IBM MaaS360 (SaaS)

This Service Description describes the Cloud Service IBM provides to Client. Client means the company 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 Management Suite (SaaS) and IBM MaaS360 Management Suite (SaaS) Step up for existing IBM MaaS360 customers

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

1.15 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.

1.16 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.

1.17 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.

1.18 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.

1.19 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.

1.20 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.

1.21 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).

1.22 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).

1.23 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 your business quickly, easily, and affordably.

1.24 IBM MaaS360 Laptop Management (SaaS)

Provides Client the ability to enroll, configure, manage, and report on OS X and Windows PC based devices alongside smartphones and tablets. Organizations can maintain consistent security policies and

profiles across both corporate and employee-owned devices within the same MaaS360 management console.

1.24.1 Windows

MaaS360 Laptop Management (SaaS) for Windows-based PCs provides over-the-air enrollment and inventory management reporting on hardware, operating system, and software information. The endpoint security reporting module provides interactive reporting and data analysis for Client provided applications such as anti-virus, backup/recovery, data encryption and personal firewall as well as missing operating system patches. The data protection module provides interactive reporting and analysis for security services, including data encryption, data leak prevention, and backup/recovery, and other integrated applications. Supports Windows XP SP3, Windows Vista, Windows 7, Windows 8+, and Windows 8+ Pro (including 32-bit and 64-bit where applicable).

Device actions include:

- Send message to the device
- Lock the device
- Locate Device (Requires MaaS360 Laptop Location)
- Stop/Start/Restart Services
- Shutdown/Reboot
- Wipe the hard drive
- Configure patch settings
- Distribute software

1.24.2 Mac OS X

MaaS360 Laptop Management (SaaS) for Mac OS X provides over the air enrollment and inventory management reporting on hardware, operating system, and software information. The endpoint security reporting module provides interactive reporting and data analysis for Client provided applications such as anti-virus, backup/recovery, data encryption and personal firewall as well as missing operating system patches. The data protection module provides interactive reporting and analysis for data security services, including data encryption. The configuration management module provides remote management of a number of device and user settings, including: password, email, VPN, and Wi-Fi. Supports Mac OS X version 10.7.3 or higher.

Device actions include:

- Lock the device
- Wipe the hard drive
- Change device policy

1.25 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 MaaS360 Laptop Management (SaaS) for Windows. Supports Windows XP SP3, Windows Vista, Windows 7, Windows 8+, and Windows 8+ Pro (including 32-bit and 64-bit where applicable).

1.26 IBM MaaS360 Laptop Lifecycle Management (SaaS)

Provides the capabilities of the MaaS360 Laptop Management (SaaS) offering and adds the following capabilities:

- Allows Client to upload packages to the MaaS360 Content Service (SaaS) platform and schedule distribution of payload to devices, which are managed by the MaaS360 Laptop Management (SaaS) service for Microsoft Windows. Client controls all aspects of distribution, including installation instructions and targeting at a device, group, or global level. Client is responsible for all packaging and installation file creation. IBM does not provide installation package creation support.

1.27 IBM MaaS360 Laptop Security (SaaS)

Provides organizations the ability to maintain consistent security policies and profiles across both corporate and employee-owned devices within the same management console.

1.28 IBM MaaS360 Essentials Suite (SaaS)

This suite enables Client to view and control the mobile devices and apps entering Client's organization. The suite offers enterprise mobile device, application and expense management from a single screen.

1.29 IBM MaaS360 Deluxe Suite (SaaS)

This suite includes all the capabilities of the MaaS360 Essentials Suite and adds a separate and security-rich office productivity application for users to access and manage their email, calendar, contacts and chat.

1.30 IBM MaaS360 Premier Suite (SaaS)

This suite includes all the capabilities of the MaaS360 Deluxe Suite and adds mobile application security, a secure mobile browser and gateway, and mobile content management

1.31 IBM MaaS360 Enterprise Suite (SaaS)

This suite includes all the capabilities of the MaaS360 Premier Suite and adds mobile threat management, a document editor, and document sync.

