SPLUNK GENERAL TERMS FOR U.S. FEDERAL END USERS

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE OFFERINGS, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

THESE GENERAL TERMS APPLY ONLY IF THE CUSTOMER IS AN EXECUTIVE AGENCY OF THE U.S. GOVERNMENT OR AN ELIGIBLE ORDERING ACTIVITY. THESE TERMS SHALL BE INCORPORATED IN ANY ORDERS ISSUED BY SUCH CUSTOMERS. IF THE CUSTOMER IS NOT AN EXECUTIVE AGENCY OF THE U.S. GOVERNMENT OR AN ELIGIBLE ORDERING ACTIVITY (EXCLUDING STATE AND LOCAL GOVERNMENT ENTITIES), THEN SPLUNK'S GENERAL TERMS AVAILABLE AT https://www.splunk.com/en_us/legal/splunk-general-terms.html APPLY.

These Splunk General Terms ("**General Terms**" or "Agreement")) between Splunk Inc., a Delaware corporation, with its principal place of business at 270 Brannan Street, San Francisco, California 94107, U.S.A ("**Splunk**" or "we" or "us" or "our") and you ("**Customer**" or "Ordering Activity" or "you" or "your") apply to the purchase of licenses and subscriptions for Splunk's Offerings. By placing a written order under a contract incorporating these General Terms, you agree to these General Terms. If you are entering into these General Terms on behalf of Customer, you represent that you have the authority to bind Customer.

See the General Terms Definitions Exhibit attached for definitions of capitalized terms not defined herein.

1. License Rights

(A) **General Rights**. You have the nonexclusive, worldwide, nontransferable and nonsublicensable right, subject to payment of applicable Fees and compliance with the terms of these General Terms, to use your Purchased Offerings for your Internal Business Purposes during the Term and up to the Capacity purchased.

(B) **Copies for On-Premise Products**. You have the right to make a reasonable number of copies of On-Premise Products for archival and back-up purposes.

(C) **Splunk Extensions**. You may use Splunk Extensions in connection with the applicable Purchased Offering subject to the same terms and conditions for that Offering (including with respect to Term) and payment of any Fees associated with the Splunk Extensions. Some Splunk Extensions may be made available under license terms that provide broader rights than the license rights you have to the applicable underlying Offering (e.g., if the Extension is Open Source Software). These broader rights will apply to that Splunk Extension. Splunk Extensions may be installed on Hosted Services pursuant to our instructions.

(D) **Trials, Evaluations, Beta and Free Licenses**.

(i) **Trials and Evaluations**. Offerings provided for trials and evaluations, as specified in an Order, are provided at no charge, and their use will be for the specified limited duration.

(ii) **Beta Licenses**. Some Offerings may be available to you as a preview, or as an alpha, beta or other pre-release version (each, a "**Beta Offering**"). All rights for Beta Offerings are solely for internal testing and evaluation. Your use of a Beta Offering will be for the term specified by us, and if no term is specified, then for the earlier of one year from the start date of the Beta Offering or when that version of the Beta Offering becomes generally available. We may discontinue the Beta Offering at any time and may decide not to make any of the features and functionality generally available

(iii) **Free Licenses**. From time to time, we may make certain Offerings available for full use (i.e., not subject to limited evaluation purposes) at no charge. These free Offerings may have limited features, functions and other technical limitations.

(E) **Test and Development Licenses**. For Offerings identified as "Test and Development" Offerings on your Order, you only have the right to use those Offerings up to the applicable Capacity on a non-production system for non-production uses, including product migration testing or pre-production staging, or testing new data sources, types, or use cases. Test and Development Offerings may not be used for any revenue generation, commercial activity, or other productive business or purpose.

(F) **Limitations**. Notwithstanding anything to the contrary in these General Terms, we do not provide maintenance and support, warranties, or indemnification for Test and Development Offerings, trials, evaluations, or free or Beta Offerings.

2. Purchasing Through Authorized Resellers

If you purchase Offerings through a Splunk authorized reseller, these General Terms will govern those Offerings. Your payment obligations for the Purchased Offerings will be with the authorized reseller, not Splunk. You will have no direct Fee payment obligations to Splunk for those Offerings.

Any terms agreed to between you and the authorized reseller that are in addition to these General Terms are solely between you and the authorized reseller. No agreement between you and an authorized reseller is binding on Splunk, or will have any force or effect with respect to the rights in, or the operation, use or provision of, the Offerings.

3. Your Contractors and Third-Party Providers

You may permit your authorized consultants, contractors, and agents ("**Third-Party Providers**") to access and use your Purchased Offerings, but only on your behalf in connection with providing services to you, and subject to the terms and conditions of these General Terms. Any access or use by a Third-Party Provider will be subject to the same limitations and restrictions that apply to you under these General Terms, and you will be responsible for any Third-Party Provider's actions relating to or use of the Offering. The aggregate use by you and all of your Third-Party Providers must not exceed the Capacity purchased, and nothing in this Section is intended to or will be deemed to increase such Capacity.

4. Hosted Services

(A) **Service Levels**. When you purchase Hosted Services as a Purchased Offering, we will make the applicable Hosted Services available to you during the Term in accordance with these General Terms. If a Service Level Schedule applies to your Hosted Service (as identified in the Specific Hosted Services Terms referenced in Section 4(I) below), the Service Level Schedule and associated remedies will apply to the availability and uptime of the Hosted Service. If applicable, service credits will be available for downtime in accordance with the Service Level Schedule.

(B) **Data Protection**. Please refer to Sections 9 and 10 below for information on Splunk's security and data protection programs for our Hosted Services.

(C) **Maintaining Protections**. Notwithstanding anything to contrary in these General Terms, or any policy or terms referenced herein via hyperlink (or any update thereto), Splunk may not, during a Term materially diminish the security protections provided by the controls set for the Hosted Service.

(D) **Connections**. You are responsible for obtaining and maintaining all telecommunications, broadband and computer equipment and services needed to access and use Hosted Services, and for paying all associated charges.

(E) **Your Responsibility for Data Protection**. You are responsible for: (i) selecting from the security configurations and security options made available by Splunk in connection with a Hosted Service; (ii) taking additional measures outside of the Hosted Service to the extent the Hosted Service Offering does not provide the controls that may be required or desired by you; and (iii) routine archiving and backing up of Customer Content. You agree to notify Splunk immediately if you believe that an unauthorized third party may be using your accounts or if your account information is lost or stolen.

(F) **Data Restrictions**. You may not transmit and/or store PHI Data, PCI Data or ITAR Data within the Hosted Services unless you have specifically purchased a Purchased Offering for that applicable regulated Hosted Services environment (as identified in an Order).

(G) **Refund Upon Termination for Splunk's Breach**. If a Hosted Service is terminated by you for Splunk's uncured material breach in accordance with these General Terms, Splunk will refund you any prepaid subscription fees covering the remainder of the Term after the effective date of termination.

(H) **Return of Customer Content**. Customer Content may be retrieved by you and removed from the Hosted Services in accordance with the applicable Documentation. We will make the Customer Content available on the Hosted Services for thirty (30) days after termination of a subscription for your retrieval. After that thirty (30) day period, we will have no obligation to maintain the storage of your Customer Content, and you hereby authorize us thereafter to delete all remaining Customer Content, unless we are otherwise legally prohibited from doing so. If you require assistance in connection with migration of your Customer Content, depending on the nature of the request, we may require a mutually agreed upon fee for assistance.

(I) **Specific Hosted Services Terms**. Specific security controls and certifications, data policies, service descriptions, Service Level Schedules and other terms specific to Hosted Services ("**Specific Hosted Services Terms**"), current as of the Effective Date, are attached to these General Terms as Exhibit E for ease of your reference, and will apply as applicable. In the event that new Hosted Services Offerings are introduced by Splunk, the parties shall work together to add additional applicable terms to these General Terms prior to adding such Offerings to these General Terms.

5. Support and Maintenance

Your Purchased Offerings may include support and maintenance services as part of your purchase. The specific Support Program purchased with a Purchased Offering will be identified in the applicable Order. Splunk will provide the purchased level of support and maintenance services in accordance with the terms of the Support Exhibit, current as of the Effective Date, attached to these General Terms as Exhibit A.

6. Configuration and Implementation Services

Splunk offers standard services to implement and configure your Purchased Offerings, subject to the payment of the Fees for these services in an Order, and the terms of the Configuration and Implementation Services Exhibit, current as of the Effective Date, attached to these General Terms as Exhibit B.

7. Use Restrictions

Except as expressly permitted in an Order or our Documentation, you agree not to (nor allow any third party to): (a) reverse engineer (except to the extent specifically permitted by statutory law), decompile, disassemble or otherwise attempt to discover source code or underlying structures, ideas or algorithms of any Offering; (b) modify, translate or create derivative works based on the Offerings; (c) use

an Offering for service bureau purposes, or for any purpose other than your own Internal Business Purposes; (d) resell, transfer or distribute any Offering; (e) access or use any Offering in order to monitor its availability, performance, or functionality for competitive purposes; (f) attempt to disable or circumvent any license key or other technological mechanisms or measures intended to prevent, limit or control use or copying of, or access to, Offerings; (g) separately use any of the applicable features and functionalities of the Offerings with external applications or code not furnished by Splunk or any data not processed by the Offering; (h) exceed the Capacity purchased or (i) use any Offering in violation of all applicable laws and regulations (including but not limited to any applicable privacy and intellectual property laws).

8. Our Ethics, Compliance and Corporate Responsibility

(A) **Ethics and Corporate Responsibility**. Splunk is committed to acting ethically and in compliance with applicable law, and we have policies and guidelines in place designed to provide awareness of, and compliance with, the laws and regulations that apply to our business globally. We are committed to ethical business conduct, and we strive to perform in accordance with the highest global ethical principles, as described in the Splunk Code of Conduct and Ethics found here: https://investors.splunk.com/code-business-conduct-and-ethics-1.

(B) **Anti-Corruption**. We use diligent efforts to implement and maintain programs to ensure compliance with applicable anti-corruption and anti-bribery laws. Splunk policy prohibits the offering or soliciting of any illegal or improper bribe, kickback, payment, gift, or thing of value to or from any of your employees or agents in connection with these General Terms. If we learn of any violation of the above, we will use reasonable efforts to promptly notify you at the main contact address provided by you to Splunk.

(C) **Export**. We certify that Splunk is not on any of the relevant U.S. government lists of prohibited persons, including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. Export information regarding our Offerings, including our export control classifications for our Offerings, is found here: https://www.splunk.com/en_us/legal/export-controls.html.

9. Data Protection

Splunk follows globally recognized data protection principles and industry-leading standards for the security of personal data. Splunk is self-certified with the U.S. Department of Commerce for the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Splunk's data protection practices include (as applicable) standard terms for the processing of Personal Data as defined under GDPR and Personal Information as defined under the CCPA. Please refer to the applicable Specific Hosted Services Terms that may apply to your Purchased Offering.

10. Security

(A) **General Security**. Splunk's information security management system ("**ISMS**") is calibrated to protect the confidentiality, integrity and availability of customer data. Splunk employees receive regular training on Splunk's security policies and procedures, including annual training on secure data handling practices, and supplemental, targeted trainings as appropriate. Employees are background checked and Splunk vendors are risk assessed prior to onboarding to determine if their data protection and security practices meet Splunk's standards**.**

(B) **Offering Security**. Hosted Services meet industry leading cloud security standards appropriate to the nature of service provided, e.g., Splunk Cloud HIPAA Offering certified to HIPAA security requirements. We have commercially reasonable physical, technical and procedural measures in place to protect Customer Content against destruction, loss, alteration, unauthorized disclosure to third parties or unauthorized access by employees or contractors employed by Splunk. Any specific and additional security controls for a Hosted Service are set forth in the applicable Documentation and Specific Hosted Services Terms www.splunk.com/SpecificTerms. Third-party certificates of compliance are issued as part of Splunk's audited third-party compliance program. In addition, for On-Premise Products, which are not provided as a service and therefore are not audited for compliance, Splunk follows industry standard security controls for the processing of customer data accessed or received through activities such as maintenance, implementation or configuration services. Those industry standard security controls are set forth in Splunk's Information Security Addendum ("**ISA**") located at www.splunk.com/on-prem-isa.

