IBM Case Manager on Cloud

This Service Description describes the Cloud Service IBM provides to Client. Client means the company 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 Case Manager on Cloud provides:

a. IBM Content Navigator to access advanced case management applications;

b. Content-centric Case Management, enabling knowledge workers or business analysts to:
   1. utilize Case Builder to quickly and easily design and try out new case solutions;
   2. use sample solution templates provided;
   3. create and maintain case properties, user roles, in-boxes, document types, page and data visual layouts;
   4. employ embedded business rules which allows for easier development within the Case Manager Builder environment;
   5. create case tasks and their underlying workflows;
   6. utilize the Case Client runtime to display the solutions created by Case Builder;
   7. access the Content Navigator based UI provided;
   8. access to the Case Administrator for deploying and managing solutions;
   9. access to Case Monitor and Case Analyzer to provide current and historical reporting on cases;
   10. access provided APIs to extend solutions;
   11. have access to full, unrestricted use of Case Foundation to provide active content and case workflow management;
   12. have access to full, unrestricted use of FileNet Content Manager and its ECM repository;

c. A secure, virtual private infrastructure

d. Replication of production data to a secondary location in support of disaster recovery

e. Up to 4 TB of outbound bandwidth; higher bandwidth quoted separately

f. 24x7 production environment monitoring, data encryption in transit and at rest, virus scanning, intrusion detection / penetration testing services, software patches, and software upgrades (data migration services or activities required for custom configurations or extensions quoted separately).

g. Active Directory Integration

Included Options: (Microsoft Active Directory or IBM Tivoli Directory Server)

1. Authentication to the Cloud Service LDAP Server replicating back to on-premise Client LDAP
   a. Provide a (Read Only) domain controller in the Cloud Service that is in the Client domain
   b. Client manages all end user access to the cloud environment (groups, IDs, access)
   c. Full Admin rights to Client

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

3. Point to on-premise Client domain controller for authentication
   a. Possible performance implications
   b. Authenticated for the life of the session

Other configurations (e.g. manual or scripted excerpts of LDAP file directory to the Cloud Service; federation options including SAML, MS Federation Services, or others) quoted separately.
Custom solution implementation, configuration, and integration services are available for an additional charge under a statement of work.

Software upgrades as part of the service are included. Upgrades requiring migration of data or any custom extensions are not included.

Client must purchase a subscription to a base Cloud Service offering as defined below.

### 1.2 Base Services Offering Entitlement

Each base offering represents capacity to process certain amount of data volume and user operations 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 usage.

#### 1.2.1 IBM Case Manager Bronze 2.0

- Bronze configuration is intended to support up to 30,000 new cases per year. This type of deployment typically will support ingesting and storing up to 500 case artifact documents per day and up to 50 knowledge workers concurrently working and completing as many as 200 cases per day.
- Bronze configuration provides 1TB of Storage; additional storage entitlement can be separately purchased.

#### 1.2.2 IBM Case Manager Silver 2.0

- Silver configuration is intended to support up to 300,000 new cases per year. This type of deployment typically will support ingesting and storing up to 20,000 case artifact documents per day and up to 250 knowledge workers concurrently working and completing as many as 1,000 cases per day.
- Silver configuration provides 1TB of Storage; additional storage entitlement can be separately purchased.

#### 1.2.3 IBM Case Manager Gold 2.0

- Gold configuration is intended to support up to 750,000 new cases per year. This type of deployment typically will support ingesting and storing up to 50,000 case artifact documents per day and up to 1,000 knowledge workers concurrently working and completing as many as 2,500 cases per day.
- Gold configuration provides 3TB of Storage; additional storage entitlement can be separately purchased.

#### 1.2.4 IBM Case Manager Platinum 2.0

- Platinum configuration is intended to support up to 3,000,000 new cases per year. This type of deployment typically will support ingesting and storing up to 200,000 case artifact documents per day and 5,000 knowledge workers actively working and completing as many as 10,000 cases per day.
- Platinum configuration provides 5TB of Storage; additional storage entitlement can be separately purchased.

### 1.3 Optional Entitlements

#### 1.3.1 IBM Case Manager Storage Add-On 2.0

If Client exceeds the TB storage included with the selected configuration, Client must purchase additional entitlement.

#### 1.3.2 IBM Case Manager Non-Production Environment 2.0

Client may purchase a separate instance for test and development purposes. This development environment may not be used for production purposes.

a. The non-production environment configuration is sized the same as the Bronze configuration
b. The non-production environment does not provide high availability or disaster recovery

#### 1.3.3 IBM Case Manager Dedicated Add-On 2.0

a. Client may upgrade a selected virtual private environment to a single tenant private infrastructure. This includes up to 20 TB of outbound bandwidth; higher bandwidth quoted separately
2. **Security**
This Cloud Service follows IBM’s data security and privacy principles for IBM SaaS, which are available at [https://www.ibm.com/cloud/resourcecenter/content/80](https://www.ibm.com/cloud/resourcecenter/content/80) and any additional terms provided in this section.

