PARTICPATING ADDENDUM TO SPLUNK CLOUD TERMS OF SERVICE

This Participating Addendum, by and between AppDynamics LLC (“**AppDynamics**”) and Splunk Inc., (“**Supplier**”) (the “Addendum”) is effective as of July 12, 2021 (“**Effective Date**”).

Whereas, Supplier, a Delaware corporation, having its principal place of business at 270 Brannan Street, San Francisco, CA 94107, and Cisco Systems, Inc., a California corporation, having its principal place of business at 170 West Tasman Drive, San Jose, CA 95134, entered into that certain Splunk Cloud Terms of Service (“the Agreement”) fully executed as of September 25, 2019, as it may be amended and restated from time to time and attached hereto as Exhibit 1, to procure Services from Supplier; and

Whereas, AppDynamics, the undersigned Affiliate of Cisco, a Delaware limited liability company, having its principal place of business at 303 Second Street, North Tower, Eighth Floor, San Francisco, CA 94107 desires to participate in the Agreement by entering into this Addendum to also procure Services from Supplier in connection with AppDynamics’ rights as an Affiliate of Cisco. Supplier hereby acknowledges that AppDynamics is a wholly owned subsidiary of Cisco, a party to the Agreement; and

Whereas, AppDynamics and Supplier wish to enter into this Addendum to: (i) facilitate AppDynamics’ purchases of Services under the Agreement and (ii) include certain additional rights and obligations on the parties.

Therefore, the parties agree as follows:

1. Each party to this Addendum covenants and agrees that it will be bound by all of the provisions of the Agreement, as modified by this Addendum, as if:

   a. all references to Cisco and/or “Customer” in the Agreement will be references to AppDynamics and its Affiliates as if AppDynamics had been an original party thereto, and AppDynamics will have all of the rights and obligations of Cisco under the Agreement; and

2. Cisco will not be liable for AppDynamics’s performance of the obligations set forth in the Agreement, or the performance of any other Affiliate of AppDynamics.

3. Capitalized terms and expressions not otherwise defined in this Addendum shall have the meanings ascribed to them in the Agreement.

4. Notwithstanding the foregoing, the Agreement will be amended in the Addendum as follows:

   a. Section 6.1 (Term and Renewal) is deleted and replaced in its entirety with the following:

      6.1 Term and Renewal. This Agreement will expire upon the expiration or termination of Customer’s account or subscription to a Service. The Subscription Initial Term and Agreement term will be for three (3) years from the date of the last signature below and will renew upon execution of an Order document.

b. The following shall be added to Section 9 (Limitation of Liability):

Notwithstanding anything to the contrary, the foregoing limitation of liability shall not apply to Splunk's unauthorized access or unauthorized disclosure of Customer Content on a Hosted Service provided that aggregate liability of Splunk and its Affiliates arising from such events shall be limited to $7M except if such breach is caused by Customer's failure to secure its login or Customer Content.

c. Section 16.9 (Notices to Customers and Consent to Electronic Communications) is deleted and replaced in its entirety with the following:

16.9 Notices to Customers and Consent to Electronic Communications. Customer consents to receiving either electronic or written communications and notifications from Splunk in connection with the Services, and the linked policies and the Agreement. Customer agrees that any such communication will satisfy any applicable legal communication requirements, including that such communications be in writing. Splunk may provide Customer with notices regarding the Services, including changes to this Agreement and the linked policies, by email to legal@appdynamics.com, or by regular mail to AppDynamics LLC, 303 Second Street, North Tower, Eighth Floor, San Francisco, CA, 94107, USA. It is Customer responsibility to keep Customer email address current. Customer will be deemed to have received any email sent to the email address then associated with Customer’s account when Splunk sends the email. In the event Customer does not wish to accept any material change to the Services, the linked policies or to this Agreement, Customer will have the right, as its sole remedy, to terminate this Agreement within thirty (30) days of Splunk’s notice of such change, and, if Customer exercises such termination right, Splunk will provide a pro rata refund to Customer equal to the amount fees pre-paid by Customer for the Service that corresponds to the period after the date of such termination for the Term.

5. Authority. The person signing this Addendum for each party represents that s/he is duly authorized by all necessary and appropriate corporate action to enter into this Addendum on behalf of such party.

6. Law and Jurisdiction. The parties agree that this Addendum and any dispute arising hereunder shall be governed by the laws of the State of California to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Addendum or its subject matter or formation.

IN WITNESS WHEREOF, the parties hereto have executed this Addendum as of the Effective Date.

Splunk Inc.	DocuSigned by:	**AppDynamics LLC:**	DocuSigned by:
Signature:	Amos Wang C2571D8EE24740A...	Signature:	Linda Tong BFD8FF4665DA4A7...
Name:	Amos Wang	Name:	Linda Tong
Title:	Director of Revenue	Title:	GM
Date:	12-Jul-2021	Date:	July 12, 2021

DS

EXHIBIT 1

Splunk Cloud Terms of Service

These Splunk Cloud Terms of Service **(“Agreement“)** between you (“**Customer**”) and Splunk Inc. **(“Splunk”)**, govern Customer’s access to and use of the Service (as defined below). By accessing or using a Service in any manner, Customer agrees to the Agreement. Please refer to Section 17 for definitions of certain capitalized terms.

1. SPLUNK’S RESPONSIBLITIES

1.1 Service Subscriptions; Support; Service Levels. Subject to Customer’s compliance with this Agreement, Splunk will make the applicable Services available to Customer during the Subscription Term. Splunk will provide Support for the applicable Services to Customer during the Subscription Term at no additional charge. During the Subscription Term Splunk’s Service Level Schedule, attached hereto as of the Effective Date as Exhibit A, will apply to the availability and uptime of the Service, 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.

1.2 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 Splunk Cloud Security Addendum located at attached hereto as of the Effective Date as Exhibit B (“**Cloud Security Addendum**”). Splunk’s security safeguards include, without limitation, employee (and contractor, as applicable) security training regarding handling and protection of personal data prior to such access, background testing and confidentiality obligations. Splunk’s security controls adhere to generally accepted industry standards, rules, laws and regulations applicable to Splunk in its performance hereunder and 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.

1.3 Maintaining Protections and Support Levels. Notwithstanding anything to contrary in this Agreement, or any policy or terms referenced herein, including via hyperlink (or any update thereto), , Splunk may not, during a paid Subscription Term (a) materially diminish the security protections provided by the controls set for the Cloud Security Addendum, or (b) reduce the level of support purchased by Customer under the applicable Support plan.