(C) **Product Development Security**. Splunk deploys secure software development practices and uses a risk-based approach when applying its standard software development lifecycle ("**SDLC**") methodology, which may include such things as performing security architecture reviews, open source security scans, virus detection, dynamic application security testing, network vulnerability scans and external penetration testing in the development environment. Product-specific information about the SDLC in our Offerings is detailed more fully in the ISA. Splunk's Product Security Portal contains detailed information about Splunk's program for managing and communicating product vulnerabilities. Splunk categorizes product vulnerabilities in accordance with the Common Vulnerability Scoring System ("Medium," "High," or "Critical") and uses commercially reasonable efforts to remediate vulnerabilities depending on their severity level in accordance with industry standards.

11. Usage Data

From time to time, Splunk may collect Usage Data generated as a by-product of your use of Offerings (e.g., technical information about your operating environment and sessions, systems architecture, page loads and views, product versions, number and type of searches, number of users, source type and format). Usage Data does not include Customer Content. We collect Usage Data for a variety of reasons, such as to identify, understand, and anticipate performance issues and the factors that affect them, to provide updates and personalized experiences to customers, and to improve the Splunk Offerings.

12. Capacity and Usage Verification

(A) **Certification**. At Splunk's request, you will furnish Splunk a certification signed by your authorized representative verifying that your use of the Purchased Offering is in accordance with these General Terms and the applicable Order. Also, if your Purchased Offering requires usage reporting (as specified and agreed in the Order), you agree to provide this reporting pursuant to those requirements.

(B) **Specific Product Verification**. For On-Premise Products, we may ask you from time to time, but not more frequently than once per calendar period, to cooperate with us to verify usage and adherence to purchased Capacities. If Splunk requests a verification process, you agree to provide Splunk reasonable access to the On-Premise Product installed at your facility (or as hosted by your Third-Party Provider). If Splunk does any verification, it will be performed with as little interference as possible to your use of the On-Premise Product and your business operations. Splunk will comply with your (or your Third-Party Providers') reasonable security procedures.

(C) **Overages**. If a verification or usage report reveals that you have exceeded the purchased Capacity or the scope of your license grant for your Purchased Offering (e.g. used as a service bureau) during the period reviewed, then we will have the right to invoice you using the applicable Fees at list price then in effect, which will be payable in accordance with these General Terms. Without limiting Splunk's foregoing rights, with respect to Hosted Services, Splunk may work with you to reduce usage so that it conforms to the applicable usage limit, and we will in good faith discuss options to right size your subscription as appropriate. For the avoidance of doubt, notwithstanding anything to the contrary herein, Splunk will have the right to directly invoice you for overages, regardless of whether you purchased the Purchased Offering from an authorized reseller. See the Specific Hosted Services Terms for any additional information related to overages for a Hosted Service.

13. Our Use of Open Source

Certain Offerings may contain Open Source Software. Splunk makes available in the applicable Documentation a list of Open Source Software incorporated in our On-Premise Products as required by the respective Open Source Software licenses. The List of Open Source Software can be found in the "Release Notes" in the Documentation, e.g. for Splunk Enterprise here: http://docs.splunk.com/Documentation/Splunk/latest/ReleaseNotes/Credits, (or on an updated link which may be provided from time to time). Any Open Source Software that is delivered as part of your Offering and which may not be removed or used separately from the Offering is covered by the warranty, support and indemnification provisions applicable to the Offering. Some of the Open Source Software may have additional terms that apply to the use of the Offering (e.g., the obligation for us to provide attribution of the specific licensor), and those terms will be included in the Documentation; however, these terms will not (a) impose any additional restrictions on your use of the Offering, or (b) negate or amend any of our responsibilities with respect to the Offering.

14. Splunk Developer Tools and Customer Extensions

Splunk makes Splunk Developer Tools available to you so you can develop Extensions for use with your Purchased Offerings (Extensions that you develop, "**Customer Extensions**").

You have a nonexclusive, worldwide, nontransferable, non-sublicensable right, subject to the terms of these General Terms, to use Splunk Developer Tools to (a) copy and modify Splunk Developer Tools to develop your Customer Extensions, including to support interoperability between the Offering and your system or environment, and (b) distribute your Customer Extensions exclusively for use with the designated Offering. Your rights are subject to the following conditions: (x) Splunk proprietary legends or notices contained in the Splunk Developer Tools may not be removed or altered when used in or with your Customer Extension; and (y) you may not make any statement that your Customer Extension is certified or that its performance is guaranteed by Splunk. You retain title to your Customer Extensions, subject to Splunk's ownership in our Offerings and any materials and technology provided by Splunk in connection with the Splunk Developer Tools. If you allow end users of Customer Extensions to modify or distribute the Customer Extensions, you will limit such modification or distribution to use with the designated Offering only, and will flow down the conditions in (x) and (y) above to end users of Customer Extensions. You agree to assume full responsibility for the performance and distribution of Customer Extensions.

15. Third-Party Extensions, Third-Party Content and Unsupported Splunk Extensions

(A) **Third-Party Extensions**. Splunk makes no promises or guarantees related to Extensions on Splunkbase developed and/or made available by a third-party ("**Third-Party Extension**"). Splunk makes Third-Party Extensions available for download on Splunkbase as a convenience to its customers. Splunk neither controls nor endorses, nor is Splunk responsible for, any Third-Party Extension, including the accuracy, integrity, quality, legality, usefulness or security of the Third-Party Extension. Nothing in these General Terms or on Splunkbase will be deemed to be a representation or warranty by Splunk with respect to any Third-Party Extension, even if a particular Third-Party Extension is identified as "certified" or "validated" for use with an Offering. We may, in our reasonable discretion, block or disable access to any Third-Party Extension at any time. Your use of a Third-Party Extension is at your own risk and may be subject to any additional terms, conditions and policies applicable to that Third-Party Extension (such as license terms, terms of service, or privacy policies of the providers of such Third-Party Extension). By executing this agreement, the Ordering Activity does not agree to be bound by any third-party terms without executing an agreement in writing. The Ordering Activity acknowledges that third-party software has different terms and the Ordering Activity will not use Third-Party Extensions without first agreeing in writing to be bound by any applicable Third Party terms.

(B) **Third-Party Content**. Hosted Services may contain features or functions that enable interoperation with Third-Party Content that you, in your sole discretion, choose to add to a Hosted Service. You may be required to obtain access separately to such Third-Party Content from the respective providers, and you may be required to grant Splunk access to your accounts with such providers to the extent necessary for Splunk to allow the interoperation with the Hosted Service. By requesting or allowing Splunk to enable access to such Third-Party Content in connection with the Hosted Services, you certify that you are authorized under the provider's terms to allow such access. If you install or enable (or direct or otherwise authorize Splunk to install or enable) Third-Party Content for use with a Hosted Service where the interoperation includes access by the third party provider to your Customer Content, you hereby authorize Splunk to allow the provider of such Third-Party Content to access Customer Content as necessary for the interoperation. You agree that Splunk is not responsible or liable for disclosure, modification or deletion of Customer Content resulting from access to Customer Content by such Third-Party Content, nor is Splunk liable for any damages or downtime that you may incur or any impact on your experience of the Hosted Service, directly or indirectly, as a result of your use of, and/or reliance upon, any Third-Party Content, sites or resources.

(C) **Unsupported Splunk Extensions**. The Service Level Schedule commitments for any applicable Hosted Services will not apply to Splunk Extensions labeled on Splunkbase as "**Not Supported.**" You agree that Splunk is not responsible for any impact on your experience of a Hosted Service as a result of your installation and/or use of any "Not Supported" Splunk Extensions, and that your sole remedy will be to remove the "Not Supported" Splunk Extension from the applicable Hosted Service. Further, some Splunk Extensions may not be compatible or certified for use with that Hosted Service (e.g., only specific Splunk Extensions are validated for our FedRAMP authorized environment for Splunk Cloud). Please refer to the applicable Documentation for more information related to the Splunk Extensions compatible with your specific Purchased Offering.

16. Your Compliance

(A) **Lawful Use of Offerings**. When you access and use an Offering, you are responsible for complying with all laws, rules, and regulations applicable to your access and use. This includes being responsible for your Customer Content and users, for your users' compliance with these General Terms, and the accuracy, lawful use of, and the means by which you acquired your Customer Content.

(B) **Registration**. You agree to provide accurate and complete information when you register for and use any Offering and agree to keep this information current. Each person who uses any Offering must have a separate username and password. For Hosted Services, you must provide a valid email address for each person authorized to use your Hosted Services, and you may only have one person per username and password. Splunk may reasonably require additional information in connection with certain Offerings (e.g., technical information necessary for your connection to a Hosted Service), and you will provide this information as reasonably requested by Splunk. You are responsible for securing, protecting and maintaining the confidentiality of your account usernames, passwords and access tokens.

(C) **Export Compliance**. You will comply with all applicable export laws and regulations of the United States and any other country ("**Export Laws**") where your users use any of the Offerings. You certify that you are not on any of the relevant U.S. government lists of prohibited persons, including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. You will not export, re-export, ship, transfer or otherwise use the Offerings in any country subject to an embargo or other sanction by the United States, including, without limitation, Iran, Syria, Cuba, the Crimea Region of Ukraine, Sudan and North Korea, and you will not use any Offering for any purpose prohibited by the Export Laws.

(D) **GovCloud Services**. If you access or use any Hosted Services in the specially isolated Amazon Web Services ("**AWS**") GovCloud (US) region (including without limitation any Hosted Services that are provisioned in a FedRAMP authorized environment), you represent and warrant that users will only access the Hosted Services in the AWS GovCloud (US) region if users: (i) are "US Person(s)" as defined under ITAR (see 22 CFR part 120.15); (ii) have and will maintain a valid Directorate of Defense Trade Controls registration, if required by ITAR; (iii) are not subject to export control restrictions under US export control laws and regulations (i.e., users are not denied or debarred parties or otherwise subject to sanctions); and (iv) maintain an effective compliance program to ensure compliance with applicable US export control laws and regulations, including ITAR, as applicable. You are responsible for verifying that any user accessing Customer Content in the Hosted Services in the AWS GovCloud (US) region is eligible to access to such Customer Content. The Hosted Services in the AWS GovCloud (US) region may not be used to process or store classified data. You will be responsible for all sanitization costs incurred by Splunk if users introduce classified data into the Hosted Services in the AWS GovCloud (US) region.

(E) **Acceptable Use**. Without limiting any terms under these General Terms, you will also abide by our Hosted Services acceptable use policy: https://www.splunk.com/view/SP-CAAAMB6, current as of the Effective Date, is attached to these General Terms as Exhibit D for ease of your reference.

(F) **Respecting the Rights of Third Parties and Applicable Regulations**. You represent and warrant that (i) your Customer Content or Customer Extensions does not infringe or misappropriate such third-party patents, copyrights, trademarks or trade secrets, or violates another right of a third party; and that (ii) your Customer Content or your use of any Offering does not violate applicable laws or regulations.

