IBM Trusteer Mobile

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

IBM Trusteer Mobile helps detect real-time device and session risks. It helps maintain the integrity of the application in which it has been embedded by leveraging advanced analytics and real- time device risk detection. Trusteer Mobile assesses the device to determine if it is compromised, such as malware, Remote Access Trojans, jailbroken/rooted detection, overlay attack evidence, and SMS stealing apps. Additional cross-channel indicators are continuously processed, leveraging advanced technologies such as behavioral anomalies, navigation discrepancies, and phishing compromise.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Trusteer Mobile SDK for Business and/or IBM Trusteer Mobile SDK for Retail

IBM Trusteer Mobile SDK Cloud Services are designed to add another layer of protection to provide safe web access onto Client's Business and/or Retail Applications for which Client has subscribed to Cloud Services coverage, devices' risk assessment, and pharming protection. Secure Wi-Fi detection is only available for Android platforms.

IBM Trusteer Mobile SDK Cloud Services include a proprietary mobile software developer's kit ("SDK"), a software package containing documentation, programming proprietary software libraries and other related files and items, known as IBM Trusteer mobile library as well as the "Run-time Component", or "Redistributable", a proprietary code generated by the IBM Trusteer Mobile SDK that can be embedded and integrated into Client's protected standalone iOS or Android mobile applications for which Client has subscribed to Cloud Services coverage. ("Client Integrated Mobile App").

IBM Trusteer Mobile SDK for Retail is available in packs of 100 Eligible Participants or packs of 100 Client Devices, and IBM Trusteer Mobile SDK for Business is available in packs of 10 Eligible Participants or packs of 10 Client Devices.

Through the TMA, the Client (and unlimited number of its authorized personnel) may receive event data reporting and risk trends assessments. IBM Trusteer Pinpoint Detect and IBM Trusteer Pinpoint Verify are used as part of the TMA login. Through the Client Integrated Mobile App, Client can receive risk analysis and mobile device information relating to mobile devices of the Eligible Participants who have downloaded the Client Integrated Mobile App, allowing the Client to formulate a fraud preventive policy enforcing mitigation actions toward these risks. For purpose of this offering, "mobile devices" include only supported mobile phones and tablets and do not include PCs or MACs.

Client can:

a. internally use the IBM Trusteer Mobile SDK solely for the purpose of developing Client Integrated Mobile App;

b. embed the Redistributable (solely in object code format), as an integral, non-separable way in Client Integrated Mobile App. Any modified or merged portion of Redistributable pursuant to this license grant shall be subject to the terms of this Service Description; and

c. market and distribute the Redistributable for download onto mobile devices of Eligible Participants or onto Client Device holder, provided that:

- Except as expressly permitted in this Agreement, Client (1) may not use, copy, modify, or distribute the SDK; (2) may not reverse assemble, reverse compile, or otherwise translate, or reverse engineer the SDK, except as expressly permitted by law without the possibility of contractual waiver; (3) may not sublicense, rent, or lease the SDK; (4) may not remove any copyright or notice files contained in the Redistributable; (5) may not use the same path name as the original Redistributable files/modules; and (6) may not use IBM's, its licensors' or distributors' names or trademarks in connection with the marketing of the Client Integrated Mobile App without IBM's or that licensor's or distributor's prior written consent.

- The Redistributable must remain integrated in a non-separable way within the Client Integrated Mobile App. The Redistributable must be in object code form only and must conform to all directions, instruction and specifications in the SDK and its documentation. The end user license agreement for the Client Integrated Mobile App must notify the end user that the Redistributable may not be i) used for any purpose other than to enable the Client Integrated Mobile App ii) copied (except for backup purposes), iii) further distributed or transferred iv) reverse assembled, reverse compiled, or otherwise translated except as specifically permitted by law and without the possibility of a contractual waiver. Client's license agreement must be at least as protective of IBM as the terms of this Agreement.
- The SDK may only be deployed as part of Client's internal development and unit testing on Client's specified mobile testing devices. Client is not authorized to use the SDK for processing production workloads, simulating production workloads or testing scalability of any code, application or system. Client is not authorized to use any part of the SDK for any other purposes.

Client is solely responsible for development, testing and support of Client Integrated Mobile App. Client is responsible for all technical assistance for Client Integrated Mobile App and for any modifications to the Redistributables made by Client, as permitted herein.

Client is authorized to install and use the Redistributables and the IBM Security Mobile SDK only to support Client's use of the Cloud Services.

