verizon

SECURITY SAAS – WHITEHAT SENTINEL SERVICE +

Part I: Rates and Charges.
Part II: Service Description and Requirements.
Part III: Service Terms and Conditions.
Part IV: Definitions.

Part I: Rates and Charges. This service attachment describes the terms and conditions for the WhiteHat Sentinel Service ("WhiteHat Sentinel") or WhiteHat Sentinel Source. WhiteHat Sentinel and WhiteHat Sentinel Source are collectively referred to herein as "WhiteHat Sentinel +". Customer will pay the annual recurring charge ("ARC") shown in the Customer's Contract, based upon the quantity of (1) Web Applications, in the case of WhiteHat Sentinel or (2) Source Code Branches, in the case of WhiteHat Sentinel Source. "Web Application" means a group of Host Names and one set of User Credentials (as defined below) and "Source Code Branch" means one or more branches of an application codebase (preferably the actively developed "trunk/master/head") (collectively referred to herein as "Customer Materials" where applicable). Customer will be invoiced the ARC upon the Service Activation Date which is the RFS date as defined below. Verizon reserves the right to change the ARC for additional orders beyond the initial order, including increases in the quantity of Customer Materials. Verizon may also charge applicable non-recurring charges ("NRC") for such additional orders, and NRC at the following URL: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm.

1. **Service Commitment.** The Service Commitment for WhiteHat Sentinel Service is shown in the Contract. The minimum Service Commitment is 12 months. WhiteHat Sentinel Services are offered on a subscription basis. Customer may order additional subscriptions at any time and each order will have its own Service Commitment, and be billed at Verizon's then-current rates. Unless Verizon or Customer provides notice of termination of all or part of an order 45 days prior to the expiration of a Service Commitment, each order will automatically renew for a minimum period of 12 months (and will be considered a new order). Verizon reserves the right to change the ARC to be effective at the beginning of a new Service Commitment with 60 days' notice prior to the expiration of the then current Service Commitment. If: (a) Customer terminates any WhiteHat Sentinel Service or any subscription before the end of the relevant Service Commitment for reasons other than Cause; or (b) Verizon terminates any WhiteHat Sentinel Service for Cause, then Customer will pay an amount equal to the relevant ARC for the terminated subscriptions remaining during the relevant Service Commitment or Service Commitments.

Part II: Service Description and Requirements.

1. **Service Description.**
   - 1.1 **WhiteHat Sentinel.** WhiteHat Sentinel is a web-based application service that i) allows Customer to scan Web Applications, as defined below, located on Customer's external and internal networks for vulnerabilities and ii) provides information that will help Customer to remediate those vulnerabilities. Verizon will provide WhiteHat Sentinel upon Customer's order. WhiteHat Sentinel does not require Customer to install any software or hardware to scan Web Applications located on external networks. Access to WhiteHat Sentinel is provided via the online End User Management Console portal. The End User Management Console allows Customer to configure and schedule the date and time of Web Application vulnerability scans, review the results of vulnerabilities discovered, read more information about these vulnerabilities, and generate reports about the findings.
     - 1.1.1 **Levels of Service.** WhiteHat Sentinel is offered at the level(s) of service listed below. Each level of service offers unlimited scans along with security engineer verification of all vulnerabilities.
       - 1.1.1.1 **Sentinel – Premium Edition ("Sentinel-PE").** Sentinel-PE tests for technical and business logic website security vulnerabilities detected by the WhiteHat Sentinel Service and identified by the vulnerability classification guide on the End User Management Console ("Security Vulnerabilities"). Sentinel-PE includes security engineer custom scan configuration and custom testing to identify business logic vulnerabilities. This custom testing includes manual review by security engineers to test, for example, account structures and the contextual logic in Web Applications.
       - 1.1.1.2 **Sentinel – Standard Edition ("Sentinel-SE")**. Sentinel-SE can test Web Applications with complex functionality such as multiple forms and login points. Sentinel-SE includes custom scan configuration and custom testing for web forms and templates. Sentinel-SE only tests for technical website Security Vulnerabilities.
       - 1.1.1.3 **Sentinel – Baseline Edition ("Sentinel-BE").** Sentinel-BE tests Web Applications that are seasonal or temporary in nature and have limited functionality. Sentinel-BE tests for technical website Security Vulnerabilities. Sentinel-BE does not i) provide any custom

scan configurations or testing, ii) test form templates for vulnerabilities, nor iii) provide a mechanism to automatically or manually complete Web Application forms for testing.

