IBM Cloud Service Description: IBM Sterling B2B Services – File Transfer Service

The following is the Service Description for your Order:

1. Cloud Service

The Cloud Service offering including the base offering and 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 confirming the start date and term of the Cloud Services and when invoicing will commence

1.1 IBM Sterling B2B Services – File Transfer Service

IBM Sterling B2B Services – File Transfer Service is a cloud-based, business-to-business (B2B) software-as-a-service solution that provides for machine-to-machine transfers of large files with a select community of the client's trading partners. Your trading partners are organizational entities with which you have a business relationship. IBM will retain and provide on-line visibility to your data in the Cloud Service which is 0-14 days old, via browser-based visibility tools. After 14 days the data is purged. However, for the following protocols that require data to be picked up, data is only available for pick up for 7 days: FTP, SFTP, FTPS, and OFTP2, after which the data is purged. File Transfer Service also includes 1.) File Encryption consists of decrypting a file encrypted with PGP for which IBM and Customer have exchanged a key, and transmitting to either you or your trading partner as applicable; or encrypting with PGP an unencrypted file and then transmitting to either you or your trading partner as applicable. 2.) File Compression consists of decompressing a file compressed in the .zip format and then transmitting to either you or your trading partner as applicable; or compressing into the .zip format an uncompressed file and then transmitting to either you or your trading partner as applicable.

IBM will provide the solution resources of the base offering described below to plan, build, and implement the Cloud Service. This will include the following phases:

a. Service design phase is the design of the business and technical environment. IBM will provide an assessment of your current environment including review of any previously prepared architecture document along with any additional requirements gathering IBM deems necessary for initial setup of hardware systems, communications, applications interfaces, and trading partner requirements.

b. Service provisioning phase is the migration of your existing trading partner community (i.e. Entity IDs) to the Cloud Service. IBM will:

   (1) Initiate connectivity between you and the Cloud Service,

   (2) Initiate connectivity between your trading partners and the Cloud Service,

   (3) Conduct connectivity testing in accordance with IBM test plans, and

   (4) Work with you to manage the implementation of your trading partner community.

c. Operations Phase is IBM's management of the day-to-day operations of the Cloud Service. IBM will operate and manage facilities that house hardware and software related to your file transfer infrastructure within the Cloud Service.

1.2 Optional Features

1.2.1 IBM Sterling B2B Services – File Transfer Service - Extended Data Retention

IBM Sterling B2B Services – File Transfer Service - Extended Data Retention consists of storing gigabytes of data for a predetermined, extended period of time. The amount of data to be stored (as measured on the last day of each month) and the period of time that the data will be retained, are set forth in your Order Document.

1.2.2 IBM Sterling B2B Services - File Transfer Service - Partner Support

IBM Sterling B2B Services - File Transfer Service - Partner Support consists of providing support for your trading partners, which includes responding to their inquiries with respect to the Cloud Service and determining the extent of any reported failure with your trading partners' use of the Cloud Service with the intent to coordinate resolution of such failure with you. IBM will provide support to your trading partners

through e-mail or telephone. This level of support is in addition to the standard support provided for the Cloud Service.

2. Security Description

2.1 Security Policies

IBM maintains privacy and security policies that are communicated to IBM employees. IBM requires privacy and security training to personnel who support IBM data centers. We have an information security team. 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

Access to client data, if required, is allowed only by authorized IBM support representatives according to principles of segregation of duties. IBM 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. WIFI use is prohibited within IBM data centers that support this Cloud Service.

2.3 Service Integrity & Availability

Modifications to operating systems 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 reviewed by the IBM security staff before implementation. IBM monitors the data center 24x7. 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 used in 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.

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. 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 detect 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 IBM data centers. Only limited access points exist into the data centers, which are controlled by two-factor authentication and monitored by surveillance cameras. Access is allowed only to authorized staff that 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. Delivery areas and loading docks and other points where unauthorized persons may enter the premises are controlled and isolated.

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. IBM performs industry standard SSAE 16 audits (or their equivalent) 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. IBM employees and vendor employees complete workforce security and awareness training annually. Personnel are reminded of their job objectives and their responsibility to meet ethical business conduct, confidentiality, and IBM's security obligations annually.

3. Service Level Commitment

IBM provides the following availability service level agreement ("SLA") for the Cloud Service. You understand that the SLA does not constitute a warranty to you.

3.1 Definitions

a. "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.

b. "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.

c. "Contracted Month" means each full month during the term 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.

d. "Downtime" means a period of time during which production system processing for the Cloud Service has stopped and your users are unable to use all aspects of the Cloud Service for which they have permissions. Downtime does not include the period of time when the Cloud Service is not available because of:

   (1) A scheduled outage for the purpose of maintenance;

   (2) Events or causes beyond IBM's control (e.g., natural disaster, internet outages, emergency maintenance, etc.);

   (3) Problems with your applications, equipment or data, or a third party's applications, equipment or data;

   (4) Your failure to adhere to required system configurations and supported platforms for accessing the Service; or

   (5) IBM's compliance with any designs, specifications, or instructions that you provide to IBM or a third party provides to IBM on your behalf.

