

Service Description – HCL AppScan on Cloud

This Service Description (“**Service Description**”) describes the HCL AppScan on Cloud (“**HCL AppScan on Cloud**” or “**Service**”). Additional terms governing the HCL AppScan on Cloud is set forth in the either the HCLSoftware Cloud Services Agreement or the Cloud Services Addendum, available at <https://www.hcltechsw.com/wps/portal/resources/master-agreements>, or set forth in the applicable agreement between HCLSoftware and Customer (collectively, “CSA”). This Service Description, any applicable Attachments, Orders, and the CSA are the complete agreement regarding transactions under the CSA (collectively, the "Agreement"). Any capitalized terms used but not defined in this Service Description shall have the meanings given to such terms in the CSA or other applicable documents of the Agreement.

1 HCL AppScan on Cloud

HCL AppScan on Cloud includes various types of application security scanning techniques, each of which identifies security issues in that application.

HCL AppScan on Cloud provides the following capabilities:

- Scanning production or pre-production, publicly facing or on private network, Websites and Web services for security vulnerabilities using Dynamic Analysis Security Testing.
- Scanning the code within Web, Mobile, and Desktop applications for security vulnerabilities using Static Analysis Security Testing.
- Analyzing Web applications and Web services while they are being executed to detect security vulnerabilities using Interactive Application Security Testing.
- Identifying vulnerable Open Source packages used in an application using Software Composition Analysis.
- 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.

Customer may subscribe to one or more of the following available offerings:

HCL AppScan DAST Analyzer (“Dynamic Analyzer”)

HCL AppScan DAST Analyzer tests pre-production or production websites. HCL AppScan DAST can be ordered per Application Instance, per Job (scan), or per Concurrent Event (scan) as defined in section 1.4.

HCL AppScan Static Analyzer (“SAST”)

HCL AppScan SAST tests byte or source code of the application. HCL AppScan SAST can be ordered per Application Instance, per Job (scan), or per Concurrent Event (scan).

HCL Interactive Analyzer (“IAST”)

HCL AppScan IAST identifies security vulnerabilities in running Web applications and Web services. An IAST agent instruments the application to passively monitor its behavior while it is being interacted with and report the identified vulnerabilities to HCL AppScan on Cloud. HCL AppScan IAST can be ordered per Application Instance or per Concurrent Event (session).

HCL AppScan Software Composition Analysis (“SCA”)

HCL AppScan SCA discovers and identifies open source packages used in application code. It reviews these packages for vulnerabilities and provides remediation advice. HCL AppScan SCA can be ordered per Application Instance, per Job (scan), or per Concurrent Event (scan)

Details on each AppScan on Cloud subscription type are provided in Table 1.3.1 below.

1.1 HCLSoftware AppScan on Cloud (Software as a Service - SaaS): HCLSoftware will provision, operate and maintain HCLSoftware AppScan on Cloud which consists of the following:

- Setup and configuration of the service
- Online service management tooling
- Provision of tooling for customer premises (optional)
- Service Level Agreement (SLA)
- Support services
- Infrastructure and application health monitoring
- Security monitoring, scanning and remediation
- Infrastructure/software maintenance, upgrades and updates
- Incidents management and remediation
- Backup of the data in real-time and with geo-redundancy
- Business Continuity and Disaster Recovery

1.2 HCLSoftware Infrastructure Capacity

HCL AppScan on Cloud can scale on-demand. The maximum amount of these resources a Customer can have, use or consume will be listed in the Order Schedule. If thresholds are exceeded, HCLSoftware reserves the right to charge for the excess consumption at HCLSoftware's current list price.

1.3 HCL AppScan on Cloud Usage Metrics (or Charge Metrics)

The following charge metrics apply to this Cloud Service:

- **Application Instance** means one (1) Project or ten (10) Microservices.
- **Project** means a single codebase which is maintained over time and used to build a particular named software module or application.
- **Microservice** means a single codebase up to twenty thousand (20,000) lines of code that is independently deployable with well-defined interfaces and operations, which is part of a suite of modular components or services and supports a specific task or a business goal.
- **Concurrent Events** is the total number of simultaneous occurrences of a specific event that is processed by or related to the use of the Cloud Service.
- **Job** is an object within the Cloud Service that cannot be further divided and represents a computing process including all its sub-processes managed or processed by the Cloud Service. Sufficient entitlements must be obtained to cover the total number of Jobs which are processed or managed by the Cloud Service during the measurement period specified in the Order or other applicable Attachment.