1.1.1.4 **Sentinel – Enterprise Baseline ("Enterprise-BE").** Enterprise-BE discovers production websites, analyzes them for security risks, and assesses each site for vulnerabilities. Assessments are performed on a continuous basis, for an unlimited number of times, and identify vulnerabilities listed on the Web Application Security Consortium (WASC) and Open Web Application Security Project (OWASP) Top 10. This services covers up to 200 designated Web Applications.

1.1.1.5 **Sentinel – Pre-Launch ("Sentinel-PL").** Sentinel PL is a completely automated scanning solution designed for quality assurance or staging websites. Sentinel-PL scans for the same vulnerabilities as Sentinel-SE with the following differences: i) forms are tested automatically without any configuration, ii) tests and speed of the scan are more aggressive that should not be used for production sites but can be used for testing quality assurance or staging sites, iii) the End User Management Console user interface has user-configurable options for customizing Sentinel-PL scans to focus on certain vulnerabilities, certain sections of the site, or to include/exclude certain URLs or URL patterns, iv) Sentinel-PL requires a virtual appliance (the Sentinel VM Satellite Appliance) to provide communication between the scanning engine and the Threat Research Center that validates the vulnerabilities found by the engine. All vulnerabilities are verified by WhiteHat.

1.1.1.6 **Sentinel Pre-Launch Enterprise Edition**. Sentinel Pre-Launch Enterprise Edition includes all of the features of Sentinel-PL as well as the ability to replace or substitute the host names comprising the Web Applications with different host names during the Service Commitment. The host name changes may be initiated at any time. When a host name is replaced for a Web Application, all historical vulnerability data for the Web Application comprised of the replaced host names will no longer be available to Customer, and it is Customer's responsibility to download any necessary data and/or reports prior to replacing any host names.

1.2 **Sentinel Source**. WhiteHat Sentinel Source is an application that allows Customer to test the security of application software coding throughout the software development lifecycle ("SDLC"). The Service utilizes the Sentinel Source Satellite Virtual Machine ("VM") appliance to test Customer's source code within Customer's own environment. The VM provides a secure communication mechanism from the source code engine that is integrated with the source code repository, with the WhiteHat Threat Research Center ("TRC"). The VM transmits information regarding potential vulnerabilities in the code to the TRC for validation. This detection of vulnerabilities within software code under development enables Customer to identify and remediate problems early in the SDLC. Verizon will provide WhiteHat Sentinel Source upon Customer's order.

1.2.1 **Levels of Service.** WhiteHat Sentinel Source is offered at the level(s) of service listed below. Each level of service offers unlimited scans along with security engineer verification of all vulnerabilities.

1.2.1.1 **Sentinel Source Single Branch.** Single Branch allows Customer to conduct vulnerability scanning on a single Source Code Branch.

1.2.1.2 **Sentinel Source Multiple Branch.** Multiple Branch allows Customer to conduct vulnerability scanning on multiple Source Code Branches.

1.3 **Sentinel Computer Based Training.** WhiteHat Security Computer Based Training ("CBT") is a computer-based training course designed to help developers remediate vulnerabilities identified during WhiteHat Sentinel assessments. WhiteHat CBT provides training with in-depth coverage for risks in the OWASP Top 10 and provides remediation examples in the most popular languages. WhiteHat CBT is web-based and can be accessed from from any web browser; 24 x 7 x 365. WhiteHat CBT does not require equipment installation, and integrates with the Customer's sharable content object reference model (SCORM) - compliant learning management systems (LMS)**.** User access is unlimited for each Customer. Pricing is offered on a per user basis, subject to an annual subscription.

1.4 **Standard Features.**

1.4.1 **WhiteHat Sentinel Scan Management.** For WhiteHat Sentinel, Customer can create and configure vulnerability scanning schedules as required. Customer can initiate a manual scan or establish automatic scan schedules to execute scans daily or weekly. As vulnerabilities are identified, they are classified into vulnerability classes, e.g. cross-site scripting, directory traversal, or SQL injection. The website Security Vulnerabilities lists both business logic vulnerabilities and technical vulnerabilities. When scans are executed, security engineers verify each vulnerability for false positives before it is displayed in the End User Management Console.