17. Confidentiality

(A) **Confidential Information**. Each party will protect the Confidential Information of the other. Accordingly, Receiving Party agrees to: (i) protect the Disclosing Party's Confidential Information using the same degree of care (but in no event less than reasonable care) that it uses to protect its own Confidential Information of a similar nature; (ii) limit use of Disclosing Party's Confidential Information for purposes consistent with these General Terms, and (iii) use commercially reasonable efforts to limit access to Disclosing Party's Confidential Information to its employees, contractors and agents or those of its Affiliates who have a bona fide need to access such Confidential Information for purposes consistent with these General Terms and who are subject to confidentiality obligations no less stringent than those herein. Splunk recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

(B) **Compelled Disclosure of Confidential Information**. Notwithstanding the foregoing terms, the Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law enforcement agencies or regulators to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a Party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

18. Payment

This agreement is intended only for when you purchase from an authorized reseller; the payment terms are between you and the authorized reseller.

19. Splunk's Warranties

(A) **Relationship to Applicable Law**. We will not seek to limit our liability, or any of your warranties, rights and remedies, to the extent the limits are not permitted by applicable law (e.g., warranties, remedies or liabilities that cannot be excluded by applicable law).

(B) **General Corporate Warranty**. Splunk warrants that it has the legal power and authority to enter into these General Terms.

(C) **Hosted Services Warranty**. Splunk warrants that during the applicable Term: (i) Splunk will not materially decrease the overall functionality of the Hosted Services; and (ii) the Hosted Services will perform materially in accordance with the applicable Documentation. Our sole and exclusive liability, and your sole and exclusive remedy for any breach of these warranties, will be your right to terminate the applicable Hosted Services Purchased Offering, and we will refund to you any prepaid but unused Fees for the remainder of the Term.

(D) **On-Premise Product Warranty**. Splunk warrants that for a period of ninety (90) days from the Delivery of an On-Premise Product, the On-Premise Product will substantially perform the material functions described in the applicable Documentation for such On-Premise Product, when used in accordance with the applicable Documentation. Splunk's sole liability, and your sole remedy, for any failure of the On-Premise Product to conform to the foregoing warranty, is for Splunk to do one of the following (at Splunk's sole option and discretion) (i) modify, or provide an Enhancement for, the On-Premise Product so that it conforms to the foregoing warranty, (ii) replace your copy of the On-Premise Product with a copy that conforms to the foregoing warranty, or (iii) terminate the Purchased Offering with respect to the non-conforming On-Premise Product and refund the Fees paid by you for such non-conforming On-Premise Product.

(E) **Disclaimer of Implied Warranties**. **Except as expressly set forth above, the Offerings are provided "as is" with no warranties or representations whatsoever, express or implied. Splunk and its suppliers and licensors disclaim all warranties and representations, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, noninfringement, or quiet enjoyment, and any warranties arising out of course of dealing or trade usage. Splunk does not warrant that use of Offerings will be uninterrupted, error free or secure, or that all defects will be corrected**. IN THE EVENT OF A BREACH OF WARRANTY, THE U.S. GOVERNMENT RESERVES ALL RIGHTS AND REMEDIES UNDER THE CONTRACT, THE FEDERAL ACQUISITION REGULATIONS, AND THE CONTRACT DISPUTES ACT, 41 U.S.C. 7101-7109.

20. Ownership

(A) **Offerings**. As between you and Splunk, Splunk owns and reserves all right, title, and interest in and to the Offerings, developer tools and other Splunk materials, including all intellectual property rights therein. We retain rights in anything delivered or developed by us or on our behalf under these General Terms. No rights are granted to you other than as expressly set forth in these General Terms.

(B) **Customer Content**. You own and reserve all right, title and interest in your Customer Content. By sending Customer Content to a Hosted Service, you grant us a worldwide, royalty free, non-exclusive license to access and use the Customer Content for purposes of providing you the Hosted Service.

(C) **Feedback**. You have no obligation to provide us with ideas for improvement, suggestions or other feedback (collectively, "**Feedback**") in connection with an Offering, unless otherwise expressly set forth in the applicable Order. If, however, you provide any Feedback, you hereby grant to Splunk a non-exclusive, transferable, irrevocable, worldwide, royalty-free license (with rights to sublicense) to make, use, sell, offer to sell, reproduce, modify, distribute, make available, publicly display and perform, disclose and otherwise commercially exploit the Feedback.

21. Term and Termination

(A) **Term and Renewal**. These General Terms will commence upon the Effective Date and will remain in effect until the expiration of all applicable Purchased Offerings, unless earlier terminated pursuant to this Section. Termination of a specific Purchased Offering will not affect the Term of any other Purchased Offering. Termination of these General Terms will have the effect of terminating all Purchased Offerings. Grounds for terminating a Purchased Offering (e.g., for non-payment), that are specific to the Purchased Offering, will not be grounds to terminate Purchased Offerings where no breach exists Unless indicated otherwise in an Order, the Term of a Purchased Offering (and these General Terms) may be renewed for an additional period of time equal to the length of the preceding Term or other agreed upon period, upon the issuance of a purchase order by you, or execution of an Order document, or other agreement for renewal by you.

(B) **Termination**. When the Customer is an instrumentality of the U.S., the Prime Contractor may have recourse against the United States for any alleged breach of this Agreement by initiating a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, for so long as the Term of the Customer's license subject to the dispute has not expired, Splunk shall proceed diligently with performance of said license pursuant to this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.. For clarity, there is no ongoing obligation for Splunk to continue to provide any Offering after the expiration of the applicable Term. Upon any expiration or termination of a Purchased Offering, the rights and licenses granted to you for that Purchased Offering will automatically terminate, and you agree to immediately (i) cease using and accessing the Offering, (ii) return or destroy all copies of any On-Premise Products and other Splunk materials and Splunk Confidential Information in your possession or control, and, (iii) upon our request, certify in writing the completion of such return or destruction. Upon termination of these General Terms or any Purchased Offering, Splunk will have no obligation to refund any Fees or other amounts received from you during the Term. Notwithstanding any early termination above, except for your termination for our uncured material breach, you will still be required to pay all Fees payable under an Order.

(C) **Survival**. The termination or expiration of these General Terms will not affect any provisions herein which by their nature survive termination or expiration, including the provisions that deal with the following subject matters: definitions, ownership of intellectual property, confidentiality, payment obligations, effect of termination, limitation of liability, privacy, and the "Miscellaneous" section in these General Terms.

(D) **Suspension of Service.**. If your activities violate the Hosted Services Acceptable Use Policy, Splunk may, without limiting its other rights and remedies, temporarily suspend the applicable Hosted Service until the issue is resolved. For the avoidance of doubt, suspensions of the applicable Hosted Service(s) will have no impact on the then-current Term, its associated payments or the relevant duration of the subscription Term. For clarity, there is no ongoing obligation for Splunk to continue to provide any Offering after the expiration of the applicable Term. . .

22. Limitation of Liability

In no event will the aggregate liability of either party, together with any of its Affiliates, arising out of or related to any Purchased Offering exceed the total amount paid by the Ordering Activity to Splunk for that Purchased Offering in the twelve (12) months preceding the first incident out of which liability arose For the avoidance of doubt, the foregoing limitation will not limit your obligations under the "Payment" section above, and will not be deemed to limit your rights to any service level credits under any applicable Service Level Schedule. Furthermore, the cap above will not be deemed to limit Splunk's right to recover amounts for your use of an Offering in excess of the Capacity purchased or use outside of Internal Business Purposes.

In no event will either party or its Affiliates have any liability arising out of or related to these General Terms for any lost profits, revenues, goodwill, or indirect, special, incidental, consequential, cover, business interruption or punitive damages.

The foregoing limitations will apply whether the action is in contract or tort and regardless of the theory of liability, even if a party or its Affiliates have been advised of the possibility of such damages or if a party's or its Affiliates' remedy otherwise fails of its essential purpose.

The limitation of liability herein will not apply to a party's infringement of the other party's intellectual property rights, indemnification obligations, Customer's breach of sections 7(i), 16(E), or 16(F), or the fraud, gross negligence or willful misconduct of a party.

The foregoing disclaimers of damages will also not apply to the extent prohibited by law. Some jurisdictions do not allow the exclusion or limitation of certain damages. To the extent such a law applies to you, some or all of the exclusions or limitations set forth above may not apply to you, and you may have additional rights. THIS AGREEMENT ESTABLISHES LIMITATIONS ON THE LIABILITY OF THE PARTIES. NOTHING IN THESE GENERAL TERMS SHALL IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER AGAINST THE PRIME CONTRACTOR FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733. FURTHERMORE, THIS CLAUSE SHALL NOT IMPAIR NOR PREJUDICE THE U.S. GOVERNMENT'S RIGHT TO EXPRESS REMEDIES PROVIDED IN THE GSA SCHEDULE CONTRACT (E.G., CLAUSE 552.238-75 – PRICE REDUCTIONS, CLAUSE 52.212-4(H) – PATENT INDEMNIFICATION, AND GSAR 552.215-72 – PRICE ADJUSTMENT – FAILURE TO PROVIDE ACCURATE INFORMATION).

23. Indemnity

(A) **Our Indemnification to You**. Splunk has the right to intervene to defend and indemnify you, and pay all damages (including attorneys' fees and costs) awarded against you, or that are agreed to in a settlement, to the extent a claim, demand, suit or proceeding is made or brought against you or your Affiliates by a third party (including those brought by the government) alleging that a Purchased Offering infringes or misappropriates such third party's patent, copyright, trademark or trade secret (a "**Customer Claim**"). Splunk will have no obligation under the foregoing provision to the extent a Customer Claim arises from your breach of these General Terms, your Customer Content, Third-Party Extension, or the combination of the Offering with: (i) Customer Content; (ii) Third-Party Extensions; (iii) any software other than software provided by Splunk; or (iv) any hardware or equipment. However, Splunk will indemnify against combination claims to the extent (y) the combined software is necessary for the normal operation of the Purchased Offering (e.g., an operating system), or (z) the Purchased Offering provides substantially all the essential elements of the asserted infringement or misappropriation claim. Splunk may in its sole discretion and at no cost to you: (1) modify any Purchased Offering so that it no longer infringes or misappropriates a third party right, (2) obtain a license for your continued use of the Purchased Offering, in accordance with these General Terms, or (3) terminate the Purchased Offering and refund to you any prepaid fees covering the unexpired Term. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

(B) **Your Indemnification to Us**. Reserved.

(C) **Mutual Indemnity**. Splunk has the right to intervene to defend (or settle), indemnify and hold harmless at its expense, any action brought against the other party by a third party to the extent that it is based upon a claim for bodily injury, personal injury (including death) to any person, or damage to tangible property resulting from the negligent acts or willful misconduct of the indemnifying party or its personnel hereunder, and will pay any reasonable, direct, out-of-pocket costs, damages and reasonable attorneys' fees attributable to such claim that are awarded against the indemnified party (or are payable in settlement by the indemnified party).

(D) **Process for Indemnification**. The indemnification obligations above are subject to the party seeking indemnification to: (i) provide the other party with prompt written notice of the specific claim; (ii) give the indemnifying party control of the defense and settlement of the claim (except that the indemnifying party may not settle any claim that requires any action or forbearance on the indemnified party's part without their prior consent, which will not unreasonably withhold or delay); and (iii) gives the indemnifying party all reasonable assistance, at such party's expense.

24. Updates to Offerings

Our Offerings and policies may be updated over the course of our relationship. From time to time, Splunk may update or modify an Offering and our policies, provided that: (a) the change and modification applies to all customers generally, and are not targeted to any particular customer; (b) no such change or modification will impose additional fees on you during the applicable Term or additional restrictions on your use of the Offering, or alter our liability or the allocation of risk between us under these General Terms; (c) no such change or modification will materially reduce the security protections or overall functionality of the applicable Offering; and (d) any such change or modification will apply only prospectively, and will not apply to any breach or dispute that arose between the parties prior to the effective date of the change or modification.