For this Cloud Service, Application Instances are consecutive scans of a single application further defined as follows:

- For Dynamic Testing: a Website or Web service addressable via public or private URL. Each Application Instance entitles a site of up to five thousand (5,000) pages in a single domain.
- For Static Testing: a unit of code built for a single executable environment. Each Application Instance entitles scanning units of code up to one million (1,000,000) lines.
- For Interactive Testing: a Website or Web service addressable via public or private URL.

- For Software Composition Analysis: a unit of code built for a single executable environment. Each Application Instance entitles scanning units of code up to one million (1,000,000) lines.
- Distinct deployments of an Application Instance in multiple environments (such as test, development, staging or production) or multiple instances of an application within a single environment (Java Application Server, for example) are considered separate Application Instances.

1.3.1 AppScan on Cloud Subscriptions

HCL AppScan per Job (Scan)	
Subscription Type	Description
Application Security Analyzer Per Scan (Pay per scan)	Provides a single scan (which shall be considered a Job) of an application using any of these scanning technologies (SAST, DAST, SCA). Purchased scans must be utilized within twelve (12) months from the purchase date, after which time they expire without refund. No time limit per scan; scans will run to completion.
HCL AppScan per Application Instance	
Subscription Type	Description
HCL AppScan on Cloud Analyzer per Application Instance (Pay per application)	Annual subscription providing unlimited scanning of one (1) application ("Application Instance") using either of these scanning technologies (SAST or DAST) which are appropriate based on the application. Limit to only one (1) running Job at a time of each technology (SAST, DAST) under an Application Instance
HCL AppScan on Cloud Interactive Application Security Testing (IAST) per Application Instance (IAST pay per application)	Annual subscription providing unlimited IAST scanning of one (1) application ("Application Instance"). Limit to only one (1) running IAST Job at a time under an Application Instance
HCL AppScan on Cloud Software Composition Analysis per Application Instance (SCA pay per application)	Annual subscription providing unlimited SCA scanning of one (1) application ("Application Instance"). Limit to only one (1) running Job at a time under an Application Instance
HCL AppScan Concurrent Pricing Options	
HCL AppScan on Cloud's concurrent pricing options allow organizations to create unlimited application workspaces and run an unlimited number of scans or IAST sessions. The number of scans or IAST sessions that can be simultaneously executed is limited by the number of "concurrent events" entitlements purchased.	
Subscription Type	Description
HCL AppScan on Cloud Silver (ASoC_Silver)	Annual subscription providing scanning of any number of applications using a single technology choice from SAST, DAST, SCA, or IAST. The choice of technology is set for the duration of the subscription and subsequent renewals

	Limit to one (1) running Job(scan) for each one (1) entitlement for SAST, DAST or SCA. Limit to five (5) running Jobs(sessions) for each one (1) entitlement for IAST.
HCL AppScan on Cloud Gold (ASoC_Gold)	Annual subscription providing scanning of any number of applications using two technologies. (Any selected two of SAST, DAST, SCA, or IAST.) The choice of technologies is set for the duration of the subscription and renewals. Each of the technologies will be able to run scans or sessions as listed below. Limit to one (1) running Job(scan) for each one (1) entitlement for each for SAST, DAST, or SCA. Limit to five (5) running Jobs(sessions) for each one (1) entitlement for IAST.
HCL AppScan on Cloud Platinum (ASoC_Platinum)	Annual subscription providing scanning of any number of applications using any technology SAST, DAST, SCA, or IAST. Each of the technologies will be able to run scans or sessions as listed below. Limit to one (1) running Job(scan) for each one (1) entitlement for each for SAST, DAST, or SCA. Limit to five (5) running Jobs(sessions) for each one (1) entitlement for IAST.

1.4.2 AppScan on Cloud limits the quantity of retained scan jobs under an AppScan on Cloud application workspace to a maximum of two thousand (2000) per application workspace. AppScan on Cloud provides optional functionality to automatically remove scan jobs in excess of the maximum 2000, commencing with the oldest first.