1.4.2 **WhiteHat Sentinel Web Application.** WhiteHat Sentinel detects website Security Vulnerabilities in Web Applications. A "Host Name" means an identifying domain name assigned to a host

computer, usually a combination of the host's local name (e.g. www, www2, or mail) with its parent domain's name (e.g. example.com to create www.example.com, www2.example.com, or mail.example.com). "User Credentials" means a pair of any user credentials (e.g., logon ID, password, or PIN) required to access a role or level of functionality for a Host Name. This means that if a Host Name is accessible with multiple roles or levels (e.g., user, supervisor, or administrator), then User Credentials refers to pairs of user credentials for each role or level applicable to such Host Name.

1.4.3 **WhiteHat Sentinel Source Code Testing.** WhiteHat Sentinel Source is a subscription-based Static Application Security Testing solution that directly inspects source code for vulnerabilities. WhiteHat Sentinel Source allows developers to begin scanning their Source Code Branch(es) for vulnerabilities from the first line of code, without having to wait until the application is complete. WhiteHat Sentinel Source integrates with an end user's source code repository and gives developers accurate vulnerability data, which enables them to assess and fix code continuously throughout the SDLC. WhiteHat Sentinel Source includes verification of all vulnerabilities via the WhiteHat TRC.

1.4.4 **End User Management Console.** Customer interacts with and manages the WhiteHat Sentinel Service via the End User Management Console. The End User Management Console is an on-line, Internet accessible portal that is available 24 hours per day and seven days per week, except during maintenance windows. Customer is responsible to identify to Verizon the users who will have access to the End User Management Console.

The End User Management Console has six main functions:

- Summary: An overview of the security status of Customer Materials (shown as a "site" on the console)
- Findings: A list of vulnerabilities discovered by the scans
- Schedule: The ability to schedule, view and manage scan events
- Reports: A criteria input page to generate and print vulnerability reports
- Resources: A collection of white papers, a glossary, and help references
- Account: Customer account information, including e-mail options

1.4.5 **Results Information and Reporting.** Discovered Security Vulnerabilities are displayed on the End User Management Console after being manually verified by a security engineer. Customer can retest a single or multiple vulnerabilities from the End User Management Console to confirm whether or not its remediation efforts were successful. Reports can be generated about one, several, or all of Customer's Materials. The reports are created and available for download from the End User Management Console. Vulnerability reports can be customized such that Customer can select which vulnerability classes or severity levels should appear as well as adjust the timeframe and other parameters.

1.5 **Optional Features.**

1.5.1 **WhiteHat Sentinel Application Programming Interface.** An Application Programming Interface ("API") is made available through the End User Management Console at no additional charge. Through the use of this API, Customer may integrate the WhiteHat Sentinel Service with other systems to directly transfer discovered vulnerability data. The discovered data can be automatically integrated with bug-tracking systems, security information and event management ("SIEM") systems, or web application firewalls ("WAF").

2. **Service Delivery Process.**

2.1 The service delivery process for the WhiteHat Sentinel Service is as follows:

2.1.1 **WhiteHat Sentinel.** There are two WhiteHat Sentinel delivery phases: (a) initial implementation of Web Applications; and (b) ongoing assessment of Web Applications. The initial implementation phase includes, as required by the ordered level of service, configuration and fine-tuning WhiteHat Sentinel, creation and testing of User Credentials, testing of business logic, and identification of forms. Ongoing assessment includes, as required by the ordered level of service, reassessment of Web Applications and minor adjustments to any custom tests.

2.1.2 **WhiteHat Sentinel Source.** Sentinel Source is implemented in three phases: (a) initial set up of the VM scanning appliance and onboarding of the Source Code Branch(es) contracted for testing, (b) initial testing of the Source Code Branch(es) and conference with the customer to review findings with the TRC and (c) flexible assessment scheduling by the Customer to gather immediate feedback and provide a structured timeline for testing within the SDLC.