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

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

3.2 Availability Credits

a. To submit a Claim, you must log a Severity 1 support ticket (as defined below in the Technical Support section) for each Event with the IBM technical 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 information about the Event and reasonably assist IBM with the diagnosis and resolution of the Event.

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

c. Availability Credits are 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.

d. 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.

3.3 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 _____ 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

3.4 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, participants and permitted invitees of the Cloud Service or to any beta or trial services that IBM provides. The SLA only applies to the Cloud Services that are in production use, so it does not apply to non-production environments, including but not limited to test, disaster recovery, quality assurance, or development.

4. Entitlement and Billing Information

4.1 Charge Metrics

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

a. Entity ID is a unit of measure by which the Cloud Service can be obtained. An Entity ID is a unique identifier for any entity represented within the Cloud Service. Sufficient entitlements must be obtained to cover the number of Entity IDs identified in the Cloud Service during the measurement period specified in Customer's Proof of Entitlement (PoE) or Order Document.

   For this Cloud Service, an Entity ID is a unique identifier for a trading entity, regardless of that trading entity's organizational structure.

b. Gigabyte is a unit of measure by which the Cloud Service can be obtained. A Gigabyte is defined as 2 to the 30th power bytes of data (1,073,741,824 bytes). Sufficient entitlements must be obtained to cover the total number of Gigabytes processed by the Cloud Service during the measurement period specified in Customer's Proof of Entitlement (PoE) or Order Document.

4.2 Charges and Billing

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

4.2.1 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.

4.2.2 Overages

If your actual usage of the Cloud Service exceeds the entitlement specified in the Order Document, then you will be invoiced for the overage in accordance with the overage rates specified in the Order Document.

4.2.3 On-Demand

On-Demand options will be invoiced in the month the on-demand option is employed by you at the rate set forth in the Order Document.

4.2.4 Set-up

Set-up charges will be specified in an 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 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 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 for the Cloud Service is available during the subscription period. The standard technical support may be enhanced with the premium support services options, described in Section 1 above.

Regular Phone and Email Support Hours of Operation are as follows:

8:00 a.m. – 11:00 p.m. Eastern Time zone, U.S., Monday – Friday

After Hours Support:

After Hours Support (outside of the regular operating hours stated above) is available only for Severity 1 issues on business days, weekends, and holidays.

Support Hotline: 1-877-432-4300

Email: scn_support@us.ibm.com

Support web portal: https://support.ibmcloud.com/

Severity	Severity Definition	Response Time Objectives	Response Time Coverage
1	**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.	Within 1 hour	24x7
2	**Significant business impact:** A service business feature or function of the service is severely restricted in its use or you are in jeopardy of missing business deadlines.	Within 2 business hours	M-F business hours
3	**Minor business impact:** Indicates the service or functionality is usable and it is not a critical impact on operations.	Within 4 business hours	M-F business hours

4	**Minimal business impact:** An inquiry or non-technical request	Within 1 business day	M-F business hours

7. Additional Information

a. IBM (a) may compile and analyze anonymous, aggregate, summary data related to your use of the Cloud Service, and (b) may prepare reports, studies, analyses, and other work product resulting from this compilation and analysis.

b. IBM may copy data to a non-production server within the Cloud Services environment for the exclusive purpose of testing and improving the quality of IBM's offerings.

c. The Cloud Service may involve the transmission of content including customer ID and password from, to, or over third-party systems or networks, such as the Internet and other interconnect services, over which IBM exercises no control and for which IBM is not responsible or liable. Senders and receivers of the content that is coming through the Cloud Services environment for your trading community might not treat that content as confidential. Accordingly, you should encrypt the content if you want to make the content unreadable or indecipherable in the Cloud Services environment and in transit over IBM and other third party networks. You are responsible for, and assume any risk for, choosing the protocols and means you use to transmit content over IBM and other third party networks.

d. The Cloud Service is not designed to comply with the U.S. Health Insurance Portability and Accountability Act ("HIPAA") and may not be used for the transmission or storage of any personal or individually identifiable health care claim data or other health information.

e. IBM must approve any communications software, devices and equipment used to transmit data to (and receive data from) IBM. You are responsible for obtaining an appropriate internet service account and connection for accessing the Cloud Service.

f. Your successful use of the Cloud Service will depend on your assistance with ensuring that you and your trading partners do the following:

   (1) Implement connectivity between you and IBM and work with IBM during joint connectivity testing between you and IBM;

   (2) Ensure adequate security over your respective applications, hardware (including installing and maintaining appropriate firewalls to prevent unauthorized access), mailboxes, and transmission and monitor those mailboxes and transmissions;

   (3) Inspect data for accuracy and completeness and ensure that appropriate safeguards are in place to identify data, processing, and transmission errors;

   (4) Promptly notify IBM of any translation errors or failures, processing errors or failures, nonconforming transmissions, failures to send or receive transmissions, or inability to access any mailbox;

   (5) Set the applicable data-processing parameters and transmissions parameters;

   (6) Maintain supporting data, files, and other materials sufficient to enable IBM to recover all data, files, and other materials (such as card files, tape files, disk files, and printer outputs) needed to re-perform any service provided by the Cloud Service; and

   (7) Maintain business continuity and communicate expectations to your trading partner community, as it relates to test periods, migrations, and conversions of and to the Cloud Service.

7.1 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.