IBM Application Security on Cloud

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, Client 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.

1. IBM SaaS

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

- IBM Application Security Analyzer

2. Charge Metrics

The IBM SaaS is sold under the following charge metrics as specified in the Transaction Document:

a. 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 Client'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 Pay per Use

Pay per Use options will be invoiced in the month following when the service is used at the rate specified in the Transaction Document.

3.2 Partial Month Charge

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

1. Term and Renewal Options

The term of the IBM SaaS begins on the date IBM notifies Client of their access to the IBM SaaS, as documented in the PoE. The PoE will specify whether the IBM SaaS 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 IBM SaaS will automatically renew for the term specified in the PoE.

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

4. Technical Support

During the Subscription Period and after IBM notifies Client that access to the IBM SaaS is available, technical support is provided via online forums and as standard support during the period of time in which

the Client incurs Pay per Use charges. From within IBM SaaS, Clients can submit a support ticket or open a chat session for assistance. IBM will make available the IBM Software as a Service Support Handbook which provides technical support contact information and other information and processes.

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

4.1 Access to Client Data

IBM will be able to access Client data for the purpose of diagnosing issues with the service, and facilitating scans of your application by the service. IBM will access the data only for the purposes of fixing defects or to provide support for IBM products or services.

5. IBM SaaS Offering Additional Terms

Security Scans may not identify all security risks in an application.

The IBM SaaS can be used to help Client meet compliance obligations, which may be based on laws, regulations, standards or practices. Any directions, suggested usage, or guidance provided by the Service does not constitute legal, accounting, or other professional advice, and Client is cautioned to obtain its own legal or other expert counsel. Client is solely responsible for ensuring that Client and Client's activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of this Service does not guarantee compliance with any law, regulation, standard or practice.

The IBM SaaS performs invasive and non-invasive tests on the website and web or mobile application Client chooses to scan, which testing entails certain risks, including without limitation the following:

a. Client's computer systems while running applications under test may hang or crash, resulting in temporary system unavailability or loss of data;

b. the performance and throughput of Client's systems, as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded during testing;

c. excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;

d. data may be changed or deleted as a result of probing vulnerabilities;

e. alarms may be triggered by intrusion detection systems;

f. emails may be triggered by the email function of the web application being tested;

g. the IBM SaaS may intercept the traffic of the monitored network for the purpose of looking for events.

In the event that Client inputs authenticated log-in credentials for the application under test into the Service, Client should only input such credentials for test accounts and not for production users. Use of production user credentials may result in personal data being transmitted via the Service.

The IBM SaaS may be configured to scan production web applications. When Client sets the scan type as "production," the service is designed to perform scans in a manner that reduces the risks listed above; however, in certain situations the IBM SaaS may lead to performance degradation or instability within the

tested production sites and infrastructure. IBM makes no warranties or representations with respect to the suitability of using the IBM SaaS to scan production sites.

IT IS CLIENT'S RESPONSIBILITY TO DETERMINE IF THE SERVICE IS APPROPRIATE OR SAFE FOR CLIENT'S WEBSITE, WEB APPLICATION, MOBILE APPLICATION OR TECHNICAL ENVIRONMENT.

The IBM SaaS is designed to identify a variety of potential security and compliance issues in mobile and web applications and 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 Client's web application, systems and employees, and any remedial actions, are Client's responsibility alone. It is solely within Client's discretion to use or not use any of the information provided by the Service.

Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. CLIENT IS RESPONSIBLE FOR ENSURING THAT CLIENT DOES NOT USE THE SERVICE TO SCAN ANY WEBSITES AND/OR APPLICATIONS OTHER THAN WEBSITES AND/OR APPLICATIONS OWNED BY CLIENT OR THOSE THAT CLIENT HAS THE RIGHT AND AUTHORITY TO SCAN.

5.2 Cookies

Client is aware and agrees that IBM may, as part of the normal operation and support of the IBM SaaS, collect personal information from Client (your employees and contractors) related to the use of the IBM SaaS, through tracking and other technologies. IBM does so to gather usage statistics and information about effectiveness of our IBM SaaS for the purpose of improving user experience and/or tailoring interactions with Client. Client confirms that it 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 Client's employees and contractors to access, update, correct or delete their collected personal information.

5.3 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) Client 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 Client provides additional information to IBM. Client is responsible for keeping such information current and providing any changes to IBM.

Appendix A

1. IBM Application Security on Cloud General Description

IBM Application Security on Cloud provides a single place to assist the Client in identifying security vulnerabilities (such as SQL Injection, Cross-Site Scripting, and Data Leakage) for a variety of applications. The service includes various types of application security scanning techniques, each of which identifies security issues in that application.

IBM Application Security on Cloud provides the following capabilities:

- Scanning Mobile Applications for security vulnerabilities. This is done via dynamic (blackbox) and Interactive (glassbox) security analysis technologies.
- Scanning production or pre-production, publicly facing or on private network, Web sites for security vulnerabilities. This is done via dynamic (blackbox) security analysis techniques.
- Scanning the dataflows within Web and Desktop applications for security vulnerabilities. This is done via static (whitebox) security analysis techniques.
- Detailed security vulnerability reports that include both high-level summaries of the findings and remediation steps that can be followed by developers
- Integration with various DevOps platforms such as Maven and IBM UrbanCode