IBM Terms of Use – SaaS Specific Offering Terms

MaaS360 (SaaS)

The Terms of Use ("ToU") is composed of this IBM Terms of Use - SaaS Specific Offering Terms ("SaaS Specific Offering Terms") and a document entitled IBM Terms of Use - General Terms ("General Terms") available at the following URL: **www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/**.

In the event of a conflict, the SaaS Specific Offering Terms prevail over the General Terms. By ordering, accessing or using the IBM SaaS, Customer agrees to the ToU.

The ToU is governed by the IBM International Passport Advantage Agreement, the IBM International Passport Advantage Express Agreement, or the IBM International Agreement for Selected IBM SaaS Offerings, as applicable ("Agreement") and together with the ToU make the complete agreement.

Part 1 – IBM Terms

1. IBM SaaS

The following IBM SaaS offerings are covered by these SaaS Specific Offering Terms:

- IBM MaaS360 Mobile Device Management (SaaS)
- IBM MaaS360 Mobile Device Management (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Application Management (SaaS)
- IBM MaaS360 Mobile Application Management (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Application Security (SaaS)
- IBM MaaS360 Mobile Application Security (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Enterprise Gateway for Apps (SaaS)
- IBM MaaS360 Mobile Enterprise Gateway for Apps (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Content Management (SaaS)
- IBM MaaS360 Mobile Content Management (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Secure Document Sync (SaaS)
- IBM MaaS360 Secure Document Sync (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Secure Editor (SaaS)
- IBM MaaS360 Secure Editor (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Enterprise Gateway for Documents (SaaS)
- IBM MaaS360 Mobile Enterprise Gateway for Documents (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Email Management (SaaS)
- IBM MaaS360 Mobile Email Management (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Secure Browser (SaaS)
- IBM MaaS360 Secure Browser (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Enterprise Gateway for Secure Browser (SaaS)
- IBM MaaS360 Mobile Enterprise Gateway for Secure Browser (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Enterprise Server Management for BlackBerry (SaaS)
- IBM MaaS360 Enterprise Server Management for BlackBerry (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Expense Management (SaaS)
- IBM MaaS360 Mobile Expense Management (SaaS) Step up for existing IBM MaaS360 customers

- IBM MaaS360 Advanced Mobile Management Suite (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Secure Productivity Suite (SaaS)
- IBM MaaS360 Secure Productivity Suite (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Secure Mail (SaaS)
- IBM MaaS360 Secure Mail (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Enterprise Gateway Suite (SaaS)
- IBM MaaS360 Mobile Enterprise Gateway Suite (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Secure Document Sharing Suite (SaaS)
- IBM MaaS360 Secure Document Sharing Suite (SaaS) Step up for existing IBM MaaS360 customers
- IBM MaaS360 Mobile Threat Management (SaaS)
- IBM MaaS360 Content Service (SaaS)
- IBM MaaS360 Content Service Storage (SaaS)
- IBM MaaS360 Content Service Bandwidth (SaaS)

2. Charge Metrics

The IBM SaaS is sold under one of the following charge metric(s) as specified in the Transaction Document:

a. Authorized User is a unit of measure by which the IBM SaaS can be obtained. Customer must obtain separate, dedicated entitlements for each unique Authorized User given access to the IBM SaaS 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 IBM SaaS during the measurement period specified in Customer's Proof of Entitlement (PoE) or Transaction Document.

b. Gigabyte is a unit of measure by which the IBM SaaS 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 IBM SaaS during the measurement period specified in Customer's Proof of Entitlement (PoE) or Transaction Document.

c. Managed Client Device is a unit of measure by which IBM SaaS can be obtained. A Client Device is a single user computing device or special purpose sensor or telemetry device that requests the execution of or receives for execution a set of commands, procedures, or applications from or provides data to another computer system that is typically referred to as a server or is otherwise managed by the server. Multiple Client Devices may share access to a common server. A Client Device may have some processing capability or be programmable to allow a user to do work. Customer must obtain Managed Client Device entitlements for every Client Device managed by the IBM SaaS during the measurement period specified in Customer's Proof of Entitlement (PoE) or Transaction Document.