2.2 **Initial Implementation.**

2.2.1 **WhiteHat Sentinel.** Upon order, Verizon and/or WhiteHat will provide an order confirmation and the "WhiteHat Sentinel Implementation Form" via separate email messages. The date that the order confirmation is sent is the "Order Confirmation Date." The WhiteHat Sentinel Implementation Form is used to identify Customer's primary point of contact and collect Host Name(s) information

relative to Customer's Web Application(s) and the levels of service. Customer must submit this form to an email address provided by Verizon and/or WhiteHat. This initial process to setup WhiteHat Sentinel will be completed within 5 business days of Customer's submission of the WhiteHat Sentinel Implementation Form, at which point Verizon (via WhiteHat) will provide login credentials to the End User Management Console for Customer to log in for the first time to configure WhiteHat Sentinel. If the WhiteHat Sentinel Implementation Form is not received by Verizon within 30 days after receipt by Customer, Customer will be set up in the End User Management Console with no Web Applications and Verizon (via WhiteHat) will provide login credentials to the End User Management Console for Customer to log in. When Verizon (via WhiteHat) has provided such login credentials, Customer is deemed ready for service ("RFS").

2.2.1.1 Customer must provide any User Credentials needed to access Customer's Web Application. When Customer has scheduled a scan by entering the time and date that the assessment is to begin, the End User Management Console will notify WhiteHat security engineers of the schedule and the security engineers will begin to verify the information provided, including the provided User Credentials. Contact information for WhiteHat will be provided to Customer as part of the implementation process.

2.2.1.2 The series of tasks performed by Verizon (via WhiteHat) during the initial implementation phase of WhiteHat Sentinel includes the following, depending on the level of service:

2.2.1.2.1 Test User Credentials (including adding new users/roles, as necessary).

2.2.1.2.2 Configuration and fine-tuning of the WhiteHat Sentinel service to scan Customer's Web Application's forms and fill them out, perform business logic functions, and complete workflows. Form workflow often occurs in layers that may require multiple scans to fully discover vulnerabilities. For example, if it requires four forms to complete a transaction, WhiteHat Sentinel will find the first form, and the security engineers will configure WhiteHat Sentinel to interact with that form. The next time WhiteHat Sentinel scans that particular Web Application, it will take those actions on the form, and only then find the next form.

2.2.1.2.3 Define "fuzzer" tests to iterate through integer values such that the responses can be compared to each based on the different input values. Fuzzer testing is a technique to see how an application responds to random, unexpected, and/or invalid data inputs.

2.2.1.2.4 Write custom tests for the Web Applications based upon manual review of the business logic.

2.2.1.2.5 Establish request/response tuning for edge case/unique uses of rich media (e.g., Flash).

2.2.1.3 Following the initial configuration and testing of WhiteHat Sentinel to assess the target Web Application, and as required by the ordered level of service, a security engineer is available to review the findings with the Customer and explain how the findings relate/map to software development practices and discuss remediation strategies.

2.2.2 **WhiteHat Sentinel Source.** The WhiteHat TRC provisions a VM scanning appliance for Customer, which Customer must install before Sentinel Source can be initiated. Once the VM appliance is operational, Customer may onboard its Source Code Branch(es) using the application wizard. Alternatively, Customer may contact WhiteHat Customer Support and supply the necessary credentials, URL(s), scan schedule and any additional information necessary to onboard the Source Code Branch(es) to WhiteHat Customer Support. WhiteHat Customer Support will then onboard the Source Code Branch(es) for Customer.

2.2.2.1 Customer is in control of start times, stop times and scheduling of the automated scanning process through the Sentinel Management Console. Prior to posting to the End User Management Console, vulnerabilities are verified by the WhiteHat Security Operations team and rated both by impact and likelihood of exploitation to enable Customer's developers to prioritize the remediation process. Customer is responsible for any remediation of the code.

2.2.2.2 After the initial testing of the Source Code Branch(es), The WhiteHat TRC team will be available to review the findings with Customer. The TRC team will explain the discovered vulnerabilities to Customer's designated contact(s) via email or conference call. This explanation will include how the vulnerabilities relate to software development practices and the appropriate remediation strategies for Customer's situation.