25. Governing Law

These General Terms will be governed by and construed in accordance with the Federal laws of the United States.

Neither the Uniform Computer Information Transactions Act nor the United Nations Convention for the International Sale of Goods will apply to these General Terms.

26. Use of Customer Name

You agree that we may add your name to our customer list and identify you as a Splunk customer on Splunk's websites to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71. Any further public use of your name in connection with Splunk marketing activities (e.g., press releases) will require your prior written approval.

27. Miscellaneous

(A) **Different Terms**. As pertaining to Splunk's performance under this agreement, Splunk expressly rejects terms or conditions in any Customer purchase order or other similar document that are different from or additional to the terms and conditions set forth in these General Terms. Such different or additional terms and conditions will not become a part of the agreement between the parties notwithstanding any subsequent acknowledgement, invoice or license key that Splunk may issue unless they have been agreed to in writing as an Order.

(B) **No Future Functionality.** You agree that your purchase of any Offering is not contingent on the delivery of any future functionality or features, or dependent on any oral or written statements made by Splunk regarding future functionality or features.

(C) **Notices**. Except as otherwise specified in these General Terms, all notices related to these General Terms will be sent in writing to the addresses set forth in the applicable Order, or to such other address as may be specified by either party to the other party, and will be effective upon (i) personal delivery, (ii) the second business day after mailing, or (c), except for notices of termination or an indemnifiable claim ("**Legal Notices**"), which shall clearly be identifiable as Legal Notices, the day of sending by email. Billing-related notices to Customer will be addressed to the relevant billing contact designated by Customer. All other notices to Customer will be addressed to the relevant system administrator designated by Customer.

(D) **Assignment**. Neither party may assign, delegate or transfer these General Terms, in whole or in part, by agreement, operation of law or otherwise without the prior written consent of the other party, however Splunk may assign these General Terms in whole or in part to an Affiliate or in connection with an internal reorganization or a merger, acquisition, or sale of all or substantially all of Splunk's assets to which these General Terms relates. Any attempt to assign these General Terms other than as permitted herein will be null and void. Subject to the foregoing, these General Terms will bind and inure to the benefit of the parties' permitted successors and assigns.

(E) **U.S. Government Use Terms**. Splunk provides Offerings for U.S. federal government end use solely in accordance with the following: Government technical data and rights related to Offerings include only those rights customarily provided to the public as defined in these General Terms. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software) and, for Department of Defense transactions, DFARS 252.227-7015 (Technical Data–Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Commercial Computer Software Documentation. If a government agency has a need for rights not conveyed under these terms, it must negotiate with Splunk to

determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

(F) **Waiver; Severability**. The waiver by either party of a breach of or a default under these General Terms will not be effective unless in writing. The failure by either party to enforce any provisions of these General Terms will not constitute a waiver of any other right hereunder or of any subsequent enforcement of that or any other provisions. If a court of competent jurisdiction holds any provision of these General Terms invalid or unenforceable, the remaining provisions of these General Terms will remain in full force and effect, and the provision affected will be construed so as to be enforceable to the maximum extent permissible by law.

(G) **Integration; Entire Agreement**. These General Terms along with any additional terms incorporated herein by reference, constitute the complete and exclusive understanding and agreement between the parties and supersedes any and all prior or contemporaneous agreements, communications and understandings, written or oral, relating to their subject matter. Except as otherwise expressly set forth herein, any waiver, modification or amendment of any provision of these General Terms will be effective only if in writing and signed by duly authorized representatives of both parties.

(H) **Force Majeure**. Excusable delays shall be governed by FAR 52.212-4(f). For clarity, notifications to the contracting officer will be provided by the Prime Contractor.(I) **Independent Contractors; No Third-Party Beneficiaries**. The parties are independent contractors. These General Terms does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. There are no third-party beneficiaries of these General Terms. Neither party has the authority to bind or act on behalf of the other party in any capacity or circumstance whether by contract or otherwise.

General Terms Definitions Exhibit

"**Affiliates**" means a corporation, partnership or other entity controlling, controlled by or under common control with such party, but only so long as such control continues to exist. For purposes of this definition, "control" means ownership, directly or indirectly, of greater than fifty percent (50%) of the voting rights in such entity (or, in the case of a noncorporate entity, equivalent rights).

"**Capacity**" means the measurement of usage of an Offering (e.g., aggregate daily volume of data indexed, specific source type rights, number of search and compute units, number of monitored accounts, virtual CPUs, user seats, use cases, storage capacity, etc.) that is purchased for an Offering, as set forth in the applicable Order. The Capacities for each of our Offerings can be found here: https://www.splunk.com/en_us/legal/licensed-capacity.html.

"**CCPA**" means the California Consumer Privacy Act of 2018.

"**Confidential Information**" means all nonpublic information disclosed by a party ("**Disclosing Party**") to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as "confidential" or that, given the nature of the information or circumstances surrounding its disclosure, should reasonably be understood to be confidential. Notwithstanding the foregoing, "Confidential Information" does not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party. When the end user is the Federal Government, neither this Agreement nor the pricing terms are confidential information notwithstanding any such markings.

"**Content Subscription**" means the right of Customer to receive content applicable to an Offering (e.g., models, templates, searches, playbooks, rules and configurations, as described in the relevant Documentation) on a periodic basis over the applicable Term. Content Subscriptions are purchased as an add-on service and are identified in an Order.

"**Customer Content**" means any data that is ingested by or on behalf of you into an Offering from your internal data sources.

"**Delivery**" means the date of Splunk's initial delivery of the license key for the applicable Offering or, for Hosted Services, the date Splunk makes the applicable Offering available to you for access and use.

"**Documentation**" means the online user guides, documentation and help and training materials published on Splunk's website (such as at http://docs.splunk.com/Documentation) or accessible through the applicable Offering, as may be updated by Splunk from time to time.

"**Effective Date**" means the date of your Order.

"**Enhancements**" means any updates, upgrades, releases, fixes, enhancements or modifications to a Purchased Offering made generally commercially available by Splunk to its customers under the terms and conditions in the Support Exhibit.

"**Extension**" means any separately downloadable or accessible suite, configuration file, add-on, technical add-on, example module, command, function, playbook, content or application that extends the features or functionality of the applicable Offering.

"**Fees**" means the fees that are applicable to an Offering, as identified in the Order.

"**GDPR**" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) as updated, amended or replaced from time to time.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as amended and supplemented by the Health Information Technology for Economic and Clinical Health Act.

"**Hosted Service**" means a technology service hosted by or on behalf of Splunk and provided to you.

"**Internal Business Purpose**" means your use of an Offering for your own internal business operations, based on the analysis, monitoring or processing of your data from your systems, networks and devices. Such use does not include use on a service bureau basis or otherwise to provide services to, or process data for, any third party, or otherwise use to monitor or service the systems, networks and devices of third parties.

"**ITAR Data**" means information protected by the International Traffic in Arms Regulations.

"**Offerings**" means the products, services and other offerings that Splunk makes generally available, including without limitation On-Premise Products, Hosted Services, Support Programs, Content Subscriptions and Configuration and Implementation Services.

"**On-Premise Product**" means the Splunk software that is delivered to you and deployed and operated by you or on your behalf on hardware designated by you, and any Enhancements made available to you by Splunk.

"**Open Source Software**" means software that is licensed under a license approved by the Open Source Initiative or similar freeware license, with terms requiring that such software code be (i) disclosed or distributed in source code or object code form, (ii) licensed for the purpose of making derivative works, and/or (iii) redistributed under the same license terms.

"**Orders**" means Splunk's quote or ordering document (including online order form) accepted by you via your purchase order or other ordering document submitted to Splunk (directly or indirectly through an authorized reseller) to order Offerings, which references the Offering, Capacity, pricing and other applicable terms set forth in an applicable Splunk quote or ordering document. With respect to Splunk's performance under these General Terms, Orders do not include the terms of any preprinted terms on your purchase order or other terms on a purchase order that are additional or inconsistent with the terms of these General Terms unless such terms are included in the quote (directly to Customer or indirectly to the reseller, as applicable).

"**PCI Data**" means credit card information within the scope of the Payment Card Industry Data Security Standard.

"**PHI Data**" means any protected health data, as defined under HIPAA.

"**Prime Contractor**" means Carahsoft Technology Corp. or another third party who is in direct privity of contract with the Customer and through whom the Purchased Offerings are being resold pursuant to the terms of this Agreement.

"**Purchased Offerings**" means the services, subscriptions and licenses to Offerings that are acquired by you under Orders, whether directly or through an authorized reseller.

"**Service Level Schedule**" means a Splunk policy that applies to the availability and uptime of a Hosted Service and which, if applicable, offers service credits as set forth therein.

"**Splunkbase**" means Splunk's online directory of or platform for Extensions, currently located at https://splunkbase.splunk.com and any and all successors, replacements, new versions, derivatives, updates and upgrades and any other similar platform(s) owned and/or controlled by Splunk.

"**Splunk Developer Tool**" means the standard application programming interface, configurations, software development kits, libraries, command line interface tools, other tooling (including scaffolding and data generation tools), integrated development environment plug-ins or extensions, code examples, tutorials, reference guides and other related materials identified and provided by Splunk to facilitate or enable the creation of Extensions or otherwise support interoperability between the Software and your system or environment.

"**Splunk Extensions**" means Extensions made available through Splunkbase that are identified on Splunkbase as built by Splunk (and not by any third party).

"**Support Programs**" are the Support Programs offered by Splunk and identified here: http://www.splunk.com/en_us/support-and-services/support-programs.html

"**Term**" means the duration of your subscription or license to the applicable Offering that starts and ends on the date listed on the applicable Order. If no start date is specified in an Order, the start date will be the Delivery date of the Offering.

"**Third-Party Content**" means information, data, technology or materials made available to you by any third party that you license and add to a Hosted Service or direct Splunk to install in connection with a Hosted Service. Third-Party Content includes but is not limited to, Third-Party Extensions, web-based or offline software applications, data service or content that are provided by third parties.

"**Usage Data**" means data generated from the usage, configuration, deployment, access and performance of an Offering. For example, this may include such things as information about your operating environment, such as your network and systems architecture, or sessions, such as page loads and session views, duration, or interactions, errors, number of searches, source types and format (e.g., json, xml, csv), ingest volume, number of active and licensed users, or search concurrency. Usage Data does not include Customer Content.

Exhibit A to Splunk General Terms
Support Terms

This Support Exhibit forms a part of the Splunk General Terms and governs your purchase, and Splunk's provision of Support Services.

1. Support Programs

Support Programs purchased as part of a Purchased Offering will be identified in your applicable Order. Splunk will provide you the level of Support Services described under the purchased Support Program, subject to your payment of applicable Fees. "**Support Programs**" are the Support Programs offered by Splunk and identified here: http://www.splunk.com/en_us/support-and-services/support-programs.html.

2. Support Services

"**Support Services**" include technical support for your Purchased Offerings, and, when available, the provision of Enhancements for your Purchased Offerings, subject to the Support Policy described below. Technical support under a Support Program is available via email or web portal, and certain Support Programs also make support available via telephone. Support Services will be delivered by a member of Splunk's technical support team during the regional hours of operation applicable under the Support Program. Support Services are delivered in English unless you are in a location where we have made localized Support Services available.

3. Support Policy

Our Support Policy, provided here: https://www.splunk.com/en_us/legal/splunk-software-support-policy.html ("**Support Policy**"), current as of the Effective Date, is attached to these General Terms as Exhibit C for ease of your reference. It describes the duration of our Support Services for certain Splunk On-Premise Products and other policies associated with our Support Services.