1.4 Trial Services. Splunk may make certain Services, Splunk Applications or specific features and functions, available without charge for limited periods for evaluation and non-production purposes (a “**Trial**”). Some of these Trials may be made available in an online sandbox, a self-contained cloud instance that Splunk pre-configures and pre-populates with data available for the evaluation of Services, Splunk Application(s) or specific features and functionalities. The use of a Trial will be for the term specified by Splunk and may have limited features, functions, indexing capacity, data storage, data security, data continuity, data retention or other limitations as determined by Splunk, and Splunk may change or discontinue the Trial at any point. Splunk reserves the right to monitor Customer’s use of Trial in accordance with Section 2.7. Upon expiration of a specified term for an online sandbox Trial in particular, the sandbox environment and all Customer Content contained in the environment will become inaccessible. Customer understands that only Sections 2, 4, 5, 7, 9, 11.2, 12, 15, 16 and 17 of this Agreement apply to a Trial. Notwithstanding the foregoing, Section 8.2 will apply without exception for the terms of Section 8.1. Splunk is not obligated to provide any maintenance, technical or other support for Trials.

1.5 Beta Services. Splunk may make available to Customer a preview, limited release, alpha, beta or other pre-release version or feature of the Service or Splunk Applications for non-production use (each, a "**Beta Service**"). Only Sections 2, 4, 5, 7, 9, 11.2, 12, 13, 15, 16 and 17 of this Agreement apply to the Beta Service. Customer's use of a Beta Service will be for the term specified by Splunk and if no term is specified, then for the earlier of one year from the Beta start date of the Beta Service or when that version of the Beta Service becomes generally available. A Beta Service may have limited features, functions, indexing capacity, data storage, data security, data continuity, data retention or other limitations as determined by Splunk. Splunk reserves the right to monitor Customer's use of Beta Services in accordance with Section 2.7. Splunk may discontinue the Beta Service and may decide never to make the features and functionality in the Beta Service generally available. Customer acknowledges that Beta Services, by their nature, have not been fully tested and may contain defects or deficiencies which may not be corrected by Splunk, that a Beta Service may undergo significant changes prior to release of the generally available final version.

1.6 Configuration Services. Subject to Customer's payment of applicable fees, Splunk will provide the deployment, usage assistance, configuration, and/or training services (if any) set forth in an Order in accordance with the Professional Services Agreement between the parties dated November 14, 2008.

1.7 Service Data. Splunk collects Service Data to support and troubleshoot issues, provide personalized messages/updates, analyze trends and otherwise improve the Service. For more information on the use of the Service Data we collect, see Splunk's Privacy Policy, located at attached hereto as of the Effective Date as Exhibit C and , incorporated herein by reference.

2. CUSTOMER USE OF THE SERVICES

2.1 Access and Use. Customer may only access and use the Services, Splunk Applications and Splunk Content in accordance with the terms of the Agreement, within the Licensed Capacity set under the Order, and solely for Customer's Internal Business Purpose. Customer agrees to provide accurate and complete information when Customer registers for and uses any Service and agrees to update all required information promptly. Each person who uses any Service must have a separate username and password. Customer must provide a valid email address for each person that Customer authorizes to use Customer's account, and Customer may only create one account per email address. Customer must provide any other information reasonably requested by Splunk.

2.2 Purchased Volumes. Each Service is provided to Customer according to the Licensed Capacity, as purchased on the Order. Any Splunk Application licensed to Customer for use with a Service is subject to the same limitations and restrictions that apply to the Service with which such Splunk Application is used. 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 attached hereto as of the Effective Date as Exhibit D. If Customer's usage is in excess of the policy allowance, Splunk may work with Customer to reduce usage so that it conforms to the applicable usage limit. If, notwithstanding Splunk's efforts, Customer is unable or unwilling to abide by the applicable usage limit, Customer will pay any invoice for excess usage in accordance with Section 3.

2.3 Transmission of Customer Content. Customer is responsible for obtaining and maintaining all telecommunications, broadband and computer equipment and services needed to access and use the Services and for paying all charges related thereto. Customer is the owner and/or controller of all of Customer Content that Customer transmits to the Services. Without limiting Splunk's security obligations under Section 1.2 above, Customer is responsible for the security of Customer Content when transmitted to and from the Services. Customer acknowledges that any encryption of Customer Content stored (i.e., "encryption at rest") on the Service is subject to Customer's separate purchase of encryption features available from Splunk.

2.4 Customer Responsibility for Users and Customer Content. Customer is responsible for: (a) Users' compliance with the Agreement; (b) the accuracy, quality and lawful use of Customer Content and the means by which Customer acquired Customer Content; (c) taking steps to maintain appropriate security and protection of Customer Content (which may include (i) selecting certain service options that Splunk makes available for a Service, such as premium encryption at rest service, and (ii) taking additional measures outside of the Service to the extent the Service offering does not provide the controls that may be required or desired by Customer); and (d) routine archiving and back up of Customer Content. Customer is responsible for securing, protecting and maintaining the confidentiality of Customer's account username, passwords and access tokens. Neither Customer nor its Users will share Customer passwords or access codes. Customer is responsible for any access and use of the Services via Customer's accounts and for all activity that occurs in connection with Customer's accounts, regardless of whether the activities were undertaken by Customer, a User or a third party, except to the extent due to Splunk's breach of its security obligations under Section 1.2. Splunk will not be liable for any loss or damage arising from Customer's failure to maintain the security of Customer's account. Customer agrees to notify Splunk immediately if Customer believes that an unauthorized third party may be using Customer's account or if Customer's account information is lost or stolen. For the avoidance of doubt, nothing in this Section 2.4 will limit Splunk's security obligations under Section 1.2. However, Customer acknowledges that Splunk Cloud security controls cannot be customized to meet individual Customer requirements, and that Customer is responsible for determining if the Splunk Cloud security controls meet Customer's needs. Customer is responsible for implementing any additional security controls deemed necessary by the Customer, including any additional security measures not provided as part of the Service.

2.5 Data Restrictions/Regulated Data. Customer may not transmit and/or store HIPAA Data or PCI Data within the Services unless Customer has specifically purchased a Subscription for that applicable Services environment (as identified in an Order). Customer will be prohibited in all cases from transmitting or storing within the Services any or ITAR Data or any data that is restricted under export-controls as provided in Section 15.

2.6 Splunk Applications. Splunk Applications can be installed within the Service pursuant to Splunk's instructions. Some Splunk Applications are supported by Splunk while others are not supported. For further information on supporting Splunk Applications, please refer to attached hereto as of the Effective Date as Exhibit E. For those Splunk Applications that are labeled on Splunkbase as “Not Supported”, the Service Level Commitment and Service Level Credit in the Splunk Service Level Schedule will not apply. Customer agrees that Splunk is not responsible for any impact on Customer’s experience of the Service as a result of Customer’s installation and/or use of any such Splunk Applications, and that Customer’s sole remedy will be to remove the “Not Supported” Splunk Application from its Splunk environment.