2 Service Features – HCL AppScan on Cloud

2.1 Environments

The Service provides the functional infrastructure for running the software for which HCLSoftware provides the support and necessary network, hardware, and system patches. As part of the Service, HCLSoftware provides some or all of the following environments based on the Service as specified in the Order Schedule.

2.1.1 Production Environment

The final resting point for all "Run" software in the Service lifecycle management. The production environment ("Production Environment") comprises the Application, systems, and supporting systems infrastructure, that the end users and the Customers of an organization access and use on an operational basis to execute its business processes and transactions. Administrative access to this system is restricted to HCLSoftware personnel.

2.2 Backup and Restore

As part of the base Service, HCLSoftware perform data backups and test data restoration for Business Continuity / Disaster Recovery.

2.3 Service Integration

The following capabilities are provided as part of the Service. Only secure transmission protocols and methods are allowed.

- HCL AppScan on Cloud customer facing API

2.4 Network Integration

The following are the supported methods for integrating with Customer networks. Only secure transmission protocols and methods are allowed. Such supported methods apply solely to HCLSoftware integrations and not to customer-side network integrations. Customer is responsible for its internet connection.

- Access to the AppScan on Cloud Portal and AppScan on Cloud APIs is over HTTPS.
- Customers should refer to the [AppScan on Cloud System Requirements](#) for the allowed list of IP ranges or domains for proper functioning of the cloud service from the Customer's network.
- Performing Dynamic Analysis (DAST) scanning of targets within the customer's private network require the customer to install the AppScan Presence utility to enable the secure network connection between AppScan on Cloud and the tested targets (web applications, APIs or microservices).

2.5 Security Features and Responsibilities

Security monitoring and incident response is provided by 24/7 365 Security Operations Center. HCL AppScan on Cloud also implements the following security features:

- Data encryption in transit - The Service contents using the most current, stable and secure encryption protocols during data transmission between the cloud infrastructure and the endpoint networks . Customer is responsible for ensuring the feasibility of encryption protocols in the endpoint networks.
- Data encryption at rest – HCL AppScan on Cloud's data is fully encrypted at rest. All the passwords on all the files are encrypted. Other files are secured using the disk encryption of cloud provider.
- Anti-Virus & Malware Protection - Next generation anti-virus and malware software is installed and managed on HCLSoftware managed operating system software.
- Firewall - HCLSoftware applies network and application policies to restrict all unnecessary and unauthorized access to the service environments.
- Two-factor authentication is required for HCLSoftwareSoftware authorized personnel who retain access to the service environments. HCLSoftware performs proactive monitoring and management for two-factor authentication alerts for the Service.
- Network Based Intrusion Detection & Prevention - HCL implements network-based intrusion prevention, monitors the systems, responds to intrusion detection alerts and performs event correlation.
- File Integrity Monitoring - HCLSoftware implements file integrity monitoring by validating the integrity of operating system and Application software files using an automated verification method.

2.6 Disaster Recovery

In the event of an HCLSoftware declared Disaster, HCL will activate its procedures to recover the AppScan on Cloud service as soon as possible. HCL AppScan on Cloud data is backed up continuously and securely with multi-region

backup service to minimize data loss. HCLSoftware will maintain communication with Customer regarding the status and estimation for the recovery timeline.

2.7 Clock Synchronization

All clocks for all servers of this Service are synchronized to the primary time source provided by the cloud provider.

3 Service Features

3.1 Service Level Agreement ("SLA")

HCLSoftware provides the following availability service level agreement ("SLA") for the Service. The SLA is not a warranty and is Customer's sole and exclusive remedy. The SLA is available only to Customer and applies only to use in Production Environments.

3.1.1 Service Levels

Availability of the Service during a contracted month:

Availability during a contracted month	Compensation (% of monthly Service fee* for contracted month that is the subject of a claim)
Less than 99.9%	2%
Less than 99%	5%
Less than 95%	10%

*The service credit will be applied to the Customer invoice.

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

3.1.2 Availability Credits

Customer must log a Priority 1 support ticket with the HCLSoftware 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. Customer must reasonably assist HCLSoftware with any problem diagnosis and resolution.