3. **Ongoing Assessment.**

3.1 **WhiteHat Sentinel.** Depending on the ordered level of service, Customer may contact the security engineers via phone, email, or the End User Management Console for questions related to findings from

the initial configuration of WhiteHat Sentinel service for that particular Web Application. The security engineers will typically explain how the findings relate to Customer's software development practices and may recommend possible remediation strategies. The series of tasks performed by Verizon (via WhiteHat) during ongoing WhiteHat Sentinel assessment includes the following, depending on the level of service:

3.1.1 **Ongoing Assessments**. Ongoing assessments can be scheduled via the End User Management Console after the initial implementation phase for Web Applications has been completed.

3.1.2 **Re-Assessment.** For specific vulnerabilities that have been fixed, patched, or removed, single or multiple vulnerabilities can be retested as long as any required User Credentials remain valid. This re-assessment feature can be used to confirm whether remediation was successful or not.

3.1.3 **Manual re-Assessment Requests.** For business logic vulnerabilities, a request for re-assessment "Queues" a ticket for the security engineers to review and manually re-assess (i.e. re-assess by hand).

3.1.4 **Scanning New Code.** As WhiteHat Sentinel discovers new code, forms, links and business logic flows in the targeted Web Applications, tickets are generated internally for the security engineers to review and create additional custom tests as necessary. When new code is released, WhiteHat Sentinel will adapt and customize the ongoing testing processes accordingly as long as valid User Credentials are available and that the specific part of the Web Application remains accessible.

3.1.5 **Custom Tests.** Verizon (via WhiteHat) will write custom tests for the Web Applications based upon manual review of the business logic when changes to the business logic occur as long as valid User Credentials are available and that the specific part of the Web Application remains accessible.

3.1.6 **Reporting.** The End User Management Console contains both high-level and detailed vulnerability reports. Website security vulnerabilities are posted to the portal after they are discovered and verified. Customer controls what personnel has access to the End User Management Console.

3.2 **WhiteHat Sentinel Source.**

3.2.1 Customer may schedule an assessment to gather immediate feedback after Customer returns its code to the source code repository.

3.2.2 Customer also may schedule assessments at a specific time each day (via the End User Management Console) to reduce the risk of delaying assessments until further into the SDLC.

4. **Updates to WhiteHat Sentinel.** Verizon (via WhiteHat) will update the Sentinel scanning software and testing as required when a new attack vector is identified. Verizon (via WhiteHat) uses commercially reasonable efforts to augment or otherwise modify the WhiteHat Sentinel Service to identify and eliminate security vulnerabilities which are different from or are in addition to the Customer Material Security Vulnerabilities and include such vulnerabilities or weaknesses which are applicable to websites, applications or source code. Verizon reserves the right for itself and for WhiteHat to amend the WhiteHat Sentinel Service from time to time effective upon notice to Customer from Verizon or WhiteHat, as applicable, including notice via the End User Management Console; provided, that in the event of any amendment resulting in a material reduction of any WhiteHat Sentinel Service, service levels, or credits, Customer may terminate the affected WhiteHat Sentinel Service without penalty by providing Verizon written notice of termination during the 30 days following notice of such amendment. Verizon may avoid such WhiteHat Sentinel termination if, within 30 days of receipt of Customer's written notice, it agrees to amend the service agreement to eliminate the applicability of the material reduction.

5. **Customer Support.** Customer Support is available via access to End User Management Console, email or the direct WhiteHat support phone number. From the End User Management Console, Customer can submit service requests to WhiteHat Customer Support engineers 24 hours a day. Direct access to a Customer Support engineer is available from 6:00 AM – 7:00 PM Pacific Time Monday – Friday, excluding holidays.

6. **WhiteHat Sentinel Service Terms.**

6.1 In order to enable performance of the WhiteHat Sentinel Service for the Customer Materials, Customer hereby grants Verizon and WhiteHat the right to access, and use and modify and create derivative works of the Customer Materials as required for the provision of the WhiteHat Sentinel Service.

6.2 Customer acknowledges and agrees that Verizon's and/or WhiteHat's access to and use of the Customer Materials is not subject to any "Terms of Use" or other terms or conditions that may be posted or otherwise provided on the Customer Materials which purport to govern access to and use of the Customer Materials.