3. Charges and Billing

The amount payable for the IBM SaaS is specified in a Transaction Document.

3.1 Partial Month Charges

The partial month charge is a pro-rated daily rate that will be charged to Customer. The partial month charges are calculated based on the remaining days of the partial month starting on the date Customer is notified by IBM that their access to the IBM SaaS is available.

3.2 Overage Charges

If Customer’s actual usage of the IBM SaaS during the measurement period exceeds the entitlement stated on the PoE, then Customer will be invoiced for the overage, as set forth in the Transaction Document.

4. IBM SaaS Subscription Period Renewal Options

Customer's PoE will set forth whether the IBM SaaS will renew at the end of the Subscription Period, by designating one of the following:

4.1 Automatic Renewal

If Customer's PoE states that Customer's renewal is automatic, Customer may terminate the expiring IBM SaaS Subscription Period by written request to Customer's IBM sales representative or IBM Business Partner, at least ninety (90) days prior to the expiration date as set forth in the PoE. If IBM or its IBM Business Partner does not receive such termination notice by the expiration date, the expiring Subscription Period will be automatically renewed for either one year or the same duration as the original Subscription Period as set forth in the PoE.

THE RENEWAL ENTITLEMENT QUANTITY WILL BE EQUAL TO THE GREATER OF THE ORIGINAL ORDER QUANTITY OR THE MONTHLY REPORTED USAGE FOR THE MONTH PRIOR TO GENERATION OF THE RENEWAL INVOICE UNLESS IBM RECEIVES A NOTIFICATION SPECIFYING A DIFFERENT ENTITLEMENT QUANTITY.

THE RENEWAL ENTITLEMENT QUANTITY FOR STEP UP OFFERING WILL BE EQUAL TO THE ORIGINAL ORDER QUANTITY.

4.2 Continuous Billing

When the PoE states that Customer's renewal is continuous, Customer will continue to have access to the IBM SaaS and will be billed for the usage of the IBM SaaS on a continuous basis. To discontinue use of the IBM SaaS and stop the continuous billing process, Customer will need to provide IBM or its IBM Business Partner with ninety (90) days written notice requesting that Customer's IBM SaaS be cancelled. Upon cancellation of Customer's access, Customer will be billed for any outstanding access charges through the month in which the cancellation took effect.

4.3 Renewal Required

When the PoE states that Customer's renewal type is "terminate", the IBM SaaS will terminate at the end of the Subscription Period and Customer's access to the IBM SaaS will be removed. To continue to use the IBM SaaS beyond the end date, Customer will need to place an order with Customer's IBM sales representative or IBM Business Partner to purchase a new Subscription Period.

5. Technical Support

Technical support for IBM SaaS is structured 2nd level support to a customer's Operation team, not End User support and is available during the subscription period. .

Support is provided through multiple channels; 24 x 7. Information regarding support of the IBM SaaS solution can be found on product portal.

Expected Responsiveness targets:

Severity	Severity Definition	Initial 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.	30 Minutes	24x7
2	**High 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.	1 business hour	24 x 7
3	**Medium business impact:** Indicates the service or functionality is usable and it is not a critical impact on operations.	2 business hours	24 x 7
4	**Low business impact:** An inquiry or non-technical request	3 business hours	24 x 7

6. IBM SaaS Offering Additional Terms

6.1 Step up Limitation

For IBM SaaS offerings designated as “Step up for existing Customers” (“Step up SaaS”), customer must have previously or simultaneously acquired appropriate license entitlements to the associated IBM program as identified in the name of the Step up SaaS offering. For example, Customer who purchases “IBM MaaS360 Mobile Device Management (SaaS) – Step up for existing Customers” must have licensed entitlements to the associated IBM program of IBM MaaS360. Customer’s entitlements to the Step up SaaS cannot exceed Customer’s entitlements to the associated IBM program.

