IBM Cloud Service Description: IBM Security AppScan Mobile Analyzer

The following is the Service Description for your Order:

1. Cloud Service

The Cloud Service offering is described below and is specified in an Order Document for the selected entitled offerings. The Order Document will consist of the provided Quotation and the Proof of Entitlement (PoE) which confirms the start date and term of the Cloud Services. Invoicing will commence following provisioning of the Cloud Service.

1.1 IBM Security AppScan Mobile Analyzer

This service identifies security issues at the code level of Android mobile applications. It allows a developer to scan for security vulnerabilities without the need to supply the application source code. At the end of the scan the service generates a security report that includes details of detected vulnerabilities, the potential security risks to the mobile application caused by these vulnerabilities, with suggestions for how to fix them.

2. Security Description

2.1 Security Policies

IBM has an information security team and also maintains privacy and security policies that are communicated to IBM employees. IBM requires privacy and security training to personnel who support IBM data centers. IBM security policies and standards are reviewed and re-evaluated annually. IBM security incidents are handled in accordance with a comprehensive incident response procedure.

2.2 Access Control

Access to client data, if required, is allowed only by authorized IBM support representatives and service operations personnel according to principles of segregation of duties. IBM staff use two–factor authentication to an intermediate “gateway” management host. All connections are encrypted channels when accessing client data.

2.3 Service Integrity and Availability

Modifications to operating systems and application software are governed by IBM’s change management process. Changes to firewall rules are also governed by the change management process and are reviewed by the IBM security staff before implementation. IBM monitors the data center 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators and third party vendors to help detect and resolve potential system security exposures. Malware detection (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) systems are used in all IBM data centers. IBM’s data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

2.4 Activity Logging

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time to central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to detect anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

2.5 Physical Security

IBM maintains physical security standards designed to restrict unauthorized physical access to IBM data centers. Only limited access points exist into the data centers, which are controlled by two-factor authentication and monitored by surveillance cameras. Access is allowed only to authorized staff that have approved access. Operations staff verifies the approval and issues an access badge granting the necessary access. Employees issued such badges must surrender other access badges and can only possess the data center access badge for the duration of their activity. Usage of badges is logged. Non-IBM visitors are registered upon entering on premises and are escorted when they are on the premises.

Delivery areas and loading docks and other points where unauthorized persons may enter the premises are controlled and isolated.

2.6 Compliance

IBM certifies its privacy practices annually as consistent with the U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement. IBM performs industry standard SSAE 16 audits (or their equivalent) annually in production data centers. IBM reviews security and privacy-related activities for compliance with IBM's business requirements. Assessments and audits are conducted regularly by IBM to confirm compliance with its information security policies. IBM employees and vendor employees complete workforce security and awareness training annually. Personnel are reminded of their job objectives and their responsibility to meet ethical business conduct, confidentiality, and IBM's security obligations annually.

3. Entitlement and Billing Information

3.1 Charge Metrics

The Cloud Service is made available under the following charge metric as specified in the Order Document:

- Application Instance is a unit of measure by which the IBM Saas can be obtained. An Application Instance entitlement is required for each instance of an Application connected to the IBM SaaS. If an Application has multiple components, each of which serves a distinct purpose and/or user base, and each of which can be connected to or managed by the IBM SaaS, each such component is considered a separate Application. Additionally, test, development, staging, and production environments for an Application are each considered to be separate instances of the Application and each must have an entitlement. Multiple Application instances in a single environment are each considered to be separate instances of the Application and each must have an entitlement. Sufficient Entitlements must be obtained to cover the number of Application Instances connected to the IBM SaaS during the measurement period specified in Customer's Proof of Entitlement (PoE) or Transaction Document.

3.2 Charges and Billing

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

3.3 Pay as you Go

Pay as you Go options will be invoiced in the month following when the service is used at the rate specified in the Transaction Document.

4. Technical Support

Technical support for the Cloud Service is available during the subscription period.

Support Hours of Operation are as follows:

Information about hours of availability, online problem reporting systems, and other technical support communication vehicles and processes are described in the IBM Software as a Service Support Handbook.

After Hours Support:

After Hours Support (outside of the regular operating hours stated above) is available only for Severity 1 issues on business days, weekends, and holidays. Severity 1 issues require that the client is available to help diagnose issues during the 24X7 period otherwise, the issue will be downgraded to Severity 2.

4.1 Forum Support

All clients of the Cloud Service are provided forum support which is monitored regularly by IBM support representatives and developers.

a. Ask Questions:

https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. View Current Posts:

https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

4.2 Standard Support

Standard support is available during the period of time in which the client incurs Pay as you Go charges. From within the Cloud Service, clients can submit a support ticket or open a chat session for assistance.

For more information about support procedures, please consult the IBM support web portal at: **https://support.ibmcloud.com** or the IBM SaaS Software Support Handbook at: **ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf**

Severity	Severity Definition	Response Time Objectives	Response Time Coverage
1	**Critical business impact/service down:** Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.	Within 1 hour	24x7
2	**Significant business impact:** A service business feature or function of the service is severely restricted in its use or you are in jeopardy of missing business deadlines.	Within 2 business hours	M-F business hours
3	**Minor business impact:** Indicates the service or functionality is usable and it is not a critical impact on operations.	Within 4 business hours	M-F business hours
4	**Minimal business impact:** An inquiry or non-technical request	Within 1 business day	M-F business hours

5. Safe Harbor Compliance

IBM has not determined compliance of this Cloud Service with the US-EU and US-Swiss Safe Harbor Frameworks.

6. Additional Information

The Cloud Service is designed to identify a variety of potential security and compliance issues in mobile applications and mobile web services. It does not test all vulnerabilities or compliance risks, nor does it act as a barrier to security attacks. Security threats, regulations and standards continually change, and the Service may not reflect all such changes. The security and compliance of Customer's mobile application, systems and employees, and any remedial actions, are Customer's responsibility alone. It is solely within Customer's discretion to use or not use any of the information provided by the Service.

6.1 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) you identify as receiving benefit of the Cloud Services. IBM will apply taxes based upon the business address listed when ordering a Cloud Service as the primary benefit location unless you provide additional information to IBM. You are responsible for keeping such information current and providing any changes to IBM.

6.2 Cookies

You are aware and agree that IBM may, as part of the normal operation and support of the Cloud Service, collect personal information from you (your employees and contractors) related to the use of the Cloud Service through tracking and other technologies. IBM does so to gather usage statistics and information about effectiveness of our Cloud Service for the purpose of improving user experience and/or tailoring interactions with you. You confirm that you will obtain or have obtained consent to allow IBM to process the collected personal information for the above purpose within IBM, other IBM companies and their subcontractors, wherever we and our subcontractors do business, in compliance with applicable law. IBM will comply with requests from your employees and contractors to access, update, correct or delete their collected personal information.