6.3 Customer represents that it is either the owner of the Customer Materials or has the authority to permit Verizon to provide the WhiteHat Sentinel Service for the Customer Materials. Customer will provide Verizon and/or WhiteHat written evidence thereof upon request.

6.4 Customer acknowledges and agrees that it is Customer's sole responsibility to update and maintain the Customer Materials, including without limitation, fixing any security vulnerability revealed by the WhiteHat Sentinel Service and reports. Customer further acknowledges and agrees that the Customer is responsible for providing all configuration data (host names, user accounts, etc.) needed to perform the WhiteHat Sentinel Service. Failure to provide configuration data does not release Customer from any responsibility hereunder. Customer acknowledges and agrees that Customer's use of the WhiteHat Sentinel Service is dependent upon access to telecommunications and Internet services at Customer's sole cost and expense.

6.5 Customer represents and warrants that all information provided in the WhiteHat Sentinel Implementation Form is true, accurate and complete and in the event that any such information changes, Customer agrees to provide Verizon and/or WhiteHat prompt written notice thereof.

Part III: Service Terms and Conditions.

1. Customer shall not export or re-export, directly or indirectly, the WhiteHat Sentinel Service (or any component thereof) or materials provided related to the WhiteHat Sentinel Service delivered pursuant to this Service Attachment, including software ("WhiteHat Sentinel Materials") (or any component thereof), except in full compliance with all United States and other applicable laws and regulations.
2. The parties agree that in the event that either party or a party's independent contractors or suppliers are prevented from performing or are unable to perform any of its obligations under this Service Attachment, (including any delay in developing or delivering the WhiteHat Sentinel Service) due to any act of God, war, terror, strike, lockout, epidemic, riot, insurrection, unavailability or performance degradation of the Internet or any other cause beyond the reasonable control of the party invoking this section (a "Force Majeure") and if such party shall have used its reasonable efforts to mitigate the effects of such Force Majeure, such party shall give prompt written notice to the other party, its nonperformance shall be excused, and the time for the performance shall be extended for the period of delay or inability to perform due to such occurrences. Notwithstanding the foregoing, if such party is not able to perform within 30 days after the event giving rise to the excuse of Force Majeure, the other party may terminate this Service Attachment. Notwithstanding the foregoing, Customer's failure to comply with payment obligations shall not be excused or delayed due to a Force Majeure Condition, unless Customer has used its best efforts to comply with such payment obligations and is still unable to so comply solely as a result of the Force Majeure Condition. Customer's obligation to comply with payment obligations will immediately resume when the applicable Force Majeure Condition ceases.
3. **Intellectual Property Rights.**

3.1 **Ownership.** Each party agrees that except as provided below, it acquires no right, title or interest in or to the other party's information, data base rights, data, tools, processes or methods, or any copyrights, trademarks, service marks, trade secrets, patents or any other intellectual or intangible property or property rights of the other party by virtue of the provision of the WhiteHat Sentinel Service (referred to in this Section 3 as "WhiteHat Sentinel") or WhiteHat Sentinel Materials. Customer retains all right title and interest in and to the underlying factual data gathered through the provision of WhiteHat Sentinel. Verizon or WhiteHat, as applicable owns all right title and interest in and to Verizon's trade secrets, confidential information or other proprietary rights in any creative or proprietary ideas, information or other material used by Verizon or presented to Customer (each, a "Technical Element"), including, but not limited to: WhiteHat Sentinel Materials, data, software, modules, components, designs, utilities, databases, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices, report formats, manner of data expression and specifications. Verizon grants Customer a nonexclusive, royalty-free license to use each Technical Element integrated into WhiteHat Sentinel solely for Customer's internal business purposes. Customer may disclose a Technical Element integrated into a deliverable to a third party as long as such third party is subject to a written nondisclosure agreement, requiring such third party to maintain the confidentiality of such Technical Element and use such Technical Element only for the benefit of Customer. Notwithstanding anything contained in this Service Attachment to the contrary, Customer is prohibited from creating derivative works of all or any portion of a Technical Element.