2.7 Third Party Content or Resources. A Service may contain features or functions that enable the interoperation of the Services or Splunk Applications with Third Party Content. To use such features or functions, however, Customer may be required to obtain access separately to such Third Party Content from the respective providers of such Third Party Content, and Customer may be further required to grant Splunk access to Customer accounts with such providers to the extent necessary for Splunk to provide a Service. By requesting or allowing Splunk to enable access to such Third Party Content in connection with the Services, Customer certifies that it has accepted all terms related to the Third Party Content and agrees to use the Third Party Content in accordance with the license or service terms provided by the provider of the Third Party Content. If Customer installs or enables (or directs or otherwise authorizes Splunk to install or enable) Third Party Content for use with any Service, Customer hereby authorizes Splunk to allow the provider of such Third Party Content to access Customer Content as necessary for the interoperation of such Third Party Content with the applicable Services. Customer agrees 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 Customer may incur or any impact on Customer’s experience of the Service, directly or indirectly, as a result of Customer’s use of, and/or reliance upon, any Third Party Content, sites or resources.

3. PAYMENTS

3.1 Fees and Taxes. Customer agrees to pay all fees and charges agreed to in the applicable Orders. Except in the event of an uncured material breach by Splunk and as set forth in Sections 6.2 and 6.5; Subscription licenses to the Services, any Splunk Applications, and associated fees incurred are non-cancelable and non-refundable. Charges must be paid in advance, either annually or in accordance with any different billing period stated in the Order. All payments are due and payable either within 60 days from the date of Splunk’s invoice or such other period, if any, stated in the Order. All fees and charges quoted are exclusive of applicable taxes and duties, including any applicable sales and use tax. Customer is responsible for paying any taxes assessed based on Customer’s purchases under the Agreement. Any fees and payment terms for Splunk Applications not included in the Order will be as set forth on the access page for such Splunk Applications, but will only apply when Customer is purchasing such Splunk Applications via an e-commerce transaction.

3.2 Resellers. If Customer acquires a subscription through an authorized reseller of Splunk (“**Authorized Reseller**”), then, notwithstanding anything to the contrary above, Customer agrees to pay the Authorized Reseller the subscription fees associated with such subscription, and Customer will have no direct payment obligations to Splunk for such fees. However, for the avoidance of doubt, no agreement between Customer and an Authorized Reseller is binding on Splunk or will have any force or effect with respect to the operation, use or provision of the

Services. Furthermore, for the avoidance of doubt, the foregoing shall not limit Splunk's right to directly charge Customer for overages under Section 2.2.

3.3 Credit Card Payments. Unless otherwise agreed to by the parties; all Orders must have a purchase order ("PO") issued by Customer to Splunk in order to be valid. If Customer is permitted to pay by credit card, Customer: (a) will provide Splunk with valid credit card information; and (b) hereby authorizes Splunk to charge such credit card for all items mutually agreed to in the Order, provided with a PO. for the initial Subscription Term, and any renewal term(s). Such charges must be paid in advance, either annually or in accordance with any different billing frequency stated in the applicable Order. Customer is responsible for providing complete and accurate billing and contact information and notifying Splunk in a timely manner of any changes to such information.

3.4 Future Functionality. Customer agrees that its purchases are 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.

4. PROPRIETARY RIGHTS AND LICENSES

4.1 Splunk Ownership; Suggestions. As between Customer and Splunk, Splunk owns and reserves all right, title, and interest in and to the Services, the Splunk Software, the Splunk Applications and the Splunk Content, including all intellectual property rights therein. No rights are granted to Customer hereunder other than as expressly set forth herein. Customer grants to Splunk a perpetual, irrevocable, worldwide, nonexclusive, transferable, sublicensable right and license to commercially exploit in any manner Splunk deems fit any Suggestions that Customer provides to Splunk. Notwithstanding the foregoing, the parties agree that any customer suggestions relied upon by Splunk shall be at Splunk's sole risk. Customer shall have no liability, at any time for any use or implementation of any Customer suggestion.

4.2 License to Services, Splunk Applications and Splunk Content. Subject to Customer's continued compliance with this Agreement, including timely payment of the fees set forth in the applicable Order, Splunk grants Customer a limited, revocable, non-exclusive, non-sublicensable, non-transferrable license to do the following solely during the Subscription Term:

(i) Access and use the Services listed on the Order for Customer's Internal Business Purposes.

(ii) Use any applicable Splunk Applications listed on the Order (or on an access page from Splunkbase) that Customer has licensed and installed, or has licensed and asked Splunk to install on Customer's behalf, solely in connection with Customer's permitted use of the applicable Services.

(iii) Use the Splunk Content, solely in connection with Customer's permitted use of the Services.

(iv) Use the API(s) and other Service components in accordance with descriptions provided in the Documentation.

(v) Copy, modify and use the APIs solely to develop Customer Applications and distribute Customer Applications solely for use with the designated Service or Splunk Application. The foregoing license is subject to the following conditions: (x) Splunk proprietary legends or notices contained in the APIs may not be removed or altered when used in or with the Customer Application; and (y) Customer may not make any statement that Customer Application is certified or that its performance is guaranteed by Splunk. Customer retains title to the Customer Applications, subject to Splunk's ownership set forth in Section 4.1. If Customer allows end users of Customer Applications to modify or distribute the Customer Applications, Customer will limit such modification or distribution to use with the designated Service or Splunk Application only, and will flow down the conditions in (x) and (y) above to end users of Customer Applications. Customer agrees to assume full responsibility for the performance and distribution of Customer Applications.

(vi) Access and use the Forwarder solely to forward Customer Content into the applicable Services. The terms of this subsection and this Agreement supersede and replace in its entirety any click-through agreement that Customer must accept prior to accessing the Forwarder.

4.3 License Restrictions. The grant of rights to Customer in Section 4.2 is subject to the following restrictions and limitations: Customer may not, and may not permit 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, object code or underlying structures, ideas or algorithms of the Services, the Splunk Software, the Splunk Applications, the Splunk Content or any software, documentation or data related to the Services, the Splunk Software, the Splunk Applications or Splunk Content; (b) modify, translate or create derivative works based on the Services, the Splunk Software, the Splunk Applications or Splunk Content; (c) use the Services,the Splunk Software, the Splunk Applications or Splunk Content for timesharing or service bureau purposes, or for any purpose other than its own internal purposes; (d) access or use any Service in order to monitor its availability, performance, or functionality for competitive purposes; or (e) use the Services, the Splunk Software, the Splunk Applications or Splunk Content other than in accordance with the Agreement and in compliance with all applicable laws and regulations (including but not limited to any applicable privacy and intellectual property laws). Notwithstanding the foregoing, if any Splunk Application is provided to Customer under a separate license agreement that grants Customer more permissive or broader rights with respect to such Splunk Application (e.g., a separate license agreement that is provided to Customer aspart of the provisioning process for such Splunk Application), then that separate license agreement, and not the Agreement, will govern Customer's installation and use of such Splunk Application (but, for clarity, the Agreement will apply to all other Splunk Applications).