Any change to IBM’s data security and privacy principals will not degrade the security of the Cloud Service.

All data is protected using FIPS 1402 level 1 compliant whole disk encryption. The data classification for this solution defaults to data being classified as Client sensitive. IBM will work with the Client to address other regulatory requirements (such as HIPPA, PIPEDA, FFIEC, PCI, etc.) when requested by the Client for the intended workload, and may impact the solution architecture and charges.

3. **Service Level Agreements**
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 of an event that has impacted the Cloud Service availability. 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 three 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 refers to complete system unavailability, not individual or specific components of the total solution. 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 50 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

<table>
<thead>
<tr>
<th>Availability during a contracted month</th>
<th>Service Credit (% of monthly subscription fee* for contracted month that is the subject of a claim)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;99%</td>
<td>5%</td>
</tr>
<tr>
<td>&lt;97%</td>
<td>10%</td>
</tr>
<tr>
<td>&lt;95%</td>
<td>25%</td>
</tr>
<tr>
<td>&lt;90%</td>
<td>50%</td>
</tr>
</tbody>
</table>

* 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.

Example: 440 minutes total Downtime during contracted month

\[
\frac{43,200 \text{ total minutes in a 30 day contracted month}}{ \text{440 total minutes during Downtime}} = 5\% \text{ Availability credit for }
\]
4. Business Continuity
The Cloud Service is configured to support business continuity objectives defined below. Business continuity objectives help ensure that an organization's critical business functions will be recovered to an operational state, with a minimal loss of data, within a reasonably short period following a disaster at the primary computing location. Once a determination is made that an incident at the primary computing location warrants a failover to the secondary location, business continuity plans and related activities shall be executed by IBM in support of the recovery objectives noted below. For this Cloud Service the non-production environment will be refreshed and reconfigured to accept production workloads until service at the primary location is restored.

<table>
<thead>
<tr>
<th>Business Continuity Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Point Objective</td>
</tr>
</tbody>
</table>
| Recovery Time Objective       | ● 4 consecutive hours when a secondary, equivalent Base Service Entitlement is purchased  
                                ● At least 24 consecutive hours, if no secondary Base Service entitlement is purchased |

5. Technical Support
Technical support for the Cloud Service is provided via an online problem reporting system. Technical support is offered with the Cloud Service and is not available as a separate offering.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Severity Definition</th>
<th>Response Time Objectives During Support Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.</td>
<td>Within 1 hour</td>
</tr>
<tr>
<td>2</td>
<td>Significant business impact: A service feature or function is severely restricted in its use or Client is in jeopardy of missing business deadlines.</td>
<td>Within 2 business hours</td>
</tr>
<tr>
<td>3</td>
<td>Minor business impact: Indicates the service or functionality is usable and it is not presenting a critical impact on operations.</td>
<td>Within 4 business hours</td>
</tr>
<tr>
<td>4</td>
<td>Minimal business impact: An inquiry or non-technical request.</td>
<td>Within 1 business day</td>
</tr>
</tbody>
</table>

6. Entitlement and Billing Information
6.1 Charge Metrics
The Cloud Service is available under the charge metric specified in the Transaction Document:

a. Authorized User is a unit of measure by which the Cloud Service can be obtained. Client must obtain separate, dedicated entitlements for each unique Authorized User given access to the Cloud Service in any manner directly or indirectly (for example: via a multiplexing program, device, or application server) through any means. Sufficient entitlements must be obtained to cover the number of Authorized Users given access to the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.

b. 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
6.2 **Partial Month Charges**
A partial month charge as specified in the Transaction Document may be assessed on a pro-rated basis.

7. **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. 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.

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.

8. **General**

8.1 **External User Access**
Client may choose to give external users access to the Cloud Service. Client is responsible for these external users, including but not limited to a) any claims made by the external users relating to the Cloud Service, or b) any misuses of the Cloud Service by these external users.

8.2 **Virtual Private Network (VPN)**
Client may select to utilize a software VPN connection for the purpose of securely connecting to the Cloud Service. Information about the VPN will be provided upon written request by Client.

8.3 **Links to Third Party Websites or Other Services**
If Client or an Cloud Service User transmits content to a third party website or other service that is linked to or made available by the Cloud Service, Client and the IBM User provide IBM with the consent to enable any such transmission of Content, but such interaction is solely between Client and the third party website or service. IBM makes no warranties or representations about such third party sites or services, and shall have no liability for such third party sites or services.

8.4 **Cookies**
Client is aware and agrees that IBM may, as part of the normal operation and support of the Cloud Service, collect personal information from Client (your employees and contractors) related to the use of the Cloud Service, through tracking and other technologies. IBM does so to gather usage statistics and information about effectiveness of our Cloud Service for the purpose of improving user experience and/or tailoring interactions with Client. Client confirms that it 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 Client’s employees and contractors to access, update, correct or delete their collected personal information.