
<th>Availability Credit (% of Monthly Subscription Fee for a Contracted Month which is the subject of a Claim)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;99.5%</td>
<td>10%</td>
</tr>
<tr>
<td>&lt;99.0%</td>
<td>50%</td>
</tr>
<tr>
<td>&lt;95%</td>
<td>75%</td>
</tr>
<tr>
<td>&lt;90%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Availability is calculated as: (a) the total number of minutes in a Contracted Month, minus (b) the total number of minutes of Downtime in a Contracted Month, divided by (c) the total number of minutes in a Contracted Month, with the resulting fraction expressed as a percentage.

Example: 250 minutes total Downtime during a 30 day Contracted Month.

\[
\frac{43,200 \text{ total minutes in the period} - 250 \text{ minutes Downtime}}{43,200 \text{ total minutes in a Contracted Month}} = 10\% \text{ Availability Credit for 99.4\% Achieved Service Level}
\]

D. Other information about this SLA. This SLA is made available only to IBM’s clients and does not apply to claims made by your users, guests, and participants of the Service or to any beta or trial services that IBM provides. The SLA only applies to the Services that are in production use, so it does not apply to non-production environments, including but not limited to test, disaster recovery, Q&A, or development. If you have breached any material obligations under your contract for the Service, including without limitation, breach of any payment obligations, you may not make a Claim under this SLA.
4. Entitlements, Billing, Term and Support Information

A. Charge Metrics. The Cloud Service offerings are sold in accordance with the following metric(s):

i. **Install** is a unit of measure by which the Cloud Service offering can be obtained. An entitlement must be obtained for each copy or instance of the infrastructure made available to access and use the Cloud Service offering.

ii. **Application Instance** is a unit of measure by which the Cloud Service offering can be obtained. An entitlement is required for each instance of an application connected to or managed by the Cloud Service offering. An application in a test, development, staging, or production environment is each considered to be a separate instance of the application and each must have an entitlement. Multiple application instances in a single environment are each considered separate instances of the application and each must have an entitlement.

iii. **Cumulative Entitlements**

   Install and Application Instance entitlements are not alternative means for authorizing use of the Cloud Service offering. Client must obtain Application Instance entitlements to cover Client’s application endpoints connected to the Cloud Service offering, except that two application endpoints are permitted with each Install entitlement. Client must obtain either sufficient Application Instance entitlements to cover all Client application endpoints greater than two that connect to the Cloud Service offering or an entitlement to Unrestricted Application Endpoints for the relevant Installs. If the Cloud Service offering is designated as a “Development Edition”, Client is authorized to connect an unrestricted number of application endpoints to the Cloud Service Offering.

B. Charges & Billing

i. **Billing Options.** The amount payable for this offering is specified in the Cloud Services Order Document as follows:

   a) Entire commitment amount upfront
   b) Monthly (in arrears)
   c) Quarterly (upfront)
   d) Annually (upfront)

   The selected billing option will be valid for the length of the term as specified in the Order Document. The amount payable per billing cycle will be based on the annual subscription fee and number of billing cycles in a year plus any overage charges.

   
   ii. **Partial Month Charges.** The Partial Month charge is a pro-rated daily rate that will be charged to Client. The Partial Month Charges are calculated based on the remaining days of the partial month starting on the date Client is notified by IBM that their access to the Cloud Service offering is available.

   
   iii. **Overages.** If your actual usage of the Cloud Service during the measurement period exceeds the entitlement stated on the POE portion of the Order Document, then you will be invoiced for the overage, as set forth in the Order Document.

C. Term and Renewal Options

i. **Term.** The term of the Cloud Service will begin on the date that IBM notifies you that you have access to the portions of the Cloud Service that are 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, as well as how or whether the term will renew. 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 include that change in an Order Document.

   
   ii. **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:

   a. **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 an 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 portion of the Order Document.
b. **Continuous Billing.** When the Order Document notes 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 billing basis. To discontinue use of the Cloud Service and stop the continuous billing process, you will need to provide IBM or an 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.

c. **Renewal Required.** When the Order Document notes 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 the Cloud Service beyond the end date, you will need to place an order with your IBM sales representative or IBM Business Partner to purchase a new subscription term.

D. **Technical Support**

Technical support is provided during the subscription period. Technical Support does not include assistance for 1) the design and development of applications, 2) Client use of the Cloud Service offering in other than the specified operating environment, or 3) failures caused by products and services for which IBM is not responsible under the Agreement.

While Technical Support is in effect:

1. IBM provides Client assistance for your routine, short duration installation and usage (how-to) questions as well as code-related questions (“Support”).
2. IBM provides assistance via telephone and, if available, electronic access, only to Client’s information systems (IS) technical support personnel during the normal business hours (published prime shift hours) of Client’s IBM support center. (This assistance is not available to your end users.) IBM provides Severity 1 assistance 24 hours a day, every day of the year.
3. IBM may request that you allow it to access Client’s system to assist in isolating the problem cause. Client remains responsible for adequately protecting your system and all data contained in it whenever IBM accesses it with your permission.

5. **Safe Harbor.** IBM has not determined compliance of this Cloud Service with the US-EU and US-Swiss Safe Harbor Frameworks.

6. **Prohibited Components**

Notwithstanding any information to the contrary, if the Cloud Service offering is designated as a “Standard Edition”, Client is not authorized to use any of the following components or functions of the Cloud Service offering:

1. Enterprise Application Endpoints
2. Data Quality Features
3. Template Development Kit
4. Management APIs

7. **Optional Components.** The following optional components may be used with the Cloud Service if desired and are available separately as described below:

A. **IBM WebSphere Cast Iron Live: Secure Connector (“Secure Connector”).**

Secure Connector is an optional component that provides security around the transfer of data between the Cloud Service and an endpoint located behind a firewall and can be downloaded and licensed here: http://pic.dhe.ibm.com/infocenter/wci/v6r1m0/index.jsp?topic=%2Fcom.ibm.websphere.cast_iron.live.doc%2FSecure_Connector%2Fdownloading_secure_connector_configuration_files.htm

B. **IBM WebSphere Cast Iron Live: Integration Studio (“Integration Studio”).**

Integration Studio is an optional component that enables a user to design and test integration projects offline and then publish them to the Cloud Service and can be downloaded and licensed here: https://www-947.ibm.com/support/entry/myportal/support