5. CUSTOMER CONTENT

5.1 Ownership. By submitting or posting Customer Content on the Services, Customer is representing that Customer is the owner of such materials and/or has the necessary rights, licenses, and authorization to distribute it.

5.2 Access to and Use of Customer Content. By submitting or posting Customer Content on areas of the Services, Customer grants Splunk a worldwide, royalty free, non-exclusive license to access and use such Content solely to provide the Services for purposes consistent with this Agreement and in connection with Section 1.7.

6. TERM AND TERMINATION;

6.1 Term and Renewal. This Agreement will expire upon the expiration or termination of Customer's account or subscription to a Service. The Subscription Initial Term and Agreement term will be for three (3) years from the date of the last signature below and will renew, for a 12 month period each (or other period agreed upon by the parties in writing), upon Customer's issuance of a PO not less than 60 days prior to the last day of the Initial Term or Renewal Subscription Term, execution of an Order document, or other Customer agreement for renewal. Customer may notify Splunk of its intent not to renew at least ninety (90) days in advance of the expiration of the Subscription Term or then-current renewal period.

6.2 Termination for Cause. A party may terminate this Agreement for cause if there is any material breach of this Agreement by the other party, unless the breaching party has cured the material default or breach within 30 days from the date of notice.

6.3 Effect of Termination. Upon expiration or termination of Customer's account or subscription to a Service:

(i) All Customer rights under this Agreement relating to such Service will immediately terminate;

(ii) Customer will lose all access to the applicable Service, including access to Customer's account and Customer Content;

(iii) Customer will immediately return or, if instructed by Splunk, destroy all Splunk Content relating to such Service in Customer's possession or control; and

(iv) Any licenses to any Splunk Applications and Splunk Content relating to such Service will terminate.

6.4 Return of Customer Content. Customer Content may be retrieved by Customer and removed from the Services in accordance with the Documentation. Upon request by Customer made before the effective date of termination of a Service subscription, Splunk may assist Customer with the transition of Customer Content for a mutually agreed upon fee. Thirty one (31) days following expiration or termination of Customer's account or subscription for a Service, Splunk will have no obligation to maintain or provide any of Customer Content relating to such Service, and Customer hereby authorizes Splunk thereafter to delete all Customer Content relating to such Service that is in its possession or under its control, unless Splunk is otherwise legally prohibited from doing so.

6.5 Refund or Payment upon Termination. If this Agreement is terminated by Customer in accordance with Section 6.2 (Termination for Cause), Splunk will refund Customer any prepaid subscription fees covering the remainder of the Subscription Term after the effective date of termination. If this Agreement is terminated by Splunk in accordance with Section 6.2, Customer will pay any unpaid fees covering the remainder of the then current Subscription Term after the effective date of termination. In no event will termination relieve Customer of its obligation to pay any fees payable to Splunk for the period prior to the effective date of termination.

6.6 Suspension of Service. Unless otherwise agreed to by the parties, If any undisputed charge owing by Customer is sixty (60) days or more overdue, Splunk may, without limiting its other rights and remedies, suspend the applicable Services until such amounts are paid in full, provided that, Splunk will give Customer at least ten (10) days' prior notice that its payment is overdue before suspending services to Customer. For the avoidance of doubt suspensions of applicable Services will have no impact on the then-current Subscription Term, its associated payments or the relevant duration of the Subscription. Should Customer dispute a Splunk invoice, Customer will promptly notify Splunk of the dispute details and will work in good faith with Splunk to resolve any such dispute promptly thereafter.

7. CONFIDENTIALITY

7.1 Confidential Information. Unless otherwise provided in writing, the 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 this Agreement, and (iii) 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 this Agreement and who are subject to confidentiality obligations no less stringent than those herein.

7.2 Compelled Disclosure of Confidential Information. Notwithstanding the foregoing terms of Section 7.1, 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.

8. WARRANTIES AND DISCLAIMER OF WARRANTIES

8.1 Splunk's Warranties. Splunk warrants that: (a) it has the legal power and authority to enter into this Agreement; (b) during the Subscription Term Splunk will not materially decrease the overall functionality of the Services; and (c) during the Subscription Term the Services will perform materially in accordance with the applicable Documentation. For any breach of the warranties in (b) and (c), Customer's sole and exclusive remedies are those described in the Termination and Refund of Payment upon Termination sections above.

8.2 Disclaimers. EXCEPT AS EXPRESSLY SET FORTH IN 8.1 ABOVE, THE SERVICES ARE PROVIDED TO CUSTOMER ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITHOUT ANY EXPRESS REPRESENTATIONS OR WARRANTIES OF ANY KIND, AND, TO THE FULLEST EXTENT PERMITTED BY LAW, SPLUNK DISCLAIMS ALL STATUTORY OR IMPLIED REPRESENTATIONS, WARRANTIES, TERMS AND CONDITIONS WITH RESPECT TO THE SERVICES, INCLUDING ANY REPRESENTATIONS OR WARRANTIES OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES. TO THE EXTENT SUCH A LAW APPLIES TO CUSTOMER, SOME OR ALL OF THE EXCLUSIONS SET FORTH ABOVE MAY NOT APPLY TO CUSTOMER, AND CUSTOMER MAY HAVE ADDITIONAL RIGHTS.

9. LIMITATION OF LIABILITY

EXCEPT FOR EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT AND THE INDEMNIFICATION OBLIGATIONS OF BOTH PARTIES IN SECTION 11, IN NO EVENT WILL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ANY OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HEREUNDER FOR SERVICES GIVING RISE TO THE LIABILITY IN THE TWENTY FOUR

MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, BUT WILL NOT LIMIT CUSTOMER OR CUSTOMER'S AFFILIATE'S OBLIGATIONS UNDER THE "PAYMENTS" SECTION ABOVE, AND WILL NOT BE DEEMED TO LIMIT CUSTOMER'S RIGHTS TO SERVICE LEVEL CREDITS UNDER SPLUNK'S SERVICE LEVEL SCHEDULE.

IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, BUSINESS INTERRUPTION OR PUNITIVE DAMAGES, WHETHER THE ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY'S 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 FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

NOTHING IN THIS AGREEMENT SHALL LIMIT EITHER PARTY'S (1) LIABILITY FOR PERSONAL INJURY OR DEATH CAUSED BY ITS NEGLIGENCE, (2) LIABILITY IN THE TORT OF DECEIT, OR (3) LIABILITY TO THE EXTENT THAT IT CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. TO THE EXTENT SUCH A LAW APPLIES TO CUSTOMER, SOME OR ALL OF THE EXCLUSIONS OR LIMITATIONS SET FORTH ABOVE MAY NOT APPLY TO CUSTOMER, AND CUSTOMER MAY HAVE ADDITIONAL RIGHTS.

10. SPUNK INSURANCE REQUIREMENTS

The following are minimum levels and types of insurance that shall be maintained by Splunk throughout the term of any Order and/ or this Agreement.

