

IBM Cloud Service Description: IBM Intelligent Operations Center on IBM SmartCloud

The following is the Service Description for your Order:

1. Cloud Service

The Cloud Service offerings that you may order, including the base offering and available optional features are 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 confirming the start date and term of the Cloud Services and when invoicing will commence.

1.1 IBM Intelligent Operations Center Standard User on IBM SmartCloud

Standard users have the following capabilities:

- Intelligent Operations Center (IOC) console – main interface that allows user to view events and event status, geo-spatial information (this requires integration to a GIS service, which is not provided with the IBM Cloud Service), and view reports for historic trend analysis, optimizing resource deployment and on Key Performance Indicators chosen by the user (KPIs)
- Allows users to view results from analytics based on time and location of events or other data processed by the IBM Cloud Services on a map
- Allows users to pull up events based on data processed by the IBM Cloud Service
- Allows users to view reports about events or data captured in the IOC console
- Provides Standard Operating Procedure templates that can be customized by users for emergency response events
- Allows users to execute Standard Operating Procedures that can help automate a standard response to an event, KPI threshold, or condition defined in a report
- Allow users to have an “at-a-glance” summary of information across all events in a city

1.2 IBM Intelligent Operations Center Premium User on IBM SmartCloud

Premium users have access to all IBM Intelligent Operations Center Standard User on IBM SmartCloud capabilities as stated above as well the following additional capabilities:

- Allow users to create and modify KPIs and reports
- Allow users to create and modify Standard Operating Procedures, including templates for emergency response
- Allow users to administer the IBM Cloud Service via administrative interfaces
- Allow users to import data from your system or third parties' systems via integration APIs
- Allow users to configure analytics that identify correlations, based on time and location, of city events
- Allow users to define and manage interfaces, as well as configure reports, in the Citizens Collaboration Portal (defined below)
- Allows users to submit services requests to add users to the system, change user configurations, and add new screens to the user interface.

1.3 IBM Intelligent Operations Center Consumer User on IBM SmartCloud

Consumer Users may use the Citizen Collaboration Portal, which is a specialized interface that allows external, public access to the IBM Cloud Service by Consumer Users. Consumer Users have the ability to submit service requests, view the status of their request, as well as view any reports via the Citizen Collaboration Portal. Consumer Users do not have any access to any IBM Intelligent Operations Center Standard User on IBM SmartCloud or IBM Intelligent Operations Center Premium User on IBM SmartCloud capabilities.

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 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 an incident response procedure.

2.2 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 IOC 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.

2.3 Service Integrity and Availability

Modifications to operating system resources (OSRs) and application software are governed by IBM's change management process. Changes to firewall rules are governed by the change management process and are separately reviewed by the IBM security staff before implementation. IBM data center resources are monitored 24x7 by IBM staff. Internal and external vulnerability scanning is regularly conducted by authorized administrators and 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 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.

2.4 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.

2.5 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 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.

2.6 Compliance

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. 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.

3. Service Level Objective

The service level objectives for this Cloud Service are:

- 99.5% availability outside of regularly scheduled maintenance windows.
- Maximum 5 second response time indicating web page activity is occurring.

Service level objectives are a goal and do not constitute a warranty to Customer. There is no refund, credit, or other remedy available to Customer in the event IBM does not meet the service level objectives.

4. Entitlement and Billing Information

4.1 Charge Metrics

The IBM Cloud Services are sold in accordance with the following charge metric(s) as specified in the Order Document:

- a. Concurrent User is a unit of measure by which the Cloud Service can be obtained. A Concurrent User is a person who is accessing the Cloud Service at any particular point in time. Regardless of whether the person is simultaneously accessing the Cloud Service multiple times, the person counts only as a single Concurrent User. You must obtain entitlements for the maximum number of Concurrent Users simultaneously accessing the Cloud Service in any manner directly or indirectly (for example: via a multiplexing program, device, or application server) through any means during the measurement period specified in the PoE portion of the Order Document.

4.2 Charges and Billing

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

4.3 Partial Month Charges

The partial month charge is a pro-rated daily rate. 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.

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 term and the billing will not begin until the offering is fully provisioned, which means that any data loads and configuration are completed before end users access the Cloud Service. 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 your 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 following the end of your term 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 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 Cloud Service and enabling software, as applicable, during the term of the Cloud Service. Technical support is included with the Cloud Service and is not available as a separate offering. While technical support is in effect:

- a. IBM provides you assistance for your routine how-to questions as well as investigating any code-related functionality incidents.
- b. IBM provides you electronic problem reporting and assistance via a web-based support portal during the normal business hours (published prime shift hours) of your 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.
- c. IBM may request that you allow IBM to remotely access your system to assist you in isolating the problem cause. You remain responsible for adequately protecting your system and all data contained in it whenever IBM remotely accesses it with your permission.

Technical support does not include assistance for 1) the design and development of applications, 2) your use of the Cloud Service in other than their specified operating environment or 3) failures caused by products and services for which IBM is not responsible under this Service Description.

7. Enabling Software

This Cloud Service offering may include enabling software. You may use the enabling software only in association with your use of the Cloud Service in the manner described in the documentation, 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 Service Level Commitment, if any, as a component of the Cloud Service, but is otherwise provided "AS IS".

8. Safe Harbor Compliance

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

9. Additional Information

9.1 Data Collection

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 to improve user experience and/or tailor 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..

9.2 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.