An HCLSoftware support case 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 Service based on the duration of time during which Production Environment processing for the Service is not available ("Downtime"). Downtime is measured from the time Customer reports the event or external monitors report service unavailability, until the time the Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond HCLSoftware's or the selected Cloud Platform provider's control; problems with Customer or third-party content or technology, designs or instructions; unsupported system configurations and platforms or other Customer errors; or Customer-caused security incident or Customer security testing. HCLSoftware will apply the highest applicable compensation based on the cumulative availability of the 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 Service. 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.

3.2 Service Support

English language support is provided for the Service by the HCLSoftware Support team. Incidents are categorized using Priority levels as described below:

3.2.1 Priority Definition, Response Time, Coverage

Priority	Priority Definition	Response Time Objectives	Response Time Coverage
P1 (Critical)	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 15 minutes	24/7
P2 (High)	Significant business impact: A service business feature or function of the service is severely restricted in its use or Customer is in jeopardy of missing business deadlines.	Within 1 hour	24/7
P3 (Moderate)	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
P4 (Low)	Minimal business impact: An inquiry or non-technical request.	Within 1 business day	M-F business hours

Technical support for the products hosted shall be as set forth in the HCLSoftware Support Guide located at:

https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0010420.

- Customer will ensure that a resource is assigned to work with HCLSoftware to provide information or verification on an ongoing basis, until the issue is resolved.
- In the event of multiple reported Errors being worked concurrently, unless otherwise requested by Customer, HCLSoftware will prioritize based on Priority starting with Critical (P1) and then on the time the Error was reported starting with the oldest. The response time will apply to the top two Errors being worked based on this Priority.
- In the event HCLSoftware response time to an Error is negatively impacted due to Customer's delayed response to HCLSoftware request for additional information to correct an Error, the response times provided above will be extended by an amount of time proportionate to such delay.
- Both parties may agree that due to technical dependencies and other factors, certain Errors classified as Moderate and Low may be resolved in an appropriate scheduled maintenance window. Customer acknowledges that HCLSoftware does not and cannot guarantee that all Errors can or will be corrected.
- System changes for upgrades or patches will be applied during Scheduled Maintenance or as available where there will be no disruption to the Service unless the change is required to restore system availability.
- Business Days are Monday through Friday excluding national Holidays of the country from where the service is provided.

3.3 HCLSoftwareHCLSoftwareProvisioning of Environments

The HCLSoftware Order Acknowledgement and Proof of Entitlement will include instructions on how the Customer registers their organization on the HCLSoftware AppScan on Cloud regional service of their choice. The Customers organization will be provisioned upon registration.

3.4 Environment Updates

3.4.1 Software Versions

The Service is based on the generally-available HCLSoftware AppScan on Cloud ("HCLSoftware AppScan on Cloud") software. Support for the Service is available while the Customer maintains an active subscription according to the HCLSoftwareSoftware support lifecycle policy.

3.4.2 Maintenance Windows

HCLSoftware's standard weekly maintenance windows are currently scheduled for the Service. These maintenance windows do not necessarily mean the Services will be down or unavailable and Service disruptions will be minimized for HCLSoftware activities. HCLSoftware will notify the Customer if the Services will not be available during the maintenance windows.

Other scheduled and non-scheduled (emergency) down times may occur and Customer will be notified of the Services being unavailable at least five (5) business days in advance unless the vulnerability, risk of loss or Service integrity is deemed by HCLSoftware to be too high.

3.4.3 Deployment of HCLSoftware-Initiated Updates

HCLSoftware performs the required maintenance and updates of the Service which includes implementing infrastructure patches, Security Patches, and new versions (collectively, "HCLSoftware-Initiated Updates").

HCLSoftware-Initiated Updates are performed on a routine basis or during scheduled maintenance windows. Scheduled maintenance is announced at least five business days in advance or maintenance determined by HCLSoftware to be an emergency upon notice provided to a customer ("Scheduled Maintenance"). Scheduled maintenance windows are excluded from SLA calculations and remedies.

4 Term and Renewal Options

The term of the Service begins on the date HCLSoftware notifies Customer of their access to the Service, as documented in the Order Schedule.