Professional Liability (Errors and Omissions) Insurance. Splunk shall carry insurance for professional liability with limits of not less than $3,000,000 per occurrence or per claim and $3,000,000 in the annual aggregate associated with the Services under this Agreement. Such insurance shall provide contractual liability coverage. If Splunk carries the Professional Liability insurance required under this Agreement on a claims-made basis, the Splunk shall continue to maintain such insurance for two (2) years following the termination of this Agreement.

Technology Errors & Omissions / Network Security Liability and Privacy Insurance. Splunk shall carry insurance for network security liability and privacy with limits of not less than $3,000,000 per occurrence or wrongful act or per claim and $3,000,000 in the annual aggregate associated with the Services under this Agreement. Such insurance shall provide contractual liability coverage. Such insurance shall include coverage for: (a) liability arising from Customer Content and Personal Data being lost, stolen, compromised or used and/or something happening to such information that triggers a breach notice law or similar law regarding such information, and including but not limited to privacy notification costs, and (b) liability arising from the introduction of a computer virus into, or otherwise causing damage to, a customer's or third person's computer, computer system, network or similar computer-related property and the data, software and programs stored thereon. If Splunk carries the Technology Errors & Omissions / Network Security Liability and Privacy insurance required under this Agreement on a claims-made basis, the Splunk shall continue to maintain such insurance for two (2) years following the termination of this Agreement. Splunk may maintain this Technology Errors & Omissions / Network Security Liability and Privacy coverage in the same insurance policy that Splunk maintains pursuant to 10 above, provided that the limits of such insurance policy are not less than $5,000,000 per occurrence or wrongful act or per claim and $5,000,000 in the annual aggregate.

Certificates of Insurance. Upon Customer request, Splunk shall provide Customer with certificates of insurance demonstrating the maintenance of the required coverage. If any of the required insurance is cancelled or non-renewed, Splunk shall replace such insurance so that there is no lapse in coverage, and upon Customer request, Splunk shall provide Customer with a revised certificate of insurance evidencing same. Any acceptance of insurance certificates by Customer that do not comply with the requirements above, or Customer’s failure to obtain certificates, shallnot constitute a waiver of the requirements contained herein and shall not limit or relieve Splunkof the duties and responsibilities with respect to maintaining insurance assumed by it under this Agreement.

Primary and Non-Contributory; Waiver of Subrogation. The policy(ies) shall provide that Splunk’s insurance shall be primary to and noncontributory with any and all other insurance maintained by or otherwise afforded to Customer., its subsidiaries and Affiliates, and their respective officers, directors, shareholders, employees and agents, but only to the extent of liabilities falling within the indemnity obligations of Splunk pursuant to the terms of this Agreement. Except where prohibited by law and except with respect to the required Errors and Omissions insurance, Splunk and its respective insurers waive all rights of recovery or subrogation against Customer, its subsidiaries and Affiliates, and their respective officers, directors, shareholders employees, agents, and insurers, but only to the extent of liabilities falling within the indemnity obligations of Splunk pursuant to the terms of this Agreement.

11. <u>INDEMNITY</u>

11.1 Indemnification by Splunk. Splunk will defend Customer from and against any and all claims, losses, damages, liabilities, settlement, costs or expenses, and pay all damages (including attorneys’ fees and costs)(collectively “Claims”) awarded against Customer or agreed to in a court approved settlement, arising out of or in connection with (i) any infringement (or claim of infringement) of a third party’s Intellectual Property Rights or any other rights claiming that the Splunk Software or Splunk Content infringes such Intellectual Property Rights;. provided that Customer: (i) provides Splunk with prompt written notice of the Customer Claim; (ii) gives Splunk sole control of the defense and settlement of the Customer Claim (except that Splunk may not settle any Customer Claim that requires any action or forbearance on Customer’s part without Customer’s prior consent, which Customer will not unreasonably withhold or delay); and (iii) gives Splunk all reasonable assistance, at Splunk’s expense. Splunk will have no obligation under the foregoing provision to the extent a Customer Claim arises from Customer’s breach of the Agreement, Customer Content, Third Party Content, or the combination of the Splunk Software with: (a) Customer Content; (b) Third Party Content; (c) any software other than the Splunk Software; or (d) any hardware or equipment not controlled by Splunk. Splunk may in its sole discretion and at no cost to Customer: (1) modify any Service and/or Splunk Software so that it no longer infringes or misappropriates a third party right, (2) obtain a license for Customer’s continued use of the Splunk Software, in accordance with the Agreement, or (3) terminate this Agreement and refund Customer any prepaid fees covering the unexpired Subscription Term.

11.2 Customer Indemnity of Splunk. Unless expressly prohibited by applicable law, Customer will defend, and pay all damages (including attorneys' fees and costs) finally awarded against Splunk, or that are agreed to in a court-approved settlement, to the extent a claim, demand, suit or proceeding is made or brought against Splunk or its Affiliates by a third party (including those brought by a government entity) that: (i) alleges that Customer Content, Customer Applications or Customer's use of any Service infringes or misappropriates such third party's patent, copyright, trademark or trade secret, or violates another right of a third party; (ii) arises out of the activities of Users; or (iii) alleges that Customer Content, Customer Applications or Customer use of any Service violates applicable law or regulation (each, a "Splunk Claim"), provided that Splunk: (a) gives Customer prompt written notice of the Splunk Claim; (b) gives Customer sole control of the defense and settlement of the Splunk Claim except that Customer may not settle any Splunk Claim that requires any action or forbearance on Splunk's part without Splunk's prior consent (that Splunk will not unreasonably withhold or delay); and (c) Splunk gives Customer all reasonable assistance, at Customer expense.

12. U.S. GOVERNMENT USE OF THE SERVICES

13. DELETED.

14. GOVCLOUD RESTRICTED ACCESS

15. IMPORT & EXPORT CONTROL

The Services, the Splunk Software, and/or Splunk Content, or any feature or part thereof, may not be available for use in all jurisdictions, and Splunk makes no representation that the Services, the Splunk Software, and/or Splunk Content, or any feature or part thereof is appropriate or available for use in any particular jurisdiction. To the extent Customer chooses to access and use any Service, the Splunk Software, and/or Splunk Content, Customer does so at Customer's own initiative and at Customer's own risk, and Customer is responsible for complying with any applicable laws, rules, and regulations with respect to such access and use.