When acquiring Step up SaaS, Customer may not use the same associated IBM program license entitlements within their on-premise installed environment as well as with the Step up SaaS entitlements. For example, if Customer has 250 Managed Client Device entitlements to the associated IBM program and chooses to purchase 100 Step up SaaS Managed Client Device entitlements, Customer can manage 100 Step up SaaS Managed Client Devices from the IBM SaaS environment and 150 Managed Client Devices from the software installed on-premise.

Customer represents they have acquired the applicable (1) license entitlements and (2) Subscription and Support for the associated IBM program(s). During the Subscription Period of the Step up SaaS, Customer must maintain current Subscription and Support for the IBM program entitlements used in conjunction with the Step up SaaS entitlements. In the event either Customer’s license to use the associated IBM program(s) or Customer’s Subscription and Support for the associated IBM program(s) is terminated, Customer’s right to use the Step Up SaaS will terminate.

6.2 Cookies

Customer agrees that IBM may use cookies and tracking technologies to collect personally identifiable information in gathering usage statistics and information designed to help improve user experience and/or to tailor interactions with users in accordance with **http://www-01.ibm.com/software/info/product-privacy/index.html**

6.3 Cross Border Transfers

Customer agrees that IBM may process the Content, including any Personal Data, under relevant laws and requirements across a country border to processors and sub-processors in the following countries outside of the European Economic Area and countries considered by the European Commission to have adequate levels of security: the USA; and other countries: India, Singapore, Hong Kong (China.)

6.4 EU Data Privacy

If Customer makes personal data available to IBM SaaS offerings in the EU Member States, Iceland, Liechtenstein, Norway, or Switzerland, or if Customer has authorized users or devices in those countries, then Customer as the sole controller appoint IBM as a processor to process (as those terms are defined in EU Directive 95/46/EC) Personal Data. IBM will only process such personal data to the extent required to make the IBM SaaS offering available in accordance with IBM’s published descriptions of the IBM SaaS and Customer agrees that any such processing is in accordance with Customer’s instructions.

Custoemr agrees that IBM may process content including any personal data across a country border to the following processors and sub-processors:

Name of Processor/Subprocessor	Role (Data Processor or Subprocessor)	Location
The IBM Contracting Entity	Processor	As stated on the Order Document
Amazon Web Services, LLC	Sub-processor	410 Terry Ave. N Seattle, WA 98109, USA
IBM Corporation	Sub-processor	1 New Orchard Rd. Armonk, NY 10504, USA I
Fiberlink Communications Corporation, an IBM company	Sub-processor	1787 Sentry Pkwy West, Bldg 18, Ste 200 Blue Bell, PA 19422, USA

Fiberlink Software Private Limited, an IBM company	Sub-processor	#99/100 Prestige Towers Residency Road Bangalore 560 025 India
IBM India Private Limited	Sub-processor	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 India
Equinix LLC	Sub-processor	1950 Stemmons Freeway Suite 1039A Dallas, TX 75207, USA
Softlayer Technologies, Inc., an IBM company	Sub-processor	29A International Business Park East Jurong, 139964 Singapore
Softlayer Technologies, Inc., an IBM company	Sub-processor	Tseung Kwan O Industrial Estate Hong Kong

Custoemr agrees that IBM may, on notice, vary this list of country locations when it reasonably determines it necessary for the provision of the IBM SaaS.

6.5 Safe Harbor Compliance

The IBM SaaS offerings are included in Fiberlink Communications Corporation (IBM Subsidiary) US-EU Safe Harbor certification. Both IBM and Fiberlink abide by the U.S. - EU Safe Harbor Framework as set forth by the United States Department of Commerce regarding the collection, use and retention of information collected from the European Union. For more information about Safe Harbor or to access Fiberlink's certification statement, go to **http://www.export.gov/safeharbor/**.

