



IBM Cloud Services Agreement

IBM Cloud Service Description: IBM Emptoris Managed Cloud Delivery

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. Managed Cloud Delivery Services

You will receive Managed Cloud Delivery Services in connection with the operation and use of, and access to the software you have licensed, including production servers, production storage, and a connection between the production server(s) and the Internet. We may also provide an optional non-production application platform (as described below). We will integrate, set-up and configure the equipment necessary to provide the Managed Cloud Delivery Services for the licensed software described in your Order Document. Managed Cloud Delivery Services do not include data migration, which will be performed on a quoted time and materials basis, if and when requested. Further, we will provide and maintain all necessary hardware and software, telecommunications hardware and software, security software and other software that is reasonably necessary to operate and maintain the Managed Cloud Delivery Services. Authorized Users will be able to access the software at the internet uniform resource locator as published by using a computer equipped with an internet connection and a modern web browser, the specifications to be determined at the time the managed application is initiated.

B. Non-Production Application Platform

Non-production application platform is an application deployment distinct from the production application platform. The non-production application platform may be located at a different facility than the production application platform at our discretion. The non-production application platform is primarily intended for use as a platform for testing, staging, training or QA, at your discretion.

C. Disaster Recovery Services

We provide backup and recovery services for all production application platforms. In the event of an interruption of service of the production application platform caused by a declared disaster pursuant to our policies for business continuity and disaster recovery, we will endeavor to recover your data in accordance with the time periods set forth in the Service Level Objectives below and dependent upon the level of service for which you have subscribed. We may utilize the non-production application platform (if any) resources for application and data recovery and thus that system may become unavailable until the resolution of the disaster.

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 reviewed and 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 of duties. IBM support staff use two-factor authentication to an intermediate "gateway" management host. All connections are 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 IBM Emptoris data centers. Access control logs are audited regularly. Termination and employment change procedures are in place and include return of assets and access right removal.

C. Service Integrity and 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 center resources are monitored and maintained 24x7 by IBM staff. 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. IBM data center resources also include redundant and back-up power supplies.

Internal and external vulnerability scanning is regularly conducted by authorized administrators and third party vendors to help detect and resolve potential system security exposures including ingress and egress filtering on core routers to guard against address spoofing; use of private IP address space to shield core infrastructure components from the Internet system patching procedures; use of virtual IP addresses to mask hosts; and use of load balancers to buffer connection requests. Malware detection (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) systems are in place throughout all IBM data centers.

D. Activity Logging

Where technically available, for systems, applications, data repositories, middleware and network infrastructure devices, IBM's team maintains logs of its 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

Industry standard audit 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. 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. Subject to confidentiality restrictions and upon request we will provide reasonable access to the results of previously performed security audits.

G. Managed Application Infrastructure

- i. **Data Storage.** Disk storage is implemented with a RAID or equivalent storage system. Back-ups are currently performed after initial installation and daily thereafter. Database restoration tests run quarterly.
- ii. **Monitoring.** We provide the following monitoring services: a) Fault monitoring – detection of and alerts for distributed exceptions, including hardware and/or software failure and; b) Performance monitoring – detection of and alerts for response time degradation caused by application-level problems, hardware utilization and/or network congestion.

3. **Service Level Commitment.** The production application platform will have ninety-nine percent (99%) availability, twenty-four (24) hours per day, seven (7) days per week as more fully set forth in the service level commitment (“SLA”) for this Cloud Service offering set forth below:

A. Definitions

- i. "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.
- ii. "Claim" means a claim submitted by you to IBM pursuant to the SLA that a Service Level has not been met during a Contracted Month.
- iii. "Contracted Month" means each full month during the term of the Service measured from 12:00 a.m. Eastern US time on the first day of the month through 11:59 p.m. Eastern US time on the last day of the month.
- iv. "Downtime" means a period of time during which production system processing for the Service has stopped and all of your users are unable to use all aspects of the Service for which they have appropriate permissions. Downtime does not include the period of time when the Service is not available as a result of:
 - A scheduled outage for the purpose of service maintenance.
 - Events or causes beyond IBM's control (eg., natural disaster, internet outages, etc.).
 - Problems with Client or third party applications, equipment or data.
 - Failure to adhere to required system configurations and supported platforms for accessing the Service.
 - IBM's compliance with any designs, specifications, or instructions provided by Client or a third party on Client's behalf.
- v. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.
- vi. "Service" means the IBM Emptoris service(s) to which the SLA applies. The SLA applies to each Service individually and not in combination.
- vii. "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 that is the subject of the Claim.
- iii. Availability Credits will be based on the duration of the 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. For Bundled Services (individual Services packaged and sold together for a single combined price), the Availability Credit will be calculated based on the single combined monthly price for the Bundled Service, and not the monthly subscription fee for each individual Service. You may only submit Claims relating to one individual Service in a bundle in any Contracted Month, and IBM will not be liable for Availability Credits with respect to more than one Service in a bundle in any Contracted Month.