Customer's and its Users' use of the Services, the Splunk Software, and/or Splunk Content is subject to the customs and export control laws and regulations of the United States and may also be subject to the customs and export laws and regulations of other countries. Customer and its Users will fully comply with all applicable customs and export control laws and regulations of the United States and any other country where Customer or its Users use the Services, the Splunk Software, and/or Splunk Content. Customer certifies that Customer and its Users are not on any U.S. Government Lists of prohibited persons, including but not limited to the Treasury Department's List of Specially Designated Nationals, and the Commerce Department's List of Denied Persons or Entity List. Customer further certifies that Customer or its Users will not export, re-export, ship, transfer or otherwise use the Services, the Splunk Software, and/or Splunk Content in any country subject to an embargo or other sanction by the United States, including, without limitation, Iran, Syria, Cuba, Sudan and North Korea, and that Customer or its Users will not use the Services, the Splunk Software, and/or the Splunk Content for any purpose prohibited by U.S. laws, including, but not limited to, nuclear, chemical, missile or biological weapons related end uses. Customer or its Users are prohibited from sending to Customer's account any data or software that cannot be exported without prior written government authorization, including but not limited to, certain types of encryption software. These assurances and commitments will survive termination of this Agreement.

16. GENERAL TERMS

16.1 Anti-Corruption. Splunk uses diligent efforts to implement and maintain programs for its compliance with anti-corruption and anti-bribery laws. Each party agrees that it has not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any employees or agents of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. If either party learns of any violation of the above restriction, such party will use reasonable efforts to promptly notify the other party, in the case of notices to Splunk, to our Legal Department at legal-notices@splunk.com, and in the case of Customer to the main contact address provided by Customer to Splunk.

16.2 Governing Law; Venue. For Customers domiciled in the United States, Canada, Mexico, or a country in Central or South America or the Caribbean (the "**Americas**"), this Agreement willbe governed by and construed in accordance with the laws of the State of California, as if performed wholly within the state and without giving effect to the principles of conflict of law. For such Customers, any legal action or proceeding arising under this Agreement will be brought exclusively in the federal or state courts located in the Northern District of California and the parties hereby consent to personal jurisdiction and venue therein. Splunk may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of intellectual property or other proprietary rights of Splunk, its Affiliates, or any third party.

For Customers domiciled outside the Americas, this Agreement will be governed by the laws of England and Wales.

Neither the Uniform Computer Information Transactions Act ("**UCITA**"), nor the United Nations Convention for the International Sale of Goods will apply to this Agreement.

16.3 Independent Contractors; No Third Party Beneficiaries. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. The third-party licensors of Splunk Content are express third-party beneficiaries of the Agreement. There are no other third-party beneficiaries of this Agreement. Customer represents that it has the authority to bind itself and its Affiliates to the terms and conditions herein.

16.4 Amendment; Severability. This Agreement may only be amended by a written amendment signed by both parties, unless otherwise provided herein. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, invalid or unenforceable, the provision will be modified by the court and interpreted so as best to accomplish the objectives and intent of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement will remain in effect. If such construction is not possible, the invalid or unenforceable portion will be severed from this Agreement, but the remainder of the Agreement will remain in full force and effect.

16.5 Assignment. Customer may not assign, delegate or sublicense any of Customer's rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of Splunk.

16.6 No waiver. The failure of either party to exercise or enforce any right or provision of this Agreement will not constitute a waiver of such right or provision or of any other right or provision. All waivers must be in a signed writing to be effective.

16.7 Force Majeure. Splunk and its Affiliates, subsidiaries, officers, directors, employees, agents, partners and licensors will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond Splunk's or its Affiliates', officers', directors', employees', agents', partners', or licensors' reasonable control, including, without limitation, acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

16.8 Entire Agreement. This Agreement, which incorporates the Splunk Privacy Policy at the attached as of the Effective Date as Exhibit C, the Splunk Acceptable Use Policy at the attached as of the Effective Date as Exhibit F, the Splunk Standard Support Terms attached hereto as of the Effective Date as Exhibit G, the Splunk Service Level Schedule at Exhibit A attached hereto, the Documentation and the Order, as well as the terms and documents referred to in each, constitutes the entire agreement between Customer and Splunk and supersedes any prior agreements between Customer and Splunk concerning the Services, the Splunk Software, and/or Splunk Content (including, but not limited to, any prior versions of the Agreement) or any preprinted terms on a Customer's Order. This Agreement does not amend any other separate agreement Customer may have with Splunk for other software products or services that are not Services.

16.9 Notices to Customers and Consent to Electronic Communications. Customer consents to receiving electronic communications and notifications from Splunk in connection with the Services, and the linked policies and the Agreement. Customer agrees that any such communication will satisfy any applicable legal communication requirements, including that such communications be in writing. Splunk may provide Customer with notices regarding the Services, including changes to this Agreement and the linked policies, by email to the email address of Customer's administrator (and/or other alternate email address associated with Customer Account if provided), or by regular mail. It is Customer responsibility to keep Customer email address current. Customer will be deemed to have received any email sent to the email address then associated with Customer's account when Splunk sends the email. In the event Customer does not wish to accept any material change to the Services, the linked policies or to this Agreement, Customer will have the right, as its sole remedy, to terminate this Agreement within thirty (30) days of Splunk's notice of such change, and, if Customer exercises such termination right, Splunk will provide a pro rata refund to Customer equal to the amount fees pre-paid by Customer for the Service that corresponds to the period after the date of such termination for the Term.

16.10 Survival. The following sections will survive the termination or expiration of the Agreement: 2.2, 2.3, 2.4, 4.1, 5, 6.3, 6.4, 6.5 and 7-15.

17. DEFINITIONS

17.1 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

17.2 "API" or "Application Programming Interface" means a set of programming instructions, and standards for accessing a Service that Splunk provides to Customer in the Documentation and any other materials identified and provided by Splunk for and with a Service that are designed to enable the creation of Applications or otherwise support interoperability between a Service and Customer's systems or environment.

17.3 "Application" means any suite, configuration file, add-on, technical add-on, example module, command, function or application that extends the features or functionality of the applicable Service or the underlying Splunk Software.

17.4 "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. Customer Confidential Information includes Customer Content. Splunk Confidential Information will include: (i) nonpublic information relating to Splunk or its Affiliates' or business partners' products or services (including a Beta Service), technology, customers, business plans, promotional and marketing activities, finances and other business affairs; (ii) third-party information that Splunk is obligated to keep confidential; and (iii) the nature, content and existence of any discussions or negotiations between Customer and Splunk or its Affiliates. 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.

17.5 "Customer Applications" means Applications developed by Customer for use with the designated Service or Splunk Application.

17.6 "Customer Content" means the machine data (logs, metrics, or other data) that Customer ingests, or that is ingested, by a third party on Customer's behalf, into a Service.

17.7 "**Data Storage**" means the volume of data storage, as measured by uncompressed Customer Content that Customer may index using a Service, that Customer purchases, as listed in the Order subject to the policy attached hereto as of the Effective Date as Exhibit H and documentation attached hereto as of the Effective Date as Exhibit H.

17.8 "Documentation" means online user guides, documentation and help and training materials published on Splunk's website attached hereto as http://docs.splunk.com/Documentation or accessible through the applicable Services, as may be updated by Splunk from time to time.

17.9 “Effective Date” means the date a Service commences as listed on the Order.