3.1.1 Customer will not: (i) copy or otherwise reproduce, whether in whole or in part, WhiteHat Sentinel or WhiteHat Sentinel Materials to which Customer has been granted access or use; (b) modify or create any derivative work of WhiteHat Sentinel or the WhiteHat Sentinel Materials; (c) sell, rent, loan, license, sublicense, distribute, assign or otherwise transfer WhiteHat Sentinel or the WhiteHat Sentinel Materials; (d) cause or permit the disassembly, decompilation or reverse engineering of any software components of WhiteHat Sentinel Materials or otherwise attempt to gain access to the source code of such software components; or (e) cause or permit any third party to do any of the foregoing. Such restrictions shall survive the expiration or termination of this Service Attachment or the Agreement. Verizon has the right to revoke the use of the WhiteHat Sentinel Materials at any time. For purposes of clarification, in the absence of Cause by Customer, such revocation by Verizon of Customer's right to use the WhiteHat Sentinel Materials shall not affect Verizon's obligation to perform WhiteHat Sentinel. In such event, Customer shall, at Customer's sole cost and expense, promptly return WhiteHat Sentinel Materials to Verizon. Customer's right to use WhiteHat Sentinel Materials automatically terminates upon termination of this Service Attachment or upon completion of the portion of WhiteHat Sentinel for which the WhiteHat Sentinel Materials are provided.

3.1.2 **Certification Seals.** If, under the terms of this Service Attachment, Customer is granted the right to use any Verizon or WhiteHat certification seals or logos (each, a "Certification Seals"), then the

display and presentation of such Certification Seal by Customer shall be subject to Verizon's or WhiteHat's (as applicable) then-current logo guidelines.