2. Security Description

This Cloud Service follows IBM's data security and privacy principles for IBM SaaS which are available at http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp and any additional terms provided in this section. Any change to IBM's data security policies will not degrade the security of the Cloud Service.

This Cloud Service is US-EU Safe Harbor certified.

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 and does not apply to Enabling Software. 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 of an event that has impacted the Cloud Service availability. 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 three 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.

3.2 Service Levels

Availability of the Cloud 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)
Less than 99.8%	2%
Less than 98.8%	5%
Less than 95.0%	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 a contracted month.

Example: 425 minutes total Downtime during contracted month

43,200 total minutes in a 30 day Contracted Month - 425 minutes Downtime = 42,775 minutes _____ 43,200 total minutes	= 2% Availability Credit for 99.0% availability during the contracted month

4. Technical Support

Technical support for the Cloud Service is provided via chat, phone and email.

IBM will make available the IBM Software as a Service Support Handbook which provides technical support contact information, other information and processes.

Severity	Severity Definition
1	Problems or issues with the service that interrupt or prevent the entire customer population from performing regular business operations Problems or issues caused by the service having a catastrophic impact on regular business operations
2	Problems or issues with the service that interrupt or prevent a significant percentage of the customer population from performing regular business operations Problems or issues caused by the service having a major impact on regular business operations.
3	Problems or issues with the service that interrupt or prevent a small percentage of the customer population from performing regular business operations Problems or issues caused by the service having a significant impact on regular business operations
4	Problems or issues with the service that interrupt or prevent an individual user from performing regular business operations Problems or issues caused by the service having a minor impact on regular business operations

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 Cleint'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

5.2 Partial Month Charges

A partial month charge as specified in the Transaction Document may be assessed on a pro-rated basis.

5.3 Overage Charges

If actual usage of the Cloud Service during the measurement period exceeds the entitlement specified in the PoE, Client will be charged for the overage as specified in the Transaction Document

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.

6.1 Automatic Renewal

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.

6.2 Continuous Billing

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. Enabling Software

This Cloud Service includes enabling software, which may be used only in connection with Client's use of the Cloud Service and only for the Cloud Service term.

8. Additional Information

8.1 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.

8.2 Cookies

Client 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

8.3 No Personal Health Information

The Cloud Service is not designed to comply with HIPAA and may not be used for the transmission or storage of any Personal Health Information.

8.4 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.

8.5 Lawful Use and Consent

8.5.1 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.

8.5.2 Informed Consent from Data Subjects

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

Client agrees that Client has obtained or will obtain any fully informed consents, permissions, or licenses necessary to enable lawful use of the Cloud Services and to permit collection and processing of the information by IBM as Client's data processor through the Cloud Service. Client hereby authorizes IBM to obtain fully informed consents necessary to enable lawful use of the Cloud Service 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/.

8.6 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.

8.7 Data Privacy

8.7.1 Cross Border Transfers

If Client makes Personal Information available to IBM Cloud Services in the EU Member States, Iceland, Liechtenstein, Norway, or Switzerland, Turkey, and any other European country that has enacted local data privacy or protection legislation, Client 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:

Name of Processor/Subprocessor	Role (Data Processor or Subprocessor)	Location
IBM Corporation	Sub-processor	1 New Orchard Rd. Armonk, NY 10504, USA I
IBM India Private Limited	Sub-processor	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 India

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

8.7.2 EU Data Privacy

If Client makes personal data available to IBM Cloud Services in the EU Member States, Iceland, Liechtenstein, Norway, or Switzerland, Turkey, and any other European country that has enacted local data privacy or protection legislation, or if Client has authorized users or devices in those countries, then Client as the sole controller appoint IBM as a processor to process (as those terms are defined in EU Directive 95/46/EC) Personal Information. IBM will only process such Personal Information to the extent required to make the IBM Cloud Services offering available in accordance with IBM's published descriptions of IBM Cloud Services and Client agrees that any such processing is in accordance with Client's instructions.

8.8 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.