When IBM's US-EU Safe Harbor Framework does not apply to a transfer of EEA Personal Data, the parties or their relevant affiliates may enter into separate standard unmodified EU Model Clause agreements in their corresponding roles pursuant to EC Decision 2010/87/EU with optional clauses removed. All disputes or liability arising under these agreements, even if entered into by affiliates, will be treated by the parties as if the dispute or liability arose between them under the terms of this Agreement.

6.6 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) Customer identifies as receiving benefit of the IBM SaaS. IBM will apply taxes based upon the business address listed when ordering an IBM SaaS as the primary benefit location unless Customer provides additional information to IBM. Customer is responsible for keeping such information current and providing any changes to IBM.

6.7 Normative Data

Notwithstanding anything to the contrary, for normative research, analysis, demonstration and reporting purposes only, IBM may retain and use in aggregated and anonymous format (i.e., so that you or your authorized users cannot be identified as the source of the data and so that personally identifiable information allowing identification of Customer or Customer's authorized users is removed) data reflecting Customer's authorized users' individual experiences with the IBM SaaS.

6.8 Lawful Use and Consent

6.8.1 Authorization to Collect and Process Data

The IBM SaaS is designed to provision, manage, secure, monitor and control mobile devices. The IBM SaaS will collect information from users and devices who are authorized by you to interact with the IBM SaaS for which Customer has subscribed. The IBM SaaS collects information that alone or in combination may be considered Personal Information in some jurisdictions. Collected data may include authorized user name, telephone number, registered email address and device location, userID and secure browsing history, information about end user device hardware, software and settings, and information generated by the device. Customer authorizes IBM to collect, process, and use this information in accordance with the terms of this Terms of Use.

6.8.2 Informed Consent from Data Subjects

Use of the IBM SaaS may implicate various laws and regulations. The IBM SaaS may be used only for lawful purposes and in a lawful manner. Customer agrees to use the IBM SaaS pursuant to, and assume all responsibility for complying with, applicable laws, regulations, and policies.

Customer agrees that Customer has obtained or will obtain any fully informed consents, permissions, or licenses necessary to enable lawful use of the IBM SaaS and to permit collection and processing of the information by IBM as your data processor through the IBM SaaS. Customer hereby authorizes IBM to obtain fully informed consents necessary to enable lawful use of the IBM SaaS and to collect and process the information as described in the end user license agreement available at http://www.ibm.com/software/sla/sladb.nsf/.

6.9 Data Retention

IBM will delete any collected information, which may include Personal Information, within six (6) months of expiration or termination of this Terms of Use, except for that which is required to be retained according to applicable law, rule or regulation. In such case, IBM will retain the collected information for the duration required by such applicable law, rule or regulation.

Appendix A

MaaS360 is an easy-to-use cloud platform with all of the essential functionality for end-to-end management of today's mobile devices including iPhones, iPads, Androids, Kindle Fire devices, Windows Phones and BlackBerry smartphones. Following is a short description of the IBM SaaS offerings:

a. IBM MaaS360 Mobile Device Management (SaaS)

The core mobility device management (MDM) features includes device enrollment, configuration, security policy management and device actions, such as send message, locate, lock, and wipe. The Advanced MDM features include automated compliance rules, bring your own device (BYOD) privacy settings, and Mobility Intelligence dashboards and reporting.

b. IBM MaaS360 Mobile Application Management (SaaS)

MaaS360 Mobile Application Management provides the ability to add applications and distribute them to supported devices managed by MaaS360. This includes MaaS360 App Catalog, an on-device application for users to view, install, and be alerted to updated, managed applications.

c. IBM MaaS360 Mobile Application Security (SaaS)

MaaS360 Mobile Application Security provides additional data protection for enterprise applications that use the WorkPlace SDK during development, or for iOS apps upload the application (.ipa), provisioning profile, and signing certificate to be automatically integrated. Mobile Application Security integrates the app with the Secure Productivity Suite. This enables single sign on, Intranet access through the Mobile Enterprise Gateway, and enforcement of data security settings.