As we release new versions for our Offerings, we discontinue Support Services for certain older versions. Our Support Policy sets forth the schedule for the duration of support, and end of support, for Offering versions. The current versions of our Offerings that are supported under our Support Policy, and will be our "**Supported Versions**" herein. For the avoidance of doubt, the Support Policy may not apply to Hosted Services, and the product and services version we make available as our Hosted Services will be deemed Supported Versions herein.

4. Case Priority

Each Support Program offers different support levels for your case priority levels. When submitting a case, you will select the priority for initial response by logging the case online, in accordance with the priority guidelines set forth under your Support Program. When the case is received, we may in good faith change the priority if the issue does not conform to the criteria for the selected priority. When that happens, we will provide you with notice (electronic or otherwise) of such change.

5. Exclusions

We will have no obligation to provide support for issues caused by any of the following (each, a "**Customer Generated Error**"): (i) modifications to an Offering not made by Splunk; (ii) use of an Offering other than as authorized in the Agreement or as provided in the applicable Documentation; (iii) damage to the machine on which an On-Premise Product is installed; (iv) use of a version of an Offering other than the Supported Version; (vi) third-party products that are not expressly noted in the Documentation as supported by Splunk; or (vi) conflicts related to replacing or installing hardware, drivers, and software that are not expressly supported by Splunk and described in the applicable Documentation. If we determine that support requested by you is for an issue caused by a Customer Generated Error, we will notify you of that fact as soon as reasonably possible under the circumstances. If you agree that we should

provide support for the Customer Generated Error via a confirming email, then we will have the right to invoice you at our then-current time and materials rates for any such support provided by us.

6. Support for Splunk Extensions

Only Splunk Extensions that are labeled as "**Splunk Supported**" on Splunkbase, or other Splunk-branded marketplace, are eligible for support, and this support is limited. For those labeled Splunk Supported, we will provide an initial response and acknowledgement in accordance with the P3 terms that are applicable in the applicable Support Program. Enhancements for Splunk Extensions labeled as Splunk Supported when made available. No other terms of a Support Program will apply to a Splunk Application. For those labeled as "**Not Supported**," Splunk will have no support obligations.

7. Authorized Support Contacts

You are entitled to have a certain number of Support Contacts under each Support Program. "**Support Contacts**" means the individual(s) specified by you that are authorized to submit support cases.

The number of Support Contacts will be based on the Capacity of the Offering purchased, and the applicable Support Program. The number of Support Contacts will be set forth in customer's entitlement information on the Splunk support portal.

We only take support requests from, and communicate with, your Support Contacts in connection with support cases. We strongly recommend that your Support Contact(s) are trained on the applicable Offering. In order to designate Support Contacts, you must provide the individual's primary email address and Splunk.com login ID.

8. Defect Resolution

Should we determine that an Offering has a defect, we will, at our sole option, repair the defect in the version of the Offering that you are then currently using or instruct you to install a newer version of the Offering with that defect repaired. We reserve the right to provide you with a workaround in lieu of fixing a defect should we in our sole judgment determine that it is more effective to do so.

9. Your Assistance

Should you report a purported defect or error in an Offering, we may require you to provide us with the following information: (a) a general description of your operating environment; (b) a list of all hardware components, operating systems and networks; (c) a reproducible test case; and (d) any log files, trace and systems files. Your failure to provide this information may prevent us from identifying and fixing that purported defect.

10. Changes to Support Programs

You acknowledge that, subject to the Support Policy, and subject to any commitment we have under an Order with you, we have the right to discontinue the manufacture, development, sale or support of any Offering, at any time, in our sole discretion. We further reserve the right to alter Support Programs from time to time, using reasonable discretion, but in no event will such alterations, during the Term of any Order, result in diminished Support Services from the level of your applicable purchased Support Program.

.

Exhibit B to Splunk General Terms
Configuration and Implementation Services

This Configuration and Implementation Services Exhibit forms a part of the Splunk General Terms and governs your purchase, and Splunk's provision of Configuration and Implementation Services.

Capitalized terms below are defined in the General Terms, this Exhibit or in the Definition Exhibit attached to this Exhibit.

1. Services and Statements of Work

We will perform the C&I Services for you that are set forth in the applicable Statements of Work. You will pay the Fees under each Statement of Work in accordance with these General Terms, or otherwise as we may expressly agree in the applicable Statement of Work.

In each Statement of Work, we will designate our primary point of contact for you for all matters relating to the applicable C&I Services (which we may change from time to time upon notice).

2. Our Personnel

Qualifications. The Personnel we assign to perform the C&I Services will be qualified, skilled, experienced and otherwise fit for the performance of the C&I Services. If you, in your reasonable judgement, determine that Personnel assigned to your project are unfit, we will in good faith discuss alternatives, and we will replace Personnel as reasonably necessary. You acknowledge that any replacement may cause delay in the performance of the C&I Services.

Personnel Conduct. Our Personnel are subject to our Splunk Code of Conduct and Ethics https://investors.splunk.com/code-business-conduct-and-ethics-1, which includes, without limitation, an obligation to comply with our policies on protecting customer information, prohibitions on illegal drugs and any impaired job performance, avoiding conflicts of interest, and acting ethically at all times. We also background check our employees, per the Section below.

Use of Subcontractors. We reserve the right to use subcontractors in performance of the C&I Services, provided: (a) any subcontractor we use meets the requirements herein and conditions of these General Terms and the Statement of Work; (b) we will be responsible for the subcontractor's compliance with the terms herein and the Statement of Work; and (c) upon your request or inquiry, we will identify any subcontractor that we are using, or plan to use, for C&I Services, and will cooperate in good faith to provide you with all relevant information regarding such subcontractors.

No Employee Benefits. We acknowledge and agree that our Personnel are not eligible for or entitled to receive any compensation, benefits, or other incidents of employment that you make available to your employees. We are solely responsible for all employment related taxes, expenses, withholdings, and other similar statutory obligations arising out of the relationship between us and our Personnel and the performance of C&I Services by such Personnel.

3. Our Background Checks, Security and Compliance Obligations

Compliance with Your Security Program. While on your premises, our Personnel will comply with your security practices and procedures generally prescribed by you for onsite visitors and service providers. However, any requirement that is in addition to the compliance requirements set forth in this Schedule (e.g., background checks that are different from the background checks described herein) must be expressly set forth in a Statement of Work. We agree to discuss in good faith any condition or requirement you may have for our Personnel that are different from standard policies, however any additional requirement may delay C&I Services, and must be vetted and implemented by mutual agreement of the parties and expressly set forth in a Statement of Work. Splunk does not guarantee that it will be able to meet any additional requested requirements.

Our Security Practices. We implement and follow an enterprise security program, with the policies, plans, and procedures set forth here www.splunk.com/prof-serv-isa. Our Personnel will be subject to the data protection and confidentiality obligations set forth in these General Terms with respect to any of your data that we may have access to in connection with the C&I Services.

Background Checks. For U.S.-based projects, we will not assign an employee to perform C&I Services under a Statement of Work unless we have run the following background check on the employee: Criminal Felony & Misdemeanor; SSN Validation; Federal Criminal; SSN Trace; Employment Report – Three (3) Employers; Education Report – One (1) Institution; Global Sanctions & Enforcement; Prohibited Parties; Widescreen Plus National Criminal Search. You acknowledge that such background checks may not be permitted or customary outside the United States.

Permissions for Access. In the event you require any Personnel to sign any waivers, releases, or other documents as a condition to gain access to your premises for performance of the C&I Services ("**Access Documents**"), you agree: (a) that Personnel who will be required to sign Access Documents will sign on behalf of Splunk; (b) that any additional or conflicting terms in Access Documents with these General Terms will have no effect; and (c) you will pursue any claims for breach of any terms in the Access Documents against Splunk and not the individual signing.

4. Your Materials

We will have no rights in or to any Customer Materials, however you grant us the right to use Customer Materials in order to provide the C&I Services. Nothing in these General Terms will deemed to transfer to us any ownership of Customer Materials.

5. C&I Services Materials and Customizations Unique to You

C&I Services Materials. The C&I Services we perform (e.g., configuration of our Offerings), and the C&I Services Materials we offer, create, and deliver to you in connection with the C&I Services, are generally applicable to our business, and therefore we require the right to be able to re-use the C&I Services Materials we create for one customer in connection with all of our customers. For the avoidance of doubt, our use of the C&I Services Materials created for you in connection with C&I Services will comply with our ongoing obligations and restrictions with respect to your Customer Materials and your Confidential Information, and we will not identify you in any way in connection with our further use of such C&I Services Materials.

Customer Owned Work Product. However, in the unlikely event that the parties agree that C&I Services Materials for a project are custom work product unique to your business, and not applicable to other customers generally, we will transfer ownership to those agreed C&I Services Materials to you under the applicable Statement of Work. C&I Services Materials must be expressly identified as "**Customer Owned Work Product**" under a Statement of Work for ownership to pass to you. Subject to payment of applicable Fees under the Statement of Work, we hereby assign to you all rights, title and interest (including all Intellectual Property Rights therein) in and to all C&I Services Materials identified as Customer Owned Work Product (but excluding all Splunk Preexisting IP incorporated into the Customer Owned Work Product). At your request and expense, we will assist and cooperate with you in all reasonable respects and will execute documents, and take such further acts reasonably requested by you to enable you to acquire, transfer, maintain, perfect and enforce your ownership rights in such Customer Owned Work Product.

Our Ownership. Subject to your ownership rights in Customer Owned Work Product and Customer Materials, we will own all rights in and to all C&I Services Materials.

License Rights. For those C&I Services Materials that are not Customer Owned Work Product, you will have the right to access and use those C&I Services Materials in connection with your applicable Offerings, and those rights will be of the same scope and duration as your rights to the underlying Offering.

6. C&I Services Warranty

We warrant that the C&I Services will be performed in a good and workmanlike manner consistent with applicable industry standards. This warranty will be in effect for a period of thirty (30) days from the completion of any C&I Services. As your sole and exclusive remedy and our entire liability for any breach of the foregoing warranty, we will, at our option and expense, promptly re-perform any C&I Services that fail to meet this warranty or refund to you the fees paid for the non-conforming C&I Services.

7. Your Cooperation

You acknowledge that your timely provision of (and our access to) your facilities, equipment, assistance, cooperation, data, information and materials from your officers, agents and employees (the "**Cooperation**") is essential to Splunk's performance of the C&I Services. We will not be liable for any delay or deficiency in performing the C&I Services if you do not provide the necessary Cooperation. As part of the Cooperation, you will (1) designate a project manager or technical lead to liaise with us while we perform the C&I Services; (2) allocate and engage additional resources as may be required to assist us in performing the C&I Services; and (3) making available to us any data, information and any other materials reasonably required by us to perform the C&I Services, including any data, information or materials specifically identified in the Statement of Work.

8. Insurance

Throughout any period of C&I Services we perform for you, we will maintain insurance policies in the types and amounts described below at our own expense:

Commercial General Liability Insurance with a limit of not less than $1,000,000 per occurrence and a general aggregate limit of not less than $2,000,000.

Business Auto Insurance with a limit of not less than $1,000,000 per accident. Such Insurance will cover liability arising out of "hired and non-owned" automobiles.

Worker's Compensation Insurance as required by workers' compensation, occupational disease and occupational health and safety laws, statutes and regulations.

Technology Errors & Omissions Insurance with a limit of not less than $3,000,000.

Umbrella/Excess Insurance with a limit of not less than $3,000,000.

9. Change Order Process

You may submit written requests to us to change the scope of C&I Services described in a Statement of Work (each such request, a "**Change Order Request**"). If we elect to consider a Change Order Request, then we will promptly notify you if we believe that the Change Order Request requires an adjustment to the fees or to the schedule for the performance of the C&I Services. In such event, the parties will negotiate in good faith a reasonable and equitable adjustment to the fees and/or schedule, as applicable. We will continue to perform C&I Services pursuant to the existing Statement of Work and will have no obligation to perform any Change Order Request unless and until the parties have agreed in writing to such an equitable adjustment.