- v. The total Availability Credits awarded with respect to any Contracted Month shall not, under any circumstance, exceed 10 percent (10%) of one twelfth (1/12th) of the annual charge paid by you to IBM for the Service.

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

Availability during a Contracted Month	Availability Credit (% of Monthly Subscription Fee for Contracted Month that is the subject of a Claim)
<99.0%	2%
<97.0%	5%
<95.0%	10%

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

Example: 500 minutes total non-scheduled Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month - 200 minutes of planned system Downtime - 500 minutes Downtime = 42,500 minutes <hr style="width: 50%; margin-left: 0;"/> 43,200 total minutes (-200 minutes of planned system Downtime) in a 30 day Contracted Month =43,000 minutes	= 2% Availability Credit for 98.8% achieved Service Level
---	--

D. Disaster Recovery Service Level Objectives (Credits do not apply)

- i. For clients with both production and non-production environments:
 Disaster Recovery Time Objective: Maximum 3 Business Days
 Recovery Point Objective: 24 hours
- ii. For clients without a non-production environment:
 Disaster Recovery Time Objective: 10 Business Days
 Recovery Point Objective: 7 calendar days

E. 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 production Services, so it does not apply to non-production environments, including but not limited to test, disaster recovery, Q&A, or development. The SLA does not apply if Client has exceeded the number of Concurrent Users for which the system has been configured (as defined below). 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. Entitlement, Billing, Term and Support Information.

A. Charge Metrics

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

- i. **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 the Order Document.

- ii. **Connection** is a unit of measure by which the Cloud Service can be obtained. A Connection is a link or association of a database, application, server, or any other type of device to the Cloud Service. Sufficient entitlements must be obtained to cover the total number of Connections which have been or are made to the Cloud Service during the measurement period specified in client's Proof of Entitlement (PoE) or Transaction Document.

B. Charges and Billing

- i. **Billing Options.** The amount payable for the Cloud Service offerings are specified in the 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 monthly or 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 you. The Partial Month Charges are calculated based on the remaining days of the partial month starting on the date you are notified by IBM that your 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.
- iv. **On-Demand** options will be invoiced in the month the on-demand option is ordered by you at the rate set forth in the Order Document.
- v. **Set-up** charges will be specified in an 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.

5. Additional Information

A. Associated IBM Programs

The IBM Emptoris Managed Cloud Delivery services do not include subscription and support for the associated IBM program. Client represents that Client has acquired the applicable (1) license entitlements and (2) subscription and support for the IBM program. During the subscription period of the Cloud Service, to receive subscription and support for the IBM programs, Client will need to maintain current subscription and support for the IBM programs.

B. Additional Services

i. Application Upgrades

IBM will install and configure software upgrades to the production or non-production environments at a mutually agreed time, subject to scheduling availability, during normal business hours Mon 3AM GMT to Friday 11:59 PM, excluding holidays.

ii. Database Refreshes

IBM will replicate production database contents to your non-production environment once per quarter, for each non-production system purchased. Refresh services will be performed at a mutually agreed time, subject to scheduling availability, during normal business hours Mon 3AM GMT to Friday 11:59 PM, excluding holidays.

iii. Content Storage

IBM Managed Cloud Delivery services includes storage for customer data and storage capacity for associated data backups. Content capacity per application is 100GB for attachments, and 200GB for database.

iv. Backup Retention

IBM will retain a backup copy of Client's data for a maximum period of 90 days.

v. Return of Content

After termination of the service, and within 30 days of effective termination, IBM will provide an electronic copy of Client content in the native application format.

C. Security Scanning

Client has the right to perform security testing on the application(s) provided in the service. Such testing can be performed at a mutually agreed time, and only in accordance with the IBM Emptoris Managed Cloud Client Scan Agreement.

D. IBM Emptoris Sourcing Managed Cloud Delivery User Volume Performance

The infrastructure for IBM Emptoris Sourcing Managed Cloud Delivery offering has been configured to support:

- a. 300 Concurrent Users running RFP, RFI, RFQ or buyer survey events or
- b. 270 Concurrent Users running English reverse and English forward auctions or
- c. 60 Concurrent Users running Japanese or Dutch reverse or forward auctions.

Concurrent Users are defined as users who are logged onto and active in the system concurrently. The system may be configured to process additional volume of Concurrent Users depending upon various factors. Additional infrastructure resources may be required to support larger usage volumes.

E. Restriction for Emptoris Sourcing Managed Cloud Delivery and Emptoris Sourcing Managed Cloud Delivery Burst Mode

If Client utilizes the Official Journal of the European Union (OJEU) feature where the sourcing system transmits data to the Tenders Electronic Daily (TED) site, the Client is responsible for applying to the OJEU and passing the GAMMA testing. The data transmission is solely between the Client and this third party site. 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.