IBM does not guarantee that any application or output creating using mobile tools included with the IBM Security Mobile SDK will function, interoperate or be compatible with any specific mobile operating system platform or mobile device.

Source Components and Sample Materials – The IBM Trusteer Mobile SDK may include some components in source code form ("Source Components") and other materials identified as Sample Materials. Client may copy and modify Source Components and Sample Materials for internal use only provided such use is within the limits of the license rights under this Agreement, provided however that Client may not alter or delete any copyright information or notices contained in the Source Components or Sample Materials. IBM provides the Source Components and Sample Materials without obligation of support and "AS IS". Note that the Source Components or Sample Materials are provided solely as an example of how to implement the Embeddable into the CIMA, the Source Components or Sample Materials may not be compatible with Client's development environment, and Client is solely responsible for the testing and the implementation of the Embeddable into its CIMA.

The following provisions in this paragraph apply if the Cloud Services hereunder are provided by an entity other than International Business Machines Corporation, a New York corporation ("IBM Corporation"). The rights to the SDK and Redistributable hereunder are provided by IBM Corporation. IBM is acting as a distributor and delivering the SDK and Redistributable pursuant to this Agreement, and is responsible for enforcing the terms and fulfilling all obligations concerning the SDK and the Redistributable, and no right or cause of action hereunder is related in favor of Client against IBM Corporation. Client waives all claims and causes of action against IBM Corporation and agrees to look solely to IBM for any rights and remedies in connection with the SDK and the Redistributable.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below provide additional data protection information for the Cloud Services and its options regarding the types of Content that may be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. The DPA applies to personal data contained in Content, if and to the extent i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) other data protection laws identified at http://ibm.com/dpa/dpl apply.

It is clarified that the Data Sheets generally list all locations where IBM (including any third party subprocessors) hosts and processes Personal Data, without regard to the data center from which the services are deployed. For a list of hosting and processing locations that are specific to the data center from which the services are deployed, see Section 5.1 below (Additional Processing Location Information).

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Eligible Participant is an individual or entity eligible to participate in any service delivery program managed or tracked by the Cloud Services.
- Client Device is any device that requests or receives execution commands, procedures or applications from a server environment that accesses the Cloud Services.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.

5.1 Additional Processing Location Information

All hosting and processing of Personal Data, including by any third party subprocessors identified in the Data Sheet, will be conducted in the locations specified below:

For all services provided through the Germany data center, IBM will limit hosting and processing of Personal Data to the country of the IBM contracting entity and to the following countries: Germany, Israel, Ireland and The Netherlands.

For all services provided through the Japan data center, IBM will limit hosting and processing of Personal Data to the country of the IBM contracting entity and to the following countries: Japan, Israel and Ireland.

For all services provided through the U.S. data center, IBM will limit hosting and processing of Personal Data to the country of the IBM contracting entity and to the following countries: U.S., Israel, Ireland, Singapore and Australia.

In addition to the abovementioned locations, for all services provided through the Germany, Japan and U.S. data centers, support data may be hosted or processed in Germany and France by Salesforce.Com as a third party subprocessor of IBM.

IBM Trusteer support and account maintenance services may also be provided as needed, based on the availability of relevant IBM personnel, the location of the Client and the data center where the data is hosted.

5.2 Integrated Solutions

For purposes of clarification, the various offerings under the Trusteer brand could constitute an integrated solution. Therefore, if Client terminates any of these Cloud Services, IBM may retain Client data for purposes of providing to Client the remaining Cloud Services under this Service Description as well as other Trusteer services pursuant to the service descriptions applicable to such other Trusteer services.

5.3 Verification

Client will i) maintain, and provide upon request, records, and system tools output, as reasonably necessary for IBM and its independent auditor to verify Client's compliance with the Agreement, and ii) promptly order and pay for required entitlements at IBM's then current rates and for other charges and liabilities determined as a result of such verification, as IBM specifies in an invoice. These compliance verification obligations remain in effect during the term of the Cloud Service and for two years thereafter.

5.4 Data Collected as Part of Deployment

Deployment of the Cloud Service may entail Client providing certain data to IBM. Guidelines on data provided by Client to IBM as part of deployment are included in the Trusteer Deployment Guidelines to be provided to Client.

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content (Insights) or that otherwise identify Client. IBM will however use Content and other information that result from Content (except for Insights) as part of the Cloud Service for the purpose of improving the Cloud Service. IBM may also share threat identifiers and other security information embedded in Content for threat detection and protection purposes.