10. Expenses

Unless otherwise specified in the Statement of Work, we will not charge you for our expenses we incur in connection with a Statement of Work. Our daily C&I Services rates are inclusive of any expenses. In the event the parties agree that expenses are reimbursable under a Statement of Work, we will mutually agree on any travel policy and any required documentation for re-imbursement.

11. Prepaid C&I Services

Unless otherwise expressly stated in a Statement of Work, all prepaid C&I Services must be redeemed within twelve (12) months from the date of purchase/invoice.

Configuration and Implementation Services Definitions Exhibit

"**C&I Services**" means the services outlined in the Statement of Work.

"**C&I Services Materials**" means the materials and other deliverables that are provided to you as part of the C&I Services, and any materials, technology, know-how and other innovations of any kind that we or our Personnel may create or reduce to practice in the course of performing the C&I Services, including without limitation all improvements or modifications to our proprietary technology, and all Intellectual Property Rights therein.

"**Customer Materials**" means the data, information, and materials you provide to us in connection with your use of the C&I Services.

"**Fees**" means the fees that are applicable to the C&I Services, as identified in the Statement of Work.

"**Intellectual Property Rights**" means all worldwide intellectual property rights, including copyrights and other rights in works of authorship; rights in trademarks, tradenames, and other designations of source or origin; rights in trade secrets and confidential information; and patents and patent applications.

"**Offerings**" means the products, services and other offerings that Splunk makes generally available for purchase and use.

"**Orders**" means Splunk's quote or ordering document (including online order form) accepted by you in writing via your purchase order or other ordering document submitted to Splunk (directly or indirectly through an authorized reseller) to order C&I Services.

"**Personnel**" means any employee, consultant, contractor, or subcontractor of Splunk.

"**Splunk Preexisting IP**" means, with respect to any C&I Services Materials, all associated Splunk Technology and all Intellectual Property Rights created or acquired: (a) prior to the date of the Statement of Work that includes such C&I Services Materials, or (b) after the date of such Statement of Work but independently of the C&I Services provided under such Statement of Work.

"**Statement of Work**" means the statements of work and/or any all applicable Orders that describe the specific services to be performed by Splunk, including any materials and deliverables to be delivered by Splunk.

Exhibit C to Splunk General Terms

Splunk Support Policy

Splunk Inc. provides Support Services for Purchased Offerings as set forth in the Splunk General Terms to Customers with active subscriptions to a Support Program. Purchased Offerings may comprise either or both On-Premise Products ("Products") and Hosted Services Offerings ("Services"). This Policy details the timelines during which specific Product versions are eligible for Support Services, as well as other policies that determine eligibility of both Products and Services for Support Services.

Product Version Numbering

Each Product release is identified with a numerical version comprising three sets of digits separated by decimals. The digit(s) to the left of the first decimal represent the major version, the digit(s) to the right of the first decimal represent the minor version, and the digit(s) to the right of the second decimal represent the maintenance version. Any version number that specifies the second digit(s) is referred to as a minor version, even if it is the first release of a new major version. For example, 7.0, 7.1, and 7.2 are all minor versions of the 7.x major version.

For the purposes of determining the Supported Version, any maintenance release that may be provided for a given minor version is considered part of that version and does not alter the minor version release date.

Product Supported Version Timelines

Any given Product version is considered a Supported Version ("Supported") for a finite period following its release. The particular timelines for each Product are detailed below for all recent Product versions. Note that any prior version of any of these Products not listed here is End of Support.

Once a Product version is no longer Supported, it is considered End of Support. End of Support Product versions are not eligible for Support Services, and any software, associated product documentation, and Splunk Extensions that are not compatible with Supported Versions will no longer be available to Customers.

Splunk Core Products

Splunk Enterprise (Version 7.0 Onward)

Splunk Light (Version 7.x Only)

Splunk Analytics for Hadoop

Splunk Data Fabric Search

Splunk Data Stream Processor

Each minor version of these Products is Supported for twenty-four (24) months from the release of that minor version.

Splunk Enterprise & Splunk Light (Version 6.x Only)
Each minor version of Splunk Enterprise 6.x and Splunk Light 6.x was Supported from release of that minor version through the October 22, 2019 release of Splunk Enterprise 8.0. All Splunk Enterprise 6.x and all Splunk Light 6.x versions are End of Support.

Splunk Universal Forwarder (Version 7.0 Onward)
Starting with version 7.0, each minor version of Splunk Universal Forwarder is Supported from release for a total of sixty (60) months. During the first twenty-four (24) months from release of each version, the targeted Support response times will be determined by issue severity and priority, per the terms of the purchased Support Program. For the subsequent thirty-six (36) months, the targeted Support response times will be limited to the P3 level.

Splunk Universal Forwarder (Version 6.x Only)
Each minor version of Splunk Universal Forwarder version 6.x was Supported from release of that minor version through the October 22, 2019 release of Splunk Universal Forwarder 8.0.
Universal Forwarder versions 6.3 through 6.6 only will be Supported at the P3 level through the June 4, 2021 End of Support of Universal Forwarder 7.3. All minor versions of Splunk Universal Forwarder prior to version 6.3 have reached End of Support.

Security Products

Splunk Enterprise Security
Each minor version of Splunk Enterprise Security is Supported for twenty-four (24) months from release of that minor version.

Splunk Phantom
All minor versions of the latest Splunk Phantom major release and the last minor version of the prior major release are Supported.

Splunk User Behavioral Analytics
Each minor version of User Behavioral Analytics is Supported from release until the later of either:

Twelve (12) months from delivery to Customer of a license key for that version, or
Release of the second subsequent version.

IT Products

Splunk IT Service Intelligence
Each minor version of Splunk IT Service Intelligence is Supported for twenty-four (24) months from release of that minor version.

Supported Splunk Extensions

Each minor version of Splunk Extensions listed on Splunkbase or other Splunk-branded marketplace as “Splunk Supported” is Supported for twenty-four (24) months from release of that version. Support response times for these Splunk Extensions will be targeted at the P3 level.

Purchased Offering Support Services Policies

Unsupported Customers and Offerings
Support Services are provided only to Customers with an active subscription to a Support Program, exclusively for Products or Services that are part of a Customer’s Purchased Offering, or for Supported Splunk Extensions used in conjunction with such Products or Services.

Unsupported Splunk and Third Party Extensions
No Support Services are provided for any Splunk Extension listed on Splunkbase or other Splunk-branded marketplace as “Not Supported” or “Developer Supported”, nor are Support Services provided for any Third Party or Customer Extension.

Support for Multiple Offerings
When two or more Products, or any combination of Products and Services, are operated together, the versions of all must be listed as compatible in the applicable Splunk product documentation to be eligible for Support Services. For example, the Splunk Product compatibility matrix is located here and Splunk Cloud compatibility requirements can be found here.

When two or more Products are operated together, Support Services will be provided only if all Product versions are Supported. We encourage Customers to use the latest version of our Products as much as possible.

Operating System Support Status
For all Products except Splunk Universal Forwarder, no Support Services will be provided for any Product version when deployed on an operating system version that is no longer under mainstream support from its respective vendor (regardless of whether that Product version is otherwise eligible for Support Services herein). Mainstream support in this context means the period during which the vendor makes full support generally available for the operating system version, including the regular release of product enhancements and defect and security fixes, and the provision of full technical support.

The following operating system policy applies to currently-Supported minor versions of Splunk Universal Forwarder only (notwithstanding the Supported Version Timeline detailed above for Splunk Universal Forwarder):

- The targeted Support response times will be limited to the P4 level when Splunk Universal Forwarder is deployed on a compatible operating system version that is under any form of limited support from its vendor.
- Limited support in this context means an operating system vendor-defined life cycle phase following a general support phase, during which product defect and/or security fixes, but not ongoing product enhancements, are offered. If an active support subscription from the vendor is required to receive those product defects and/or security fixes, Customers must have that active support subscription to be eligible for the above described P4 level Support Services.

Support Services eligibility for a Universal Forwarder minor version on an operating system version past the end of mainstream support ends the sooner of:

a) The End of Support of that Universal Forwarder minor version, per the standard timelines for that version, or
b) The end of Customer’s active subscription to the applicable vendor support offering, or

c) (12) twelve months from the vendor-declared end of life of that operating system version, even if the vendor continues to offer support programs for that operating system version beyond that date.

Core

Splunk Enterprise / Splunk Analytics for Hadoop / Splunk Light*

Version	Release Date	End of Support Date	End of Support Criteria
6.0	Oct 1 2013	Oct 22 2019	Splunk Enterprise 8.0 Release
6.1	May 6 2014	Oct 22 2019	Splunk Enterprise 8.0 Release
6.2	Oct 7 2014	Oct 22 2019	Splunk Enterprise 8.0 Release
6.3	Sept 22 2015	Oct 22 2019	Splunk Enterprise 8.0 Release
6.4	Apr 5 2016	Oct 22 2019	Splunk Enterprise 8.0 Release
6.5	Sept 27 2016	Oct 22 2019	Splunk Enterprise 8.0 Release
6.6**	May 2 2017	Oct 22 2019	Splunk Enterprise 8.0 Release
7.0**	Sept 26 2017	Sept 26 2019	24 Months
7.1**	Apr 24 2018	Oct 31 2020	24 Months
7.2***	Oct 2 2018	April 30 2021	24 Months
7.3	June 4 2019	June 4 2021	24 Months
8.0	Oct 22 2019	Oct 22 2021	24 Months

*Splunk Light EOL applies only for 6.0 - 7.3

**A Limited Support phase was provided for Splunk Enterprise 6.6 and 7.0 from the End of Support date through January 31, 2020. All Splunk Enterprise 6.x and 7.0 versions are now End of Support. The End of Support Date for Splunk Enterprise and Splunk Light 7.1 has been extended to October 31 2020 due to the global impact of COVID-19.

***The End of Support Date for Splunk Enterprise 7.2 has been extended to April 30 2021 due to the global impact of COVID-19.

Splunk Universal Forwarder

Version	Release Date	End of Support Date	End of P3 Support Date
6.0	Oct 1 2013	Oct 22 2019	Oct 22, 2019
6.1	May 6 2014	Oct 22 2019	Oct 22, 2019
6.2	Oct 7 2014	Oct 22 2019	Oct 22, 2019
6.3	Sept 22 2015	Oct 22 2019	June 4, 2021
6.4	Apr 5 2016	Oct 22 2019	June 4, 2021
6.5	Sept 27 2016	Oct 22 2019	June 4, 2021
6.6	May 2 2017	Oct 22 2019	June 4, 2021

Version	Release Date	End of Support Date	End of Full Support Criteria	End of P3 Support Date	End of P3 Support Criteria*
7.0	Sept 26 2017	Sept 26 2019	24 Months	Sept 26 2022	36 Months
7.1	April 24 2018	April 24 2020	24 Months	April 24 2023	36 Months
7.2*	Oct 2 2018	April 30 2021	24 Months	Oct 2 2023	36 Months
7.3	June 4 2019	June 4 2021	24 Months	June 4 2024	36 Months
8.0	Oct 22 2019	Oct 22 2021	24 Months	Oct 22 2024	36 Months

*The End of Support Date for Splunk Universal Forwarder 7.2 has been extended to April 30 2021 due to the global impact of COVID-19.

Splunk Data Fabric Search

Version	Release Date	End of Support Date	End of Support Criteria
1.0	June 4 2019	June 4 2021	24 Months
1.1	Oct 22 2019	Oct 22 2021	24 Months

Splunk Data Stream Processor

Version	Release Date	End of Support Date	End of Support Criteria
1.0	Oct 30 2019	Oct 30 2021	24 Months

Security

Splunk Enterprise Security

Version	Release Date	End of Support Date	End of Support Criteria
5.0	Feb 20 2018	Feb 20 2020	24 Months
5.1**	May 14 2018	Oct 31 2020	24 Months

5.2	Oct 16 2018	Oct 31 2020	24 Months
5.3	Apr 4 2019	Apr 4 2021	24 Months
6.0	Oct 28 2019	Oct 28 2021	24 Months

**The End of Support Date for Splunk Enterprise Security 5.1 has been extended to October 31 2020 due to the global impact of COVID-19.

Splunk User Behavioral Analytics

Version	Release Date	End of Support Date	End of Support Criteria
4.1	May 24 2018	Oct 16 2019	Release of 5.0
4.2	Oct 16 2018	TBD	Next version after 5.0
4.3	Mar 26 2019	TBD	2nd version after 5.0
5.0	Oct 16 2019	TBD	3rd version after 5.0

Splunk Phantom

Version	Release Date	End of Support Date	End of Support Criteria
3.5	Mar 5 2018	TBD	Release of 5.0
4.5	May 31 2019	TBD	Release of 5.0
4.6	Sept 30 2019	TBD	Release of 5.0
4.8	Jan 30 2020	TBD	Release of 6.0

IT Operations

Splunk IT Service Intelligence

Version	Release Date	End of Support Date	End of Support Criteria
3.0	Oct 20 2017	Oct 20 2019	EOS of Enterprise 7.0
3.1	Apr 24 2018	Apr 24 2020	24 Months
4.0**	Oct 1 2018	Oct 31 2020	24 Months
4.1	Jan 1 2019	Jan 11 2021	24 Months
4.2	April 30 2019	April 30 2021	24 Months
4.3	July 17 2019	July 17 2021	24 Months
4.4	Oct 22 2019	Oct 22 2021	24 Months

**The End of Support Date for Splunk IT Service Intelligence 4.0 has been extended to October 31 2020 due to the global impact of COVID-19.

In the event of any conflict between this Splunk Support Policy exhibit attached to these General Terms and its on-line version, the on-line version will control and govern with respect to any non-material changes. For clarity, changes to pricing and changes which are contrary to the required terms and conditions prescribed by the Federal Acquisition Regulations (“FAR”) are material terms.

Exhibit D to Splunk General Terms

Splunk Acceptable Use Policy for Cloud Offerings

This Splunk Acceptable Use Policy for Cloud Offerings (this "Policy") describes prohibited uses of the cloud-based services offered by Splunk Inc. (the "Splunk Services"). The examples described in this Policy are not exhaustive. Splunk may modify the non-material terms of this Policy at any time by posting a revised version. By accessing or using the Splunk Service, Customer agrees to the latest version of this Policy unless the latest version has material changes from the policy attached hereto. If Customer violates Section 2, or Section 3 of this Policy or authorizes or assists others in doing so, Splunk may temporarily suspend Customer's use of the Splunk Service, in accordance with Section 21(D) of the Splunk General Terms and remove, disable access to or modify any content or resource which violates such Sections.

1. ILLEGAL, HARMFUL OR OFFENSIVE USE OF CONTENT

Customer may not access, use, or authorize, or encourage or facilitate the use by others of the Splunk Service for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful or offensive, such as defamatory, threatening, pornographic, abusive, libelous or otherwise objectionable material of any kind or nature, content containing any material that encourages conduct that could constitute a criminal offense, or that violates the intellectual property rights or rights to the publicity or privacy of others. Customer may not harass or interfere with another user's full use and enjoyment of any part of the Splunk Service. Customer may not access or use the Splunk Service in a manner intended to improperly avoid incurring fees or exceeding usage or capacity limits.

2. SECURITY VIOLATIONS

Customer may not access or use the Splunk Service to violate the security, integrity or policies of any network, computer or communications system, or the Splunk Software or any other software application (individually and collectively a "Service,") including but not limited to:

(a) accessing or using any Service without permission,

(b) attempting to probe, scan or test the vulnerability of a Service or to breach any security or authentication mechanisms used by a Service.

3. NETWORK ABUSE

Customer must not: damage, disable, overburden, or impair the Splunk Service (or any network connected to the Splunk Service); resell or redistribute the Splunk Service or any part of it; use any unauthorized means to modify, reroute, or gain access to the Splunk Service or attempt to carry out these activities. Customer will not store or transmit any content that contains or is used to initiate a denial of service attack, software viruses or other harmful or deleterious computer code, files or programs such as Trojan horses, worms, time bombs, cancelbots, or spyware.

4. EMAIL OR MESSAGE ABUSE

Customer will not access or use the Splunk Service to distribute, publish, send or facilitate the sending of unsolicited mass email or other messages, promotions, advertising or solicitations, including informational announcements. Customer will not alter or obscure mail headers or assume a sender's identity without permission. Customer will not collect replies to messages sent from an Internet service provider in violation of this or the Internet service provider's policies.

5. HAZARDOUS USE

Customer may not access or use the Splunk Service in connection with the operation of nuclear facilities, aircraft navigation, communication systems, medical devices, air traffic control devices, real time control systems or other similarly hazardous situations in a manner that if the Splunk Service were to fail it could lead to death, personal injury, property damage or environmental damage.

6. VIOLATIONS OF THIS POLICY

Splunk reserve the right, but Splunk does not have the obligation, to investigate any violation of this Acceptable Use Policy, the relevant Terms of Service for the applicable Splunk Service or any misuse, or potential misuse of the Splunk Service. Without notice to Customer (unless required by law), Splunk may report any activity that Splunk suspects violates any law or regulation to appropriate law enforcement authorities, regulators or other appropriate third parties. Splunk's reporting may include disclosing appropriate Customer account information and/or Customer content. Splunk may also cooperate with law enforcement agencies, regulators or

appropriate third parties to help with the investigation and prosecution of illegal conduct by providing information related to alleged violations. If Customer becomes aware of any violation of this Acceptable Use Policy, Customer must immediately notify Splunk and provide Splunk with reasonable assistance, as Splunk requests, to stop or remedy the violation. CUSTOMER AGREES TO HOLD SPLUNK HARMLESS FROM AND AGAINST, AND WAIVE (TO THE EXTENT PERMITTED BY APPLICABLE LAW) ANY CLAIMS CUSTOMER MAY HAVE AGAINST SPLUNK RESULTING FROM ANY DISCLOSURE, INVESTIGATION OR ACT OR OMISSION OF SPLUNK IN THE COURSE OF CONDUCTING OR COOPERATING WITH AN INSPECTION AS SET FORTH IN THIS ACCEPTABLE USE POLICY.

Exhibit E to Splunk General Terms

SPECIFIC TERMS FOR SPLUNK OFFERINGS

Last updated: April 2021

Additional terms apply to certain Splunk Offerings. The below terms apply to your Purchased Offerings as applicable and are incorporated into the Splunk General Terms.

.

Splunk Cloud

1. **Service Description**

https://docs.splunk.com/Documentation/SplunkCloud/latest/Service/SplunkCloudservice

2. **Security and Protection of Customer Content on Splunk Cloud.**

Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content on Splunk Cloud as set forth in the Splunk Cloud Security Addendum located at https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html ("**Cloud Security Addendum**"). .

Splunk's security safeguards include, without limitation, employee (and contractor, as applicable) security training, background testing and confidentiality obligations. Splunk's security controls adhere to generally accepted industry standards, are subject to audit by third-parties (as described in the Cloud Security Addendum) , and are designed to (a) ensure the security and integrity of Customer Content; (b) detect and protect against threats or hazards to the security or integrity of Customer Content; and (c) prevent unauthorized access to Customer Content.

3. **Service Level Schedule – Splunk Cloud**

Splunk's Splunk Cloud Service Level Schedule, set forth at https://www.splunk.com/en_us/legal/splunk-cloud-service-level-schedule.html, will apply to the availability and uptime of the Splunk Cloud, subject to planned downtime and any unscheduled emergency maintenance according to Splunk's Maintenance Policy referenced in the Splunk Service Level Schedule. Customer will be entitled to service credits for downtime in accordance with the applicable Service Level Schedule.

4. **Data Usage Policy for Splunk Cloud**

For Subscriptions based on Maximum Daily Indexing Volume, Customer is entitled to periodically exceed the daily volume purchased by Customer in accordance with Splunk's data ingestion and daily license usage policy set forth at http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DataPolicies#Data_ingestion_and_daily_license_usage.

Splunk On-Call

1. **Service Description**

   The Splunk On-Call service includes the online software service via https://www.splunk.com/en_us/investor-relations/acquisitions/splunk-on-call.html (or at such other URL as may be designated from time to time), including related application programming interfaces, interactive discussion areas, Customer accounts and profiles, mobile applications, and other related components thereof, on an individual and collective basis.

2. **Additional Users**

   If Customer wants to add additional permitted users, Customer can do so through the Offering administrative portal, and either (i) Splunk will immediately charge Customer's credit card for the prorated amount for the current term, or (ii) if Customer does not have a credit card on file, then Splunk will invoice Customer for the additional permitted users in accordance with the Terms.

3. **Necessary Integrations**

   Customer acknowledges and agrees that in order to provide certain features and functionalities of the Splunk On-Call service to Customer, Customer must allow the Splunk On-Call service communication with or access to Customer's account(s) with other third party service providers to retrieve, manipulate, process, and modify data ("**Process**"), and you expressly consent to the Splunk On-Call service accessing those accounts to Process that data solely as is necessary to provide the Splunk On-Call service. If the Splunk On-Call service cannot for any reason access your third-party accounts or Process that data, Splunk may not be able to provide Customer those features or functionalities, and Splunk will be excused from any nonperformance. Certain features and functionalities of the Splunk On-Call service require interaction with Customer's other third-party service providers, for instance, through APIs belonging to those third parties. Customer consents to Splunk interacting with Customer's other third party service providers in order to provide Customer requested features and functionality, and

Customer acknowledges that Splunk is not responsible or liable for the accuracy, content, appropriateness, or completeness of data or content Splunk receives from those third parties.

4. **Support**
   Splunk On-Call support is provided via the following portal: https://victorops.com/contact-support/.

Splunk Observability Cloud

Splunk Observability Cloud includes the following services (as part of a suite or as individual services): Splunk Infrastructure Monitoring, Splunk Application Performance Monitoring (Splunk APM), Splunk Real User Monitoring (Splunk RUM), and Splunk Log Observer.

1. **Service Descriptions**

   https://docs.splunk.com/Observability/

2.

5. **Security and Protection of Customer Content.**
   Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content as set forth in the Security Addendum located at https://www.splunk.com/en_us/legal/splunk-signalfx-security-addendum.html ("**Observability Security Addendum**").
   1. Splunk's security safeguards include, without limitation, employee (and contractor, as applicable) security training, background testing and confidentiality obligations.
   2. Splunk's security controls adhere to generally accepted industry standards, are subject to audit by third-parties (as described in the Observability Security Addendum), and are designed to (a) ensure the security and integrity of Customer Content; (b) detect and protect against threats or hazards to the security or integrity of Customer Content; and (c) prevent unauthorized access to Customer Content.
6. **Definitions.** The following definitions are applicable to Orders for Splunk Observability Cloud services.

   "Analyzed Trace" means a trace that was sent to and processed by Splunk APM.
   "APM Identities" means the count of all unique spans and initiating operations across all service endpoints for metricization. Additional dimensions on these, specified as select span tags, create further Identities based on the count of values of those tags.
   "Container" means a stand-alone, executable package of software that includes application software and sufficient operating system libraries to run in isolation but shares the underlying operating system with other Containers.
   "Custom Metric" means any Metric that is not automatically collected and reported as part of Splunk's standard Host-based integrations.
   "High Resolution Metric" means any Metric reported to Splunk that is specifically identified as a High-Resolution Metric by Customer in a manner specified by Splunk in the service documentation. Any Metric with such designation shall be processed by Splunk at a resolution no coarser than the native reporting resolution or 1-second, whichever is coarser, and shall be retained according to the Metric retention policy of the service edition purchased.
   "Host" means a virtual machine or physical server with a dedicated operating system up to 64 GB of memory.
   "Metric" means any unique combination of a metric name and dimension value reporting data to Splunk within the last hour.
   "Monitoring MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to alert on changes in application performance. A Monitoring MetricSet includes metrics such as request rate, error rate, and latency percentiles.
   "MTS" means Metric Time Series.
   "Serverless Function" means a stand-alone, executable package of single-purpose software that runs in serverless environments and is triggered by an event or message.
   "Session Volume" means the amount of Session data that customers pay for to be ingested by Splunk RUM.
   "Span" means an area of code instrumented to be captured as part of a recorded transaction (eg. rpc, function). Each service can have many spans. At a minimum, there will be 2 spans - inbound and outbound to the service.
   "TAPM" means Trace Analyzed Per Minute.
   "Trace" means an array of spans represented as a Directed Acyclic Graph.
   "Trace Volume" means amount of trace data per minute that customers pay for to be ingested by Splunk APM.
   "Troubleshooting MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to enable detailed analysis and troubleshooting of an application. A Troubleshooting MetricSet includes metrics such as the request rate, error rate, root-cause error rate and latency percentiles.

Splunk Synthetic Monitoring

1. **Service Description:**
   https://help.rigor.com/hc/en-us

2. **Security:**
   Customer hereby acknowledges and agrees that Splunk Synthetic Monitoring has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification. **The security terms in Splunk's Cloud Security Addendum and the Observability Security Addendum do NOT apply.** Customer may not upload or transmit to this environment any regulated data, such as financial information (including PCI-DSS data), protected health information, ITAR data or classified information.

Splunk Business Flow

1. **Definitions.**

The following definitions are applicable to Splunk Business Flow.
"Application Services" means the web-based, cloud service component that powers functionality of Splunk Business Flow.
"Flow Model" refers to a grouping of discrete information which represents a transaction, session, or other business process that is configured within Splunk Business Flow.
"Private Flow Model" means a Flow Model that is solely for use by administrators for testing, configuration and preview of Flow Models.
"Splunk Business Flow" means the Splunk Business Flow service that uses event data to facilitate the exploration and visualization of end-to-end business processes through Flow Models and will include any and all successors, replacements, new versions, derivatives, updates and upgrades thereto made available to Customer by Splunk. Splunk Business Flow includes a downloadable software component and functionality powered by the Application Services.

2. **Customer Use of Splunk Business Flow.** For the avoidance of doubt, data ingested for use with Splunk Business Flow counts against Customer's Capacity purchased for the applicable Purchased Offering (i.e., the Purchased Offering with which Customer uses Splunk Business Flow).
3. **Additional License Restriction.** Unless otherwise expressly permitted by Splunk, Customer may not and may not permit any third party to use Private Flow Models for purposes other than testing, configuration or preview of Flow Models by an authorized administrator of Splunk Business Flow.

Splunk Mission Control

1. **Service Description:**

https://docs.splunk.com/Documentation/MC/Current/Service/SplunkMissionControlService.

2. **Security:**

Customer hereby acknowledges and agrees that Splunk Mission Control has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification. **The security terms in Splunk's Cloud Security Addendum do NOT apply.** Customer may not upload or transmit to this environment any regulated data, such as financial information (including PCI-DSS data), protected health information, ITAR data or classified information.

Exhibit F to Splunk General Terms

Updated: February 2020

Professional Services Information Security Addendum

(For use with General Terms)

This Professional Services Information Security Addendum ("**PS-ISA**") sets forth the administrative, technical and physical safeguards Splunk takes to protect Confidential Information when performing Professional Services. The PS-ISA is based on Splunk's Information Security Program ("**ISP**"), which changes over time. Splunk may update this PS-ISA to reflect changes in its ISP, provided those changes do not materially diminish the level of security herein provided.

This PS-ISA is made a part of the Configuration and Implementation Services Exhibit to the Splunk General Terms ("**Agreement**") and applies only to the Configuration and Implementation Services set forth in an applicable Statement of Work. Any capitalized terms used, but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this PS-ISA, the terms of this PS-ISA will apply.

During the Term of the Agreement, Splunk agrees to maintain an ISP in conformance with the requirements set forth below.

1. **Splunk's Information Security Program and Security Program Office**
    1. Splunk's ISP is reasonably designed to help protect the confidentiality, integrity, and availability of Confidential Information against any anticipated threats or hazards; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss, destruction or damage.
    2. Splunk's ISP contains technical and organizational measures that are appropriate to: (i) the nature, size, and complexity of Splunk's business; (ii) the resources available to Splunk; (iii) the type of information that Splunk stores; and (iv) the need for security and confidentiality of such information.
    3. Splunk's Chief Information Security Officer leads Splunk's ISP and develops, reviews and approves (together with other stakeholders, such as Product Security, Legal and Internal Audit) Splunk Security Policies (as defined below).
2. **Security Policies and Procedures**
    1. Splunk maintains information security, use and management policies (collectively "**Security Policies**") designed to educate employees and contractors regarding appropriate use, access to and storage of Confidential Information; restrict access to Confidential Information to members of Splunk's workforce who have a "need to know" such information; prevent terminated employees from accessing Splunk information and information systems post-termination; and imposing disciplinary measures for failure to abide by such policies. Splunk performs background checks of its employees at time of hire, as permitted by law. Where feasible and as applicable, Splunk endeavors to align its Security Policies to ISO 27001 level standards for information security.
    2. Splunk Security Policies are available to employees via the corporate intranet. Splunk reviews, updates and approves Security Policies once annually to maintain their continuing relevance and accuracy.
3. **Security Training and Awareness**

New employees are required to complete security training as part of the new hire process and receive annual and targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with Security Policies, as well as other corporate policies, such as the Splunk Code of Conduct. This includes requiring Splunk employees to annually re-acknowledge the Code of Conduct and other Splunk policies as appropriate. Splunk conducts periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace.

4. **Physical and Environmental Access Controls**

Splunk limits physical access to its information systems and facilities using physical controls (e.g., coded badge access) that provide reasonable assurance that access to its data centers is limited to authorized individuals and employs camera or video surveillance systems at critical internal and external entry points. Splunk applies air temperature and humidity controls for its data centers and protects against loss due to power failure.

5. **Logical Access Controls**

Splunk employs monitoring and logging technology to help detect and prevent unauthorized access attempts to its networks and production systems. Splunk's monitoring includes a review of changes affecting systems' handling authentication, authorization, and auditing; and privileged access to Splunk production systems. Splunk uses the principle of "least privilege" (meaning access denied unless specifically granted) for access to customer data.

6. **Incident Response Plan and Breach Notification**
    1. Splunk employs an incident response framework (the "**Splunk Incident Response Framework**" or "**SIRF**") to manage and minimize the effects of unplanned security events. The SIRF includes procedures to be followed in the event of an actual or potential security breach, including: (i) an internal incident response team with a response leader; (ii) an investigation team performing a root cause analysis and identifying affected parties; (iii) internal reporting and notification processes; documenting responsive actions and remediation plans; and (iv) a post-incident review of events.
    2. For Services performed outside the US, Splunk provides notice without undue delay after becoming aware of a Data Breach. As used in this PS-ISA, Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data as defined under the General Data Protection Regulations (EU) 2016/679 ("**GDPR**") while being transmitted, stored or otherwise processed by Splunk. If Customer reasonably determines notification is required under GDPR, Splunk will provide reasonable

assistance to the extent required, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.

3. For Services performed within the US, Splunk provides notice of a breach of Personal Information, as defined under the California Consumer Privacy Act of 2018 ("**CCPA**"), as required under California law.

7. **Storage and Transmission Security**

Technical security measures to guard against unauthorized access to Customer data that is being transmitted over a public electronic communications network or stored electronically.

8. **Secure Disposal**

Policies and procedures regarding the disposal of tangible and intangible property containing Customer Confidential Information so that wherever possible, Customer Confidential Information cannot be practicably read or reconstructed.

9. **Risk Identification and Assessment**

Splunk employs a risk assessment program to help it reasonably identify foreseeable internal and external risks to Splunk's information resources and determine if its existing controls, policies, and procedures are adequate to address the identified risks.

10. **Vendors**

Third-party vendors (collectively, "**Vendors**") with access to Confidential Information are subject to contractual obligations of confidentiality and risk assessments to gauge the sensitivity of information being shared. Vendors are expected to comply with any pertinent contract terms relating to the security of data, as well as any applicable Splunk policies or procedures. Periodically, Splunk may ask the Vendor to re-evaluate its security posture to help ensure compliance.

Exhibit G to Splunk General Terms

Export Controls

Information on the export control status of Splunk products.
(As of July 10, 2018)
Many Splunk products are subject to U.S. export and trade regulations, including the U.S. Department of Commerce's, Bureau of Industry and Security's Export Administration Regulations (EAR), and the Treasury Department's Office of Foreign Assets Controls' various trade and economic sanctions regulations (OFAC regulations). Some Splunk products are classified under the EAR with an export control classification number (ECCN) of 5D002 and they are eligible for export in accordance with the EAR's license exception ENC.
View Splunk Product Export Control Classification List and FAQ's
You are agreeing to comply with all applicable export and re-export (shipment from one foreign (non-U.S.) country to another foreign country) control laws and regulations, including the EAR and the OFAC regulations as it relates to your use of Splunk's products. Splunk customers, partners and users of the products cannot -- directly or indirectly -- sell, export, re-export, ship, transfer, or divert, any products, software, or technology (including products derived from or based on such technology) received from Splunk in violation of these laws. If prior authorization is required, you may apply for the required governmental authorization by submitting a license application to the applicable government agency. The EAR are available at https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear and the OFAC regulations are available at https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

No Splunk products, or third party products available on Splunk sites, can be sold, exported, re-exported, shipped, diverted or otherwise transferred (collectively "transferred") without the required government license to an individual or entity located in an embargoed country (click here to view the latest list) or on any applicable government sanctions lists, including the U.S. Treasury Department's list of Specially Designated Nationals, or on the U.S. Commerce Department's Denied Persons List or Entity List (see Commerce Lists to Check) Further, no Splunk products, or third party products available on Splunk sites may be used for any chemical or biological weapons, sensitive nuclear end-uses, or missile related end-uses or other prohibited end-uses without the required license from the applicable U.S. Government agency.
As stated above, without limitation, parties acquiring or using any Splunk product are responsible for obtaining all required licenses or other approvals necessary for the transfer of Splunk products, or third party products available on Splunk sites. Further, you certify that you are not in an embargoed country or on any applicable government sanctions lists.

Please see links below for more information.
Sanctions Programs and Country Information (U.S. Department of the Treasury)
Office of Foreign Assets Control (OFAC) (U.S. Department of the Treasury)
Country Guidance (U.S. Department of Commerce)
Bureau of Industry and Security (U.S. Department of Commerce)
Overview of U.S. Export Control System (U.S. Department of State)

This information is for informational purposes only. Since the export control and sanctions laws are frequently amended, it is important to recognize that the posted information may not include the most recent changes to these laws and how the changes may affect our products. As such, Splunk does not represent, warrant or guarantee that the posted information is complete, accurate or up-to-date. The information does not nor is it intended to be legal advice. You should seek appropriate professional guidance if you have any questions about how the posted information may affect your export transactions or use of our products.