For renewal, the Customer must renew the term specified in the Order Schedule prior to the term expiration date to ensure uninterrupted Service.

5 Additional Terms

5.1 Security, Compliance Standards and Data Protection

HCLSoftware certifications for the Service are available at: <https://www.hcltechsw.com/legal/compliance>.

5.2 Data Protection

Customer is aware and agrees that HCL may, as part of the normal operation and support of HCL AppScan on Cloud, collect personal data from Customer (Customer's employees and contractors) related to the use of HCL AppScan on Cloud, through tracking and other technologies. HCLSoftware does so to gather usage statistics and information about effectiveness of HCL AppScan on Cloud for the purpose of improving Customer's user experience and/or tailoring

interactions with Customer. Customer confirms that it will obtain or has obtained consent to allow HCLSoftware to process the collected personal data for the above purpose within HCLSoftware, other HCLSoftware affiliates and their subcontractors, wherever HCLSoftware and such subcontractors do business, in compliance with applicable law. Customer data that does not contain personal data may also be used by HCLSoftware to improve its products and services. HCLSoftware will work with Customer to respond to valid requests from Customer's employees and contractors to access, update, correct or delete their personal data.

Customer acknowledges that its use of any personal data in HCL AppScan on shall be as a data controller and that it is Customer's responsibility to comply with all applicable laws or regulations, including but not limited to the European Union's General Data Protection Regulation 2016/679 ("GDPR"), regarding the use of PII. This includes ensuring proper configurations and settings, if applicable, in HCL AppScan on when collecting, tracking, storing or otherwise processing personal data .

PII processed by HCLSoftware as a data processor will be processed in accordance with the terms and conditions of the CSA including, if applicable, the HCLSoftware Data Processing Agreement located [here](https://www.hcltechsw.com/resources/master-agreements) or found on the HCLSoftware Master Agreements page here: <https://www.hcltechsw.com/resources/master-agreements>.

6 Definitions

Application – refers to the HCLSoftware products that provide the base functionality for the Service, including the original and all whole or partial copies: 1) machine-readable instructions and data, 2) components, 3) audio-visual content (such as images, text, recordings, or pictures), 4) related licensed materials, and 5) license use documents or keys, and documentation, which are provided by HCLSoftware and which Customer may access through the Service.

Container – a Docker container that contains HCL AppScan on Application functionality.

Disaster – is a natural or human-induced event which disrupts the operations of vital technology infrastructure and systems creating a complex or irreversible disruption to the Service.

Disaster Recovery (DR) – actions taken by the HCLSoftware Managed Service team to recover from a Disaster back to operational state.

Environment – refers to a deployable instance of the Application, including the infrastructure necessary to support that Application for its intended use, and refers to the Integration Environment, Development/Test Environment, Pre-Production Environment, Non-Production or Production Environment, as the context requires.

Extensions (also known as Customizations) – are the software artifacts and configuration provided by the Customer, or their authorized third party, to extend the Service by implementing the Customer's business process flow, manage specific data needs, and provide Customer specific branding, in support of the Customer's business requirements. This can be, but not limited to, software code, software assets, plug-ins, customizations, database extensions, scripts or files created to customize Customer's utilization of the Service, including Integrations to Third Party Services or data sources. Extensions are the responsibility of the Customer.

Gigabyte (GB) – a unit of measure for network traffic or storage.

Go-Live – is the activation of the Production Environment Site for use by the Customer for normal business activities and/or use by the Customer in servicing, in anyway, their customers and/or use by the Customer in support of revenue generation.

Payment Card Industry (PCI) Account Data – is the cardholder account information contained on a payment card, or associated with a payment card transaction, including major debit, credit, prepaid, e-purse, ATM, POS cards, including Cardholder Data (CHD) and Sensitive Account Data (SAD) subject to security and handling guidelines set by the Payment Card Industry Data Security Standard (PCI DSS).

Personally Identifiable Information (PII) – is any information which relates to an identified or identifiable individual.

Recovery Point Objective – is the maximum tolerable period in which data might be lost from an IT service due to a Disaster.

Recovery Time Objective – is the targeted duration of time, and a service level, within which a business process must be restored after a Disaster is declared in order to avoid unacceptable consequences associated with a break in business continuity.