17.10 “Forwarder” means that Splunk software application that collects data from remote end points for use as specified in the Documentation.

17.11 “HIPAA Data” means any protected health data, as defined in the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) as amended and supplemented by the Health Information Technology for Economic and Clinical Health Act, including the HIPAA omnibus final rule.

17.12 “**Initial Term**” is three (3) years from the last signature date herein.

17.13 “Internal Business Purpose” means Customer’s use of the Services for its own internal business operations, based on the indexing of Customer data from Customer’s systems, networks and devices. Such use does not include use by Customer on a service bureau basis or otherwise to provide services to, or process data for, any third party, or otherwise use to monitor or servicethe systems, networks and devices of third parties.

17.14 “ITAR Data” means information protected by the International Traffic in Arms Regulations.

17.15 “Licensed Capacity” means the maximum usage of the Services (e.g., aggregate daily volume of data indexed, based on source types, number of search and compute units, number of monitored accounts, storage capacity, etc.) that is permitted under the type of subscription included in the applicable Order.

17.16 “**Maximum Daily Indexing Volume**” means the maximum aggregate volume, in gigabytes, of uncompressed data that Customer may index using a Service each calendar day, as such maximum volume is specified in an Order.

17.17 “Order” means Splunk’s quote or ordering document (including online order form) accepted by Customer via Customer’s purchase order or other ordering document submitted to Splunk (directly or indirectly through an Authorized Reseller) to order Services, which references the Services, Licensed Capacity, pricing and other applicable terms set forth in an applicable Splunk quote or ordering document. Orders do not include the terms of any preprinted terms on a Customer purchase order or other terms on a purchase order that are additional or inconsistent with the terms of the Agreement.

17.18 “PCI Data” means credit card information within the scope of the Payment Card Industry Data Security Standard.

17.19 “**Renewal Term**” upon the expiration of the Initial Term the Agreement shall renew in 12 months increments each upon Customer’s issuance of a purchase order.

17.20 “Service” means any of the hosted services provided and maintained by Splunk for online searching, monitoring and analyzing of machine-generated data, including the associated API’s, the Splunk Software, and the Splunk Content (including, as applicable, Beta Services). The Services do not include Customer Content, or any Third Party Content, even if made available to Customer by Splunk in connection with any Service.

17.21 "Service Data" means data generated from cloud infrastructure, applications and other software, including Splunk's, tied to the usage, configuration, access, performance and security of the Services. For example, this may include such things as page views, interactions, errors, number of searches, source types and format (e.g., json, xml, csv), ingest volume, search concurrency, and session duration. Service Data does not include Customer Content.

17.22 "Splunkbase" means Splunk's online directory of or platform for Applications, currently located at https://splunkbase.splunk.com/ and any and all successors, replacements, new versions, derivatives, updates and upgrades thereto.

17.23 "Splunk Application(s)" means Applications made available through Splunkbase that are identified on Splunkbase as (i) published by Splunk (and not by any third party) and (ii) interoperable with a Service. "Splunk Application(s)" does not include Customer Content, or any Third Party Content.

17.24 "Splunk Cloud Site" means www.splunkcloud.com any successor or related site designated by Splunk for any Service.

17.25 "Splunk Content" means the information, data, technology and materials, other than Splunk Applications, that Splunk makes available at its discretion in connection with the Services or on a Splunk Cloud Site, including Documentation, sample code, software libraries, command line tools, and other related technology such as, add-ons and templates. Splunk Content does not include Splunk Software.

17.26 "Splunk Software" means a specific and unique instance of the Splunk software product that is made available to Customer as a Service or a part thereof, and includes any new releases or maintenance and support updates to such software as Splunk makes generally commercially available during the Subscription Term. Splunk Software does not include Splunk Applications.

17.27 "Subscription Term" means the duration of Customer's subscription to the applicable Service(s) under the Agreement that begins on the Effective Date and ends on the date listed on the applicable Order.

17.28 "Suggestion" means any suggested improvement or enhancement and any other recommendation or other feedback with respect to the Services, Splunk Software, Splunk Applications, Splunk Content, or Splunk Inc. that Customer provides to Splunk.

17.29 "Support" means the support terms available attached hereto as of the Effective Date as Exhibit G.

17.30 "Third Party Content" means information, data, technology, or materials made available to Customer by any third party that Customer licenses and adds to a Service or directs Splunk to install in connection with a Service. Third Party Content includes but is not limited to web-based or offline software applications, data service or content that are provided by third parties that interoperate with the Splunk Software or a Service, as for example, a software application that is developed by or for Customer, or a third-party software application that is available through www.splunkbase.com (whether they are categorized as "Developer Supported" or "Not Supported").

17.31 "User" means "Customer" and an individual whom Customer authorizes to use the Services and whom Customer (or Splunk, at Customer request) have supplied a user identification and password. Users may, for example, include Customer employees, consultants, contractors and agents.

Last revised on 06/26/2019

IN WITNESS WHEREOF, the parties hereto have executed and delivered this Agreement as of the dates set forth below.

SPLUNK INC.		**CUSTOMER: Customer Systems Inc.-Corporate Headquarters**	
Signature:	DocuSigned by: Tim Emanuelson 1B08ABB9F5E6465...	Signature:	DocuSigned by: Cathy Hilling BCD941D0892246E...
Name:	Tim Emanuelson	Name:	Cathy Hilling
Title:	VP, Controller	Title:	Contract Negotiator25-
Date:	18-Sep-2019	Date:	Sep-2019

EXHIBIT A
SPLUNK CLOUD SERVICE LEVEL SCHEDULE

Below is the Splunk Cloud Service Level Schedule as of the Effective Date, the most current schedule is available at https://www.splunk.com/en_us/legal/splunk-cloud-service-level-schedule.html.

Service Level Commitment

The Splunk Cloud Services will be available 100% of the time, as measured by Splunk over each calendar quarter of the Subscription Term, and subject to the exclusions set forth below (the "Service Level Commitment").

A Splunk Cloud Service is considered available if the Customer is able to login to its Splunk Cloud Service account and initiate a search using Splunk Software.

Service Level Credit:

If Splunk fails to achieve the above Service Level Commitment for a Splunk Cloud Service, Customer may claim a credit for such Splunk Cloud Service as provided below, up to a maximum credit per calendar quarter equal to one month's Splunk Cloud Service subscription fees.