4. **Scanning.** Customer understands that website scanning, including, without limitation, the scanning of applications, and the technology associated with it (collectively "Scanning"), has risks, including, but not limited to, the loss, disruption, or performance degradation of Customer's or a third party's business processes, or data (the "Scanning Risks"). Customer acknowledges that it understands and accepts the Scanning Risks associated with the WhiteHat Sentinel Service and authorizes Verizon or WhiteHat, as applicable, to perform the WhiteHat Sentinel Service when ordered. Verizon shall take reasonable steps to mitigate these Scanning Risks (e.g. by using limited requests per second so as to run in the background); however, Customer understands that these Scanning Risks cannot be eliminated. Customer agrees to indemnify, defend and hold harmless Verizon and its affiliates, officers, agents, successors or assigns (each, a "Verizon Indemnified Party") from and against any and all loss, damages, liabilities, costs and expenses (including legal expenses and the expenses of other professionals) incurred by Verizon, resulting directly or indirectly from any third-party claim attributable to or arising out of Verizon's use of "Scanning Technology" (each, a "Scanning Claim"), including, without limitation, the use by Verizon of "Scanning Technology" to analyze assets that are not controlled directly by Customer (e.g., servers hosted by third parties). The obligation of Customer to indemnify, defend and hold a Verizon Indemnified Party harmless in connection with a Scanning Claim will not apply to the extent that the Scanning Claim is based on Verizon's gross negligence or willful misconduct.
5. **Warranty and Limitation of Liability.**
   5.1 WITH REGARD TO SERVICES WHICH PROVIDE INFORMATION SHARING, VULNERABILITY ARTICLES, AND/OR REFERENCE INFORMATION, VERIZON DISCLAIMS ANY LIABILITY TO CUSTOMER, AND CUSTOMER ASSUMES THE ENTIRE RISK FOR (A) INFORMATION FROM THIRD PARTIES PROVIDED TO CUSTOMER WHICH TO THE BEST OF VERIZON'S INFORMATION, KNOWLEDGE AND BELIEF DID NOT CONTAIN FALSE, MISLEADING, INACCURATE OR INFRINGING INFORMATION; (B) CUSTOMER'S ACTIONS OR FAILURE TO ACT IN RELIANCE ON ANY INFORMATION FURNISHED AS PART OF THE SERVICES; AND (C) THE USE OF ANY THIRD PARTY LINKS, PATCHES, UPDATES, UPGRADES, ENHANCEMENTS, NEW RELEASES, NEW VERSIONS OR ANY OTHER REMEDY SUGGESTED BY ANY THIRD PARTY AS PART OF THE SERVICES.
   5.2 THE INFORMATION CONTAINED IN, OR DERIVED FROM, WHITEHAT SENTINEL ARE NOT INTENDED TO, AND DOES NOT, ENSURE THAT CUSTOMER IS COMPLIANT WITH SPECIFIC GOVERNMENT REGULATIONS OR SECURITY STANDARDS. VERIZON DOES NOT WARRANT THAT THE INFORMATION CONTAINED IN WHITEHAT SENTINEL REPORTS IS ERROR-FREE OR THAT DEFECTS WILL BE CORRECTED. VERIZON DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF WHITEHAT SENTINEL REPORT INFORMATION IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. BY USING THIS INFORMATION, CUSTOMER ACKNOWLEDGES ITS UNDERSTANDING OF THESE TERMS AND AGREES TO ASSUME THE ENTIRE RISK AND COST OF ANY NECESSARY EXPENSES, DAMAGES, OR LIABILITY ARISING FROM SUCH USE OF SUCH INFORMATION DERIVED FROM THE WHITEHAT SENTINEL SERVICE OR SUCH WHITEHAT SENTINEL REPORT INFORMATION.
   5.3 Except as otherwise stated herein, the parties agree that Verizon, its independent contractors and suppliers are providing the WhiteHat Sentinel Service on a "WHERE IS, AS IS" basis and make no warranties, express or implied, statutory or otherwise, and specifically disclaim all implied warranties (including those of availability, reliability, usefulness, merchantability, non-infringement, fitness for a particular purpose and those arising out of course of performance, dealing, usage or trade). Verizon does not warrant that the WhiteHat Sentinel Service is uninterruptible or error-free or that any Customer Materials scanned software or any other materials accessed through the WhiteHat Sentinel Service is free from infringing materials, viruses, malicious codes and other harmful components. For services provided to Customer from third parties and third party products (such as Service Equipment), Customer receives only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.
6. **Nature of Service.** The WhiteHat Sentinel Service does not provide service, maintenance or repair to or for any real or personal property.
7. **Service Equipment.** If Verizon or WhiteHat-owned equipment and software (''Service Equipment'') is provided to Customer for use in connection with the WhiteHat Sentinel Service, Customer shall be liable for any and all loss or damage to the Service Equipment, excluding damage attributable to normal wear and tear, in Customer's possession or under its control, unless such loss or damage is attributable to a negligent act or omission of Verizon or WhiteHat. Customer shall notify Verizon immediately of any loss or damage attributable to a negligent act or omission of Verizon. Customer agrees to (i) house the Service Equipment in a safe and serviceable environment and in accordance with reasonable instructions by Verizon as may be given from time to time; and (ii) permit Verizon or an authorized representative of Verizon to modify, relocate, repair, inspect or test the Service Equipment at all times subject to compliance with any reasonable security and safety procedures in force at the location where the Service Equipment is located or housed by or on behalf of Customer.

7.1 Verizon has the right to revoke the use of the Service Equipment at any time. For purposes of clarification, in the absence of Cause by Customer, such revocation by Verizon of Customer's right to use the Service Equipment shall not affect Verizon's obligation to perform the WhiteHat Sentinel. Upon Verizon's revocation of Service Equipment use, or termination or expiration of the WhiteHat Sentinel Service for which the Service Equipment has been provided, Customer shall immediately cease all further use of the Service Equipment and return to Verizon the Service Equipment in the same condition as such Service Equipment was received, excluding normal wear and tear, in the original or equivalent packaging materials. In such event, freight and insurance shall be prepaid by Customer and Customer shall bear all of the costs and expenses attributable to returning the Service Equipment to Verizon. If Customer fails to return the Service Equipment within 14 calendar days following termination or expiration of the applicable services, Customer shall pay the greater of: (i) 50% of the relevant set-up per site NRC indicated in the Service Order; or (ii) the actual cost and expense to replace such Service Equipment as determined by Verizon.

8. **Provision of Services Outside U.S. or U.S. Territories.** WhiteHat will perform all services under this Service Attachment in the United States or its territories. Further, Verizon will not assign any employee or subcontractor to perform services under this Service Attachment if that individual or subcontractor is located outside of the United States or its territories.

Part IV: Definitions. In addition to the definitions identified in the Master Terms, the following administrative charge definitions apply to WhiteHat Sentinel: www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm