IBM MaaS360 (SaaS)

This Service Description describes the Cloud Service IBM provides to Client. Client means the contracting party and its authorized users and recipients of the Cloud Service. The applicable Quotation and Proof of Entitlement (PoE) are provided as separate Transaction Documents.

1. Cloud Service

MaaS360 is an easy-to-use cloud platform with all of the essential functionality for end-to-end management of today's mobile devices utilizing the iOS, Android, Windows and Blackberry operating systems. Following is a short description of the Cloud Service offerings:

1.1 IBM MaaS360 Mobile Device Management (SaaS) and IBM MaaS360 Mobile Device Management (SaaS) Step up for existing customers

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.

1.2 IBM MaaS360 Mobile Application Management (SaaS) and IBM MaaS360 Mobile Application Management (SaaS) Step up for existing customers

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.

1.3 IBM MaaS360 Mobile Application Security (SaaS) and IBM MaaS360 Mobile Application Security (SaaS) Step up for existing customers

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 Productivity Suite. This enables single sign on, Intranet access through the Mobile Enterprise Gateway, and enforcement of data security settings.

1.4 IBM MaaS360 Gateway for Apps (SaaS) and IBM MaaS360 Gateway for Apps (SaaS) Step up for existing customers

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

1.5 IBM MaaS360 Mobile Content Management (SaaS) and IBM MaaS360 Mobile Content Management (SaaS) Step up for existing customers

MaaS360 Mobile Content Management allows the administrator to add and distribute documents to the supported devices that are managed by IBM MaaS360 Mobile Device Management. Includes IBM MaaS360 Doc Catalogue, an on-device, password-protected container that provides a protected 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 Gateway for Documents. Documents managed through MaaS360 can be version controlled, audited, and protected 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.

1.6 IBM MaaS360 Mobile Document Sync (SaaS) and IBM MaaS360 Mobile Document Sync (SaaS) Step up for existing customers

MaaS360 Mobile Document Sync provides users with the ability to 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 in a protected fashion both in the cloud and on the device, and accessed only through the MaaS360 Doc Catalogue.

1.7 IBM MaaS360 Mobile Document Editor (SaaS) and IBM MaaS360 Mobile Document Editor (SaaS) Step up for existing customers

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

1.8 IBM MaaS360 Gateway for Documents (SaaS) and IBM MaaS360 Gateway for Documents (SaaS) Step up for existing customers

With MaaS360 Gateway for Documents, organizations can use MaaS360 Mobile Content Management to additionally offer devices outside the enterprise network a 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 Gateway for Documents requires also purchasing MaaS360 Mobile Content Management. Supports iOS 5.0 and Android 4.0 or above.

1.9 IBM MaaS360 Email Management (SaaS) and IBM MaaS360 Email Management (SaaS) Step up for existing customers

MaaS360 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.

1.10 IBM MaaS360 Secure Mobile Browser (SaaS) and IBM MaaS360 Secure Mobile Browser (SaaS) Step up for existing customers

MaaS360 Browser is a full-featured web browser which enables 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 MobileFirst Protect Devices. It allows whitelist exceptions to websites, restrict cookies; copy, paste, and print features; and enable Kiosk mode.

1.11 IBM MaaS360 Gateway for Browser (SaaS) and IBM MaaS360 Gateway for Browser (SaaS) Step up for existing customers

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

1.12 IBM MaaS360 for BlackBerry (SaaS) and IBM MaaS360 for BlackBerry (SaaS) Step up for existing customers

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.

1.13 IBM MaaS360 Mobile Expense Management (SaaS) and IBM MaaS360 Mobile Expense Management (SaaS) Step up for existing customers

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.

1.14 IBM MaaS360 Productivity Suite (SaaS) and IBM MaaS360 Productivity Suite (SaaS) Step up for existing customers

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

1.15 IBM MaaS360 Secure Mobile Mail (SaaS) and IBM MaaS360 Secure Mobile Mail (SaaS) Step up for existing customers

MaaS360 Secure Mobile Mail provides a separate 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.

1.16 IBM MaaS360 Gateway Suite (SaaS) and IBM MaaS360 Gateway Suite (SaaS) Step up for existing customers

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

1.17 IBM MaaS360 Content Suite (SaaS) and IBM MaaS360 Content Suite (SaaS) Step up for existing customers

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

1.18 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, Client will be able to set and manage compliance policies around detected malware and other security vulnerabilities.

1.19 IBM MaaS360 Content Service (SaaS)

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

IBM MaaS360 provides each Client with 1GB of Storage. IBM MaaS360 also provides 6 GB of bandwidth utilization per device per year as a shared pool of bandwidth. The entire bandwidth pool is shared across all devices. This base storage and bandwidth allocation does not increase regardless of the number of product bundles or line items purchased. Clients are required to purchase additional storage and/or bandwidth for any amount used or required over the base amount provided.

1.20 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).

1.21 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).

1.22 IBM MaaS360 Professional (SaaS)

Provides small and medium-sized businesses with a fast and simple way to remotely configure smartphones and tablets, enforce security policies, push apps and docs, and protect the data on corporate and personal devices. Client can gain access to the right mobility management capabilities for Client's business quickly, easily, and affordably.

1.23 IBM MaaS360 VPN (SaaS)

IBM MaaS360 VPN is a virtual private network (VPN) solution that enables users to connect seamlessly to their corporate network from mobile devices. The solution consists of the VPN server and the client for mobile devices, and supports features such as Device VPN, On-demand VPN, Always on VPN, Per-app VPN and Split tunneling.

1.24 IBM MaaS360 Laptop Location (SaaS)

MaaS360 Laptop Location (SaaS) enabled the ability to locate supported laptops and tablets. MaaS360 reports the location of the Wi-Fi or IP address coordinates and translates this data into an easily recognizable address. When a device is online, its current location can be retrieved. MaaS360 stores reported locations over time, so location history is available for review. Requires one of the MaaS360 Suites. Supports Windows Vista, Windows 7, Windows 8+.

1.25 IBM MaaS360 Suites

IBM MaaS360 Suites enable Client to select the most appropriate capabilities to drive their use case. Table below captures the primary features and functions included in each MaaS360 Suite:

FEATURES	MANAGEMENT (*)	ESSENTIAL	DELUXE	PREMIER	ENTERPRISE
Mobile Device Management (iOS, Android, Windows Mobile, Windows & macOS)	✓	✓	✓	✓	✓
Mobile Application Management (iOS, Android, Windows Mobile, Windows & macOS)	✓	✓	✓	✓	✓
Patch and Update Management (**)	✓	✓	✓	✓	✓
Advisor	✓	✓	✓	✓	✓
Container App	✓	✓	✓	✓	✓
Mobile Expense Management	✓	✓	✓	✓	✓
Identity Management (***)		✓	✓	✓	✓
Secure Mobile Mail			✓	✓	✓
Secure Mobile Chat			✓	✓	✓
VPN				✓	✓
Secure Browser				✓	✓
Gateway for Browser				✓	✓
Content Management				✓	✓
Gateway for Documents				✓	✓
App Security				✓	✓
Gateway for Apps				✓	✓
Mobile Document Editor					✓
Mobile Document Sync					✓
Mobile Threat Management					✓

* The IBM MaaS360 Management Suite (SaaS) is available for existing customers also as a Step Up part.

** The Patch and Update Management feature provides the ability to identify, report on, distribute and install patches and updates for operating systems and applications running on Windows and macOS endpoints.

*** The Identity Management feature is provided by including the functions of the IBM Cloud Identity Essentials offering which provide Clients single sign-on (SSO) to the other public cloud applications they are using.

1.26 IBM MaaS360 Mobility Success Services

IBM MaaS360 Mobility Success Services are purchased as Engagements to be used within Client's current subscription term and include the following specific services. These remotely delivered Services use IBM consultants to provide guidance and assistance with best practices, configuration and training.

a. **IBM MaaS360 Quick Start Setup Service**

The IBM MaaS360 Quick Start Setup Service provides expertise and guidance for implementing a MaaS360 SaaS deployment with a target environment that includes up to three (3) cloud extenders, one (1) gateway, up to four (4) policies and up to ten (10) device enrollments with a primary goal of knowledge transfer. IBM will a deliver series of web conferences and provide no more than 40 hours of consulting expertise to assist the Client with their deployment. The consultant will discuss best practices of a Bring Your Own Device (BYOD) program, internal business practices and policies that impact deployments, help determine hardware prerequisites, production architecture and a device enrollment strategy.

The consultant will also assist in the setup and configuration of the Cloud Extender(s) and Enterprise Gateway including integration with the client's certificate authority, corporate directory and email system. The consultant will also provide MaaS360 portal and solution training including a portal walkthrough and enablement session for up to three (3) people, assistance in configuration of up to four (4) policies, one (1) container, one (1) iOS policy, one (1) Android policy, and one (1) Windows phone policy including device policy and compliance profile settings. The consultant will discuss best practices and industry standards around policy and user management, reporting, compliance rules, application management as well as app and document management and provide QA on the implemented solution for up ten (10) devices. Two (2) to four (4) weeks after the end of the engagement, the consultant will provide a health check to review use and success of Client adoption of MaaS360 and identify any subsequent services need for full adoption.

b. **IBM MaaS360 Health Check Service**

The IBM MaaS360 Health Check Service provides remotely delivered expertise and guidance which reviews the client's MaaS360 environment and implementation and produces recommendations on user experience, security, and infrastructure scaling. The IBM consultant will conduct a series of web conferences providing no more than eight (8) hours of consulting expertise to assist the Client with their deployment by reviewing critical aspects of scaling, enterprise integration, enrollment processes and will perform test case assessments for performance and user experience to understand and document the required systems and network changes needed for a stable implementation. At the end of the engagement, the IBM consultant will provide and present a Health Check Report Card that will provide details on the test cases and their results and recommendations on increasing user experience and adoption, security, and infrastructure scaling.

c. **IBM MaaS360 Mobility Training Workshop**

The IBM MaaS360 Mobility Training Workshop provides remotely delivered training for up to twelve (12) individuals delivered in English over web and video conference that includes a full curriculum of topics to provide the administrative and support staff with the tools and knowledge to support the MaaS360 solution.

The IBM trainer will deliver a two-day workshop to administrative staff and operations teams. The Client helpdesk team (level 1) will learn how to manage and answer requests from the users, process of level one support handling including IBM MaaS360 fundamentals, administration, escalation and Client deployment related items. The client's mobile operations team (level 2) will be provided additional training to understand the process and support other internal teams in the areas of the container and enterprise integration. Other related client mobile administration staff (email, security, infrastructure, mobile admin teams) will be provided additional modules on how to manage the product effectively, efficiently, and securely including multitenancy, the securing of mobile devices and content. The materials developed for the training session will be provided to all participants in soft copy.

d. **IBM MaaS360 Advisor on Demand**

The IBM MaaS360 Advisor on Demand service provides up to twenty (20) hours of an IBM professional services consultant's time that can be used for activities related to a IBM MaaS360 product optimization and deployment effort. The IBM consultant will assist with advisory technical discussions to provide dedicated support to advise on general strategy, technical design, processes, testing, and production operational best practices during the implementation or migration process. IBM will work with Client to understand and create a project schedule with specific Client requirements, including project goals, relevant technologies, desired timelines, expected deliverables, and estimated number of Advisor on Demand service Engagements. Client must provide access to necessary applications, systems and documentation required to perform the

services. The Advisor on Demand service is completed when up to 20 hours of security expertise has been performed and/or after the project schedule and/or the documented deliverables defined in the project schedule have been delivered to the Client.

1.26.2 IBM MaaS360 Mobility Success Services Responsibilities

IBM will:

- provide the Mobility Success Services purchased by the Client; and
- designate a person to perform as the IBM Engagement Manager who is responsible for working with the customer Project Manager to schedule the engagement and coordinate resources.

Client agrees:

- to be responsible for all charges associated with all Engagement requests made by Client during the contract term;
- and acknowledges, that purchased Engagements must be used within the initial contract term and do expire if unused by the contract period end date; and
- to initiate a formal request for all Set Up Services at least 30 days prior to the end date of the subscription.

In the performance of any Mobility Success Service, IBM may request information and reasonable cooperation from Client. Failure to provide requested information or cooperation in a timely manner by the Client may, as determined by IBM, result in Engagement charges as required by the services or the delay in performance of the applicable service.

In order for IBM to perform the testing accurately, Client agrees to follow IBM instructions in preparing and maintaining the environment for the engagement period, if required.

2. Security Description

This Cloud Service follows IBM's data security and privacy principles for IBM SaaS which are available at http://www.ibm.com/cloud/data-security and any additional terms provided in this section. Any change to IBM's data security and privacy principals will not degrade the security of the Cloud Service.

This Cloud Service may process device information, usernames, and email addresses that contain personal data if Client, as the data controller, determines that the technical and organizational security measures are appropriate to the risks presented by the processing and the nature of the data to be protected. Client recognizes that this Cloud Service does not offer features for the protection of sensitive personal data or data subject to additional regulatory requirements. Client acknowledges that IBM has no knowledge of the types of data that have been included in the Client's content, and cannot make an assessment as to the suitability of the Cloud Services or the security protections which are in place.

2.1 Security Features and Responsibilities

The Cloud Service implements the following security features:

The Cloud Service does encrypt content during data transmission outside of the IBM network. The Cloud Service does encrypt content when at rest awaiting data transmission.

This Cloud Service is included in IBM's Privacy Shield certification and applies when Client chooses to have the Cloud Service hosted in a data center located in the United States, and is subject to IBM's Privacy Shield Privacy Policy, available at http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

3. Service Level Agreement

IBM provides the following availability service level agreement ("SLA") for the Cloud Service as specified in a PoE. The SLA is not a warranty. The SLA is available only to Client and applies only to use in production environments.

3.1 Availability Credits

Client must log a Severity 1 support ticket with the IBM technical support help desk within 24 hours of first becoming aware that there is a critical business impact and the Cloud Service is not available. Client must reasonably assist IBM with any problem diagnosis and resolution.

A support ticket claim for failure to meet an SLA must be submitted within 3 business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the Cloud Service based on the duration of time during which production system processing for the Cloud Service is not available ("Downtime"). Downtime is measured from the time Client reports the event until

the time the Cloud Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond IBM's control; problems with Client or third party content or technology, designs or instructions; unsupported system configurations and platforms or other Client errors; or Client-caused security incident or Client security testing. IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service during each contracted month, as shown in the table below. The total compensation with respect to any contracted month cannot exceed 10 percent of one twelfth (1/12th) of the annual charge for the Cloud Service.

For bundled Cloud Services (individual Cloud Service offerings packaged and sold together as a single offering for a single combined price), the compensation will be calculated based on the single combined monthly price for the bundled Cloud Service, and not the monthly subscription fee for each individual Cloud Service. Client may only submit claims relating to one individual Cloud Service in a bundle at a given time.

3.2 Service Levels

Availability of the Cloud Service during a contracted month

Availability during a contracted month	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
< 99.8%	2%
< 98.8%	5%
< 95%	10%

* If the Cloud Service was acquired from an IBM Business Partner, the monthly subscription fee will be calculated on the then-current list price for the Cloud Service in effect for the contracted month which is the subject of a claim, discounted at a rate of 50%. IBM will make a rebate directly available to Client.

Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month minus the total number of minutes of Downtime in a contracted month divided by the total number of minutes in the contracted month.

4. Technical Support

Technical support for the Cloud Service is provided via:

- Email
- Telephone
- Live Chat

IBM will make available the IBM Software as a Service Support Handbook which provides technical support contact information and other information and processes. Technical support is offered with the Cloud Service and is not available as a separate offering.

5. Entitlement and Billing Information

5.1 Charge Metrics

The Cloud Service is available under the charge metric specified in the Transaction Document:

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

b. 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 Client's PoE or Transaction Document.

c. Managed Client Device is a unit of measure by which the Cloud Service 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. Client must obtain Managed Client Device entitlements for every Client Device managed by the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.

d. Client Device is a unit of measure by which the Cloud Service 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. Client must obtain entitlements for every Client Device which runs, provides data to, uses services provided by, or otherwise accesses the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.

e. Engagement is a unit of measure by which the services can be obtained. An Engagement consists of professional and/or training services related to the Cloud Service. Sufficient entitlements must be obtained to cover each Engagement.

5.2 Set-Up Charges

A one-time setup fee will be billed at the rate specified in the Transaction Document for each setup service ordered.

5.3 Overage Charges

If actual usage of the Cloud Service during the measurement period exceeds the entitlement specified in the PoE, an overage charge will be billed at the rate specified in the Transaction Document in the month following such overage.

6. Term and Renewal Options

The term of the Cloud Service begins on the date IBM notifies Client of their access to the Cloud Service, as documented in the PoE. The PoE will specify whether the Cloud Service renews automatically, proceeds on a continuous use basis, or terminates at the end of the term.

For automatic renewal, unless Client provides written notice not to renew at least 90 days prior to the term expiration date, the Cloud Service will automatically renew for the term specified in the PoE.

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.

For continuous use, the Cloud Service will continue to be available on a month to month basis until Client provides 90 days written notice of termination. The Cloud Service will remain available to the end of the calendar month after such 90 day period.

7. Additional Terms

7.1 Enabling Software

The Cloud Service requires the use of enabling software that Client downloads to Client systems to facilitate use of the Cloud Service. Client may use enabling software only in connection with use of the Cloud Service.

The following IBM software programs are included as enabling software under the terms of their applicable IBM program licenses, in addition to the limitations below:

a. IBM MaaS360 Cloud Extender

b. IBM MaaS360 Mobile Enterprise Gateway

c. IBM MaaS360 Mobile Device

d. IBM Security Access Manager

- Use Restriction: Client may use IBM Security Access Manager only to proxy connections from mobile devices, managed by this Cloud Service, to enterprise email servers.

7.2 Step up Limitation

For Cloud Service offerings designated as "Step up for existing Customers" ("Step up SaaS"), Client 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, Client who purchases "IBM MobileFirst Protect – Devices (SaaS) Step up for existing customers" must have licensed entitlements to the associated IBM program of IBM MobileFirst Protect. Client's entitlements to the Step up SaaS cannot exceed Client's entitlements to the associated IBM program.

When acquiring Step up SaaS, Client 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 Client has 250 Managed Client Device entitlements to the associated IBM program and chooses to purchase 100 Step up SaaS Managed Client Device entitlements, Client can manage 100 Step up SaaS Managed Client Devices from the Cloud Service environment and 150 Managed Client Devices from the software installed on-premise.

Client 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, Client must maintain current Subscription and Support for the IBM program entitlements used in conjunction with the Step up SaaS entitlements. In the event either Client's license to use the associated IBM program(s) or Client's Subscription and Support for the associated IBM program(s) is terminated, Client's right to use the Step Up SaaS will terminate.

7.3 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 Client or Client's authorized users cannot be identified as the source of the data and so that personally identifiable information allowing identification of Client or Client's authorized users is removed) data reflecting Client's authorized users' individual experiences with the Cloud Services.

7.4 Authorization to Collect and Process Data

The Cloud Service is designed to provision, manage, monitor and control mobile devices. The Cloud Service will collect information from users and devices that are authorized by Client to interact with the Cloud Service for which Client has subscribed. The Cloud Service 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 browsing history from the MaaS360 browser information about end user device hardware, software and settings, and information generated by the device. Client authorizes IBM to collect, process, and use this information in accordance with the terms of this Service Description.

7.5 Data Retention

IBM will delete any collected information, which may include Personal Information, following expiration or termination of this Service Description, except for that which is required to be retained for the purposes set forth above, or by applicable law, rule or regulation. In such case, IBM will retain the collected information for the duration required by such purpose, applicable law, rule or regulation.

7.6 Security Data

As part of the Cloud Service, that includes reporting activities, IBM will prepare and maintain de-identified and/or aggregate information collected from the Cloud Service ("Security Data"). The Security Data will not identify the Client, or an individual except as provided in (d) below. Client herein additionally agrees that IBM may use and/or copy the Security Data only for the following purposes:

a. publishing and/or distributing the Security Data (e.g., in compilations and/or analyses related to cyber security);

b. developing or enhancing products or services;

c. conducting research internally or with third parties; and

d. lawful sharing of confirmed third party perpetrator information.