d. IBM MaaS360 Mobile Enterprise Gateway for Apps (SaaS)

MaaS360 Mobile Enterprise Gateway for Apps provides users outside the enterprise network secure, seamless access to internal application resources without requiring a full-device, VPN connection.

e. IBM MaaS360 Mobile Content Management (SaaS)

MaaS360 Mobile Content Management allows the administrator to add and distribute documents to the supported devices that are managed by MaaS360 MDM. Includes MaaS360 Doc Catalogue, an on-device, password-protected container that provides a secure and simple way for users to access, view, and share documents. It includes seamless access to distributed content and repositories such as SharePoint, Box, and Google Drive. Access to private SharePoint and Windows files shares are available with the MaaS360 Mobile Enterprise Gateway. Documents managed through MaaS360 can be version controlled, audited, and secured through data loss prevention (DLP) policy options, such as require authentication, restrict copy-paste functionality, and block from being opened or shared in other applications.

f. IBM MaaS360 Secure Document Sync (SaaS)

MaaS360 Secure Document Sync provides users with the ability to easily and securely synchronize user content across managed mobile devices. Administrators can ensure that policies, such as restricting cut-copy-paste, and blocking content from being opened or shared in other apps or are in place for user content across devices. Content is stored securely, both in the cloud and on the device, and accessed only through the MaaS360 Doc Catalogue.

g. IBM MaaS360 Secure Editor (SaaS)

MaaS360 Secure Editor is a powerful office suite that allows users to work with business documents while on the go. MaaS360 Secure Editor enables to:

- Create and edit .DOC, .PPT, and .XLS files
- Presentation mode for slides
- Easily work with email attachments and other files from MaaS360 for iOS

h. IBM MaaS360 Mobile Enterprise Gateway for Documents (SaaS)

With MaaS360 Mobile Enterprise Gateway for Docs, organizations can use MaaS360 Mobile Content Management to additionally offer devices outside the enterprise network secure seamless access to internal Connections sites, SharePoint sites, Windows File Shares and other file stores

without requiring a full device VPN connection. Use of MaaS360 Mobile Enterprise Gateway for Docs requires also purchasing MaaS360 Mobile Content Management. Supports iOS 5.0 and Android 4.0 or above.

i. IBM MaaS360 Mobile Email Management (SaaS)

MaaS360 Mobile Email Management includes key features in support of Microsoft Exchange ActiveSync and Lotus Traveler.

- Exchange ActiveSync: Provides support for mobile devices connecting to Microsoft Exchange over the ActiveSync protocol. Features include core mobile device management functions, such as the ability to configure devices, create; enforce ActiveSync policies (passcode, block, or allow access to email); and take device actions, such as lock and wipe, and detailed report on device attributes.
- Lotus Traveler: Provides support for mobile devices that connect to IBM Lotus Notes® over the Lotus Traveler protocol. Features include the ability to configure devices, block or allow devices, enforce passcode policies, wipe devices, and develop detailed report on device attributes.

j. IBM MaaS360 Secure Browser (SaaS)

MaaS360 Secure Browser is a full-featured web browser to enable secure access to corporate intranet sites and enforce compliance of content policies by defining website filtering and security policies to ensure that users only access approved web content that is based on a number of content categories, such as social networking, explicit, or malware sites. Includes the ability to disable native and third-party web browsers either through application policy or blacklisting when combined with MaaS360 MDM. It allows whitelist exceptions to websites, restrict cookies; copy, paste, and print features; and enable Kiosk mode.

k. IBM MaaS360 Mobile Enterprise Gateway for Secure Browser (SaaS)

MaaS360 Mobile Enterprise Gateway for Secure Browser allows supported devices to access approved internal web sites without requiring a full-device level, VPN connection.

l. IBM MaaS360 Enterprise Server Management for BlackBerry (SaaS)

Provides support for BlackBerry Enterprise Server (BES) connected mobile devices by utilizing BlackBerry APIs. Features include remote actions such as send a message, reset passcode, assign BES policy and wipe, as well as detailed reporting on device attributes. Installation of MaaS360 Cloud Extender is required. Available only for devices viewed or managed with MaaS360 through BES 5.0.

m. IBM MaaS360 Mobile Expense Management (SaaS)

MaaS360 Mobile Expense Management allows the administrator to create data usage policies and assign them to supported devices that are managed by MaaS360, and assign these policies at a device, group, or global level and configure alert thresholds and messaging for both in network and roaming data usage.

n. IBM MaaS360 Advanced Mobile Management Suite (SaaS)

Suite/Bundle of products including MaaS360 Mobile Device Management, MaaS360 Mobile Application Management, MaaS360 Content Cloud, and MaaS360 Mobile Expense Management.

o. IBM MaaS360 Secure Productivity Suite (SaaS)

Suite/Bundle of products including MaaS360 Secure Mail, MaaS360 Mobile Application Management, MaaS360 Mobile Application Security, MaaS360 Content Cloud, and MaaS360 Secure Browser.

p. IBM MaaS360 Secure Mail (SaaS)

MaaS360 Secure Mail provides a separate and secure office productivity application for users to access and manage email, calendar, and contacts with the ability to control emails and attachments to prevent data leakage by restricting the ability to forward or move content to other applications, to enforce authentication, restrict cut-copy-paste, and lock down email attachments for view only.

q. IBM MaaS360 Mobile Enterprise Gateway Suite (SaaS)

MaaS360 Mobile Enterprise Gateway Suite allows supported apps on iOS and Android to securely and seamless communicate back to resources on the company's internal network.

r. IBM MaaS360 Secure Document Sharing Suite (SaaS)

Suite/Bundle of products including MaaS360 Mobile Content Management, MaaS360 Secure Editor, SaaS360 Secure Document Sync, and MaaS360 Content Cloud.

s. IBM MaaS360 Mobile Threat Management (SaaS)

MaaS360 Mobile Threat Management provides enhanced mobile security with mobile malware detection and advanced jailbreak/root detection. With MaaS360 Mobile Threat Management, Customer will be able to set and manage compliance policies around detected malware and other security vulnerabilities.

t. IBM MaaS360 Content Service (SaaS)

MaaS360 Content Service (SaaS) provides users with the ability to upload application packages and documents to MaaS360's Content Distribution system.

Clients with MaaS360 Content Service will also need to purchase at least one entitlement of both MaaS360 Content Service Storage (SaaS) and MaaS360 Content Service Bandwidth (SaaS).

u. IBM MaaS360 Content Service Storage (SaaS)

MaaS360 Content Service Storage (SaaS) provides users the ability to purchase a total amount of data storage available for use with the MaaS360 Content Service (SaaS)

v. IBM MaaS360 Content Service Bandwidth (SaaS)

MaaS360 Content Service Bandwidth (SaaS) provides users the ability to purchase the total amount of bandwidth available for use with the MaaS360 Content Service (SaaS)

Appendix B

IBM provides the following availability service level agreement ("SLA") for the IBM SaaS and is applicable if specified in Customer's Proof of Entitlement (PoE) or Transaction Document.

The version of this SLA that is current at the commencement or renewal of the term of your subscription will apply. You understand that the SLA does not constitute a warranty to you.