Security Patch – is a fix for a security-related vulnerability that affects the Application.

Terabyte (TB) – a unit of measure for network traffic or storage.

Third-Party Services – are third party data services, databases, web services, software, or other third-party content accessed via the Service.

Upgrade – is a new version or release of the base Application that replaces an earlier version or release, and typically includes new features and functions.

7 Enabling Software

The Service may require the use of enabling software that Customer downloads to Customer systems to facilitate use of the Service. Customer may use enabling software listed below solely in connection with use of the Service. An exception applies if the enabling software is also licensed independently. The following enabling software will be provided to Customer and use is subject to the terms of the CSA and this Service Description:

AppScan Standard
AppScan GO!
AppScan Cloud CLI
AppScan Activity Recorder
AppScan Traffic Recorder
SAST Client Util/CLI

The above mentioned enabling softwares will be added at Application Client Tools Section - https://help.hcl-software.com/appscan/ASoC/appseccloud_plugins_integrations.html This section will be updated periodically as and when required.

8. HCL AppScan on Cloud Additional Terms

8.1 Security Scans

Security scans may not identify all security risks in an application, nor are they designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life support systems, nuclear facilities, or any other applications in which failure to identify security risks could lead to death, personal injury, or property damage. Security scans are not warranted to operate uninterrupted or error free.

The HCL AppScan on Cloud can be used to help Customer 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 Customer is cautioned to obtain its own legal or other expert counsel. Customer is solely responsible for ensuring that Customer and Customer'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 HCL AppScan on Cloud performs invasive and non-invasive tests on the Website and Web or mobile application Customer chooses to scan. Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. Customer authorizes HCLSoftware to perform the Services as described herein and acknowledges that the Services constitute authorized access to Customer's computer systems. HCLSoftware may disclose this grant of authority to a

third party if deemed necessary to perform the Services. The testing entails certain risks, including without limitation the following:

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

- the performance and throughput of Customer's systems, as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded during testing;
- excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;
- data may be changed or deleted as a result of probing vulnerabilities;
- alarms may be triggered by intrusion detection systems;
- emails may be triggered by the email function of the Web application being tested;
- the HCL AppScan on Cloud may intercept the traffic of the monitored network for the purpose of looking for events.

Any service level agreement rights or remedies provided by HCLSoftware and relating to the Websites or applications subject to testing will be waived during any testing activity.

In the event that Customer inputs authenticated log-in credentials for the application under test into the Service, Customer 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 HCL AppScan on Cloud may be configured to scan production Web applications. When Customer 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 HCL AppScan on Cloud may lead to performance degradation or instability within the tested production sites and infrastructure. HCLSoftware makes no warranties or representations with respect to the suitability of using the HCL AppScan on Cloud to scan production sites.

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

The HCL AppScan on Cloud 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 Customer's Web 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.

Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. CUSTOMER IS RESPONSIBLE FOR ENSURING THAT CUSTOMER DOES NOT USE THE SERVICE TO SCAN ANY WEBSITES AND/OR APPLICATIONS OTHER THAN WEBSITES AND/OR APPLICATIONS OWNED BY CUSTOMER OR THOSE THAT CUSTOMER HAS THE RIGHT AND AUTHORITY TO SCAN. IT IS THE SOLE RESPONSIBILITY OF THE CUSTOMER TO CONFIRM THEY ARE PERMITTED TO PERFORM SCANNING AGAINST APPLICATIONS RUNNING ON THIRD-PARTY INFRASTRUCTURE OR SERVICE.

For the purpose of clarity, Customer Content described in the Data Protection section of the CSA is also deemed to include data that may become accessible to HCLSoftware during Application Security Testing.

As part of the HCL AppScan on Cloud, that includes reporting activities, HCLSoftware will prepare and maintain de-identified and aggregate information collected from HCL AppScan on Cloud (called "Security Data"). The Security Data

will not identify Customer, or an individual except as provided herein. Customer herein additionally agrees that HCLSoftware may use and/or copy the Security Data only for the following purposes:

- publishing and/or distributing the Security Data (e.g., in compilations and/or analyses related to cybersecurity);
- developing or enhancing products or services;
- conducting research internally or with third parties; and
- lawful sharing of confirmed third party perpetrator information.