1. Definitions

a. "Authorized Contact" means the individual you have specified to IBM who is authorized to submit Claims under this SLA.

b. "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 IBM SaaS.

c. "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.

d. "Contracted Month" means each full month during the term of the IBM SaaS measured from 12:00 a.m. GMT on the first day of the month through 11:59 p.m. GMT on the last day of the month.

e. "Customer" or "you" or "your" means an entity that is subscribing for the IBM SaaS directly from IBM, and that is not in default of any material obligations, including payment obligations, under its contract with IBM for the IBM SaaS.

f. "Downtime" means Application Downtime and/or Inbound Processing Downtime applicable to the corresponding Service Level shown on the table below. Downtime does not include the period of time when the IBM SaaS is not available as a result of:

- Planned System Downtime;
- Force Majeure;
- Problems with Customer or third party applications, equipment, or data;
- Customer or third party acts or omissions (including anyone gaining access to the IBM SaaS by means of your passwords or equipment);
- Failure to adhere to required system configurations and supported platforms for accessing the IBM SaaS; or
- IBM's compliance with any designs, specifications, or instructions provided by Customer or a third party on Customer's behalf.

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

h. "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 the IBM SaaS unavailability that was outside IBM's reasonable control.

i. "Planned System Downtime" means a scheduled outage of the IBM SaaS for the purpose of maintenance.

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

2. Availability Credits

a. In order to be eligible to submit a Claim you must have logged a support ticket for each Event with the IBM customer support help desk for the applicable IBM SaaS, in accordance with IBM procedure for reporting Severity 1 support issues. You must provide all necessary detailed information about the Event and reasonably assist IBM with the diagnosis and resolution of the Event to the extent required for Severity 1 support tickets. Such ticket must be logged within twenty-four (24) hours of your first becoming aware that the Event has impacted your use of the IBM SaaS.

b. Your Authorized Contact 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.

c. Your Authorized Contact must provide to IBM all reasonable details regarding the Claim, including but not limited to, detailed descriptions of all relevant Events and the Service Level claimed not to have been met.

d. IBM will measure internally total combined Downtime during each Contracted Month applicable to the corresponding Service Level shown on the table below. 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. If Customer reports an Event of Application Downtime and an Event of Inbound Data Processing Downtime occurring simultaneously, then IBM will treat the overlapping periods of Downtime as a single period of Downtime, and not as two separate periods of 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 on the tables below. IBM will not be liable for multiple Availability Credits for the same Event(s) in the same Contracted Month.

e. For Bundled Service (individual IBM SaaS 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 IBM SaaS. You may only submit Claims relating to one individual IBM SaaS in a bundle in any Contracted Month, and IBM will not be liable for Availability Credits with respect to more than one IBM SaaS in a bundle in any Contracted Month.

f. If you purchased the IBM SaaS from a valid IBM reseller in a remarketing transaction in which IBM maintains primary responsibility for fulfilling the IBM SaaS and SLA commitments, then the Availability Credit will be based on the then-current Relationship Suggested Value Price (RSVP) for the IBM SaaS in effect for the Contracted Month which is the subject of a Claim, discounted at a rate of 50%.

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

h. IBM will use its reasonable judgment to validate Claims based on information available in IBM's records, which will prevail in the event of a conflict with data in your records.

i. THE AVAILABILITY CREDITS PROVIDED TO YOU IN ACCORDANCE WITH THIS SLA ARE YOUR SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM.

3. Service Levels – Availability of the IBM SaaS during a Contracted Month

Achieved Service Level (during a Contracted Month)	**Availability Credit (% of Monthly Subscription Fee for Contracted Month which is the subject of a Claim)**
Less than 99.8%	2%
Less than 98.8%	5%
Less than 95.0%	10%

"Achieved Service Level", expressed as a percentage 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.

Example: 50 minutes total Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month -- 50 minutes Downtime = 43,150 minutes _____ 43,200 total minutes	= 2% Availability Credit for 99.8% Achieved Service Level during the Contracted Month

4. Exclusions

This SLA is made available only to IBM Customers. This SLA does not apply to the following:

- Beta and trial Services.
- Non-production environments, including but not limited to, test, disaster recovery, quality assurance, or development.
- Claims made by an IBM Customer's users, guests, participants and permitted invitees of the IBM SaaS.
- Enabling Software