PERCENTAGE AVAILABILITY PER CALENDAR QUARTER	CREDIT
100	NO CREDIT
99.99-99.999	2 HOURS
99.9-99.99	4 HOURS
99.0-99.9	8 HOURS
95.0-99.0	1 DAY
0-95.0	1 MONTH

Exclusions

A Customer will not be entitled to a service credit if it is in breach of its Agreement with Splunk, including payment obligations. The Service Level Commitment does not apply to any downtime, suspension or termination of the applicable Splunk Cloud Service (or any Splunk Content or Splunk Software operating in connection with the Splunk Cloud Service) that results from:

- Account suspension or termination due to Customer's breach of the Agreement.
- Routine scheduled maintenance (Splunk's Maintenance Policy is available at https://www.splunk.com/en_us/legal/splunk-cloud-service-maintenance-policy.html).
- Unscheduled, emergency maintenance or an emergency caused by factors outside Splunk's reasonable control, including force majeure events such as acts of God, acts of government, flood, fire, earthquake, civil unrest, acts of terror, Customer Content, Third Party Content or Internet Service Provider failures or delays.
- A Customer's equipment, software or other technology, or third-party equipment, software or technology (other than those which are under Splunk's control).
- Failures resulting from software or technology for which Splunk is not responsible under the Agreement.
- Customer's ability or inability to operate the Forwarder software is addressed by Splunk support services. For purposes of the Service Level Commitment, the Forwarder software is excluded from the calculation of the availability of the Splunk Cloud Services.

No Service Level Commitment is provided for free, proof-of-concept or unpaid trial services

Service Credit Claims.

To receive a service credit, a Customer must file a claim for such credit within five (5) days following the end of the calendar quarter in which the Service Level Commitment was not met for an applicable Splunk Cloud Service, by contacting Splunk at **splunk-cloud-billing@splunk.com** with a complete description of the downtime, how the Customer was adversely affected, and forhow long. Splunk reserves the right to deny the service credit if the Customer does not qualify.

The service credit remedy set forth in this Service Level Schedule is the Customer's sole and exclusive remedy for the unavailability of any applicable Splunk Cloud Service.

*All capitalized terms not otherwise defined are as set forth in the Splunk Cloud Terms of Service.

EXHIBIT B
SPLUNK CLOUD SECURITY ADDENDUM

Below is the Splunk Cloud Security Addendum as of the Effective Date, the most current addendum is available at https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html.

Notwithstanding anything in this Exhibit B, the “Splunk Cloud Data Processing Addendum” _(“Cloud DPA”) is attached hereto as Attachment 1. Anything in this Agreement or in this ExhibitB is deemed to be in addition to the Cloud DPA. In the event that anything in this Agreement orin this Exhibit conflicts with the Cloud DPA, the Cloud DPA shall govern the obligations of the parties regarding the processing of Personal Data.

This Splunk Cloud Security Addendum (CSA) sets forth the administrative, technical and physical safeguards Splunk takes to protect Customer Content in Splunk Cloud (Security Program). Splunk may update this CSA from time to time to reflect changes in Splunk’s security posture, provided such changes do not materially diminish the level of security herein provided.

This CSA is made a part of your Terms of Service (TOS) with Splunk (Agreement) and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement or Documentation, as applicable. In the event of any conflict between the terms of the Agreement and this CSA, this CSA will control. This CSA applies to Splunk Cloud environments initially provisioned on or after the Effective Date and does not apply to Splunk Cloud subscriptions purchased or acquired through Splunk.com, including without limitation Trial or Beta Services.

1. Purpose

1.1 This CSA describes the minimum information security standards that Splunk maintains to protect Customer Content. Requirements in this CSA are in addition to any requirements in the Agreement.
1.2 The CSA is reasonably designed to protect the confidentiality, integrity and availability of Customer Content against anticipated or actual threats or hazards; unauthorized or unlawful access, use, disclosure, alteration or destruction; and accidental loss, destruction or damage in accordance with laws applicable to the provision of the Service.

2. Splunk Security Program

2.1 Scope and Content. Splunk Security Program: (a) complies with industry recognized information security standards; (b) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Content; and (c) is appropriate to the nature, size and complexity of Splunk’s business operations.
2.2 Security Policies, Standards and Procedures. Splunk maintains security policies, standards and procedures (collectively, Security Policies) designed to safeguard the processing of Customer Content by employees and contractors in accordance with this CSA.
2.3 Security Program Office. Splunk’s Chief Information Security Officer leads Splunk’s Security Program and develops, reviews and approves (together with other stakeholders such as Legal and Internal Audit) Splunk’s Security Policies.
2.4 Security Program Updates. Splunk Security Program 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. Employees receive information and education about Splunk's Security Policies during onboarding and annually thereafter.

2.5 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 Splunk's 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.

3. Risk Management

3.1 Splunk has a security risk assessment program and management process to identify potential threats to the organization.

3.2 Splunk management rates and reviews identified, material risks to determine if existing controls, policies and procedures are adequate. Risk mitigation plans are implemented as needed to address material gaps considering the nature of Splunk's business and the information it stores.

4. Change Management

4.1 Splunk deploys changes to the Services during maintenance windows, details of which are posted to the Splunk website or communicated to customers as set forth in the Splunk Cloud Service Maintenance Policy.

4.2 Splunk follows documented change management policies and procedures for requesting, testing and approving application, infrastructure and product related changes.

4.3 Changes undergo appropriate levels of review and testing, including security and code reviews, regression testing and user acceptance prior to approval for implementation.

4.4 Software development and testing environments are maintained and logically separated from the production environment.

5. Incident Response and Breach Notification

5.1 Splunk has an incident response plan (the Splunk Incident Response Framework or SIRF) and team to assess, respond, contain and remediate (as appropriate) identified security issues, regardless of their nature (e.g., physical, cyber, product). Splunk reviews and updates the SIRF once annually to reflect emerging risks and "lessons learned."

5.2 Splunk notifies Customers without undue delay after becoming aware of a Data Breach. As used herein, Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Content under the applicable Agreement, including Personal Data as defined under the General Data Protection Regulation (EU) 2016/679 (GDPR), while being transmitted, stored or otherwise processed by Splunk.

5.3 In the event of a Data Breach involving Personal Data under the GDPR, if customer reasonably determines notification is required by law, Splunk will provide reasonable assistance to the extent required for the Customer to comply with applicable data breach notification laws, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.

5.4 In the event of a conflict between the breach notification provisions in this CSA and those set forth in an applicable Business Associate Agreement (BAA) with Splunk, the BAA breach notification terms will apply.

6. Governance and Audit

6.1 Splunk conducts internal control assessments on an ongoing basis to validate that controls are designed and operating effectively. Issues identified from assessments are documented, tracked and remediated as appropriate.

6.2 Third party assessments are performed as part of our onboarding process and periodically thereafter to validate ongoing governance of control operations and effectiveness. Issues identified are documented, tracked and remediated as appropriate.

7. Access and User Management

7.1 Splunk implements reasonable controls to manage user authentication for employees or contractors with access to Customer Content, including without limitation, assigning each employee or contractor with unique and/or time limited user authorization credentials for access to any system on which Customer Content is accessed and prohibiting employees or contractors from sharing their user authorization credentials.

7.2 Splunk allocates system privileges and permissions to users or groups on a “least privilege” principle and reviews user access lists and permissions on a quarterly basis, at minimum.

7.3 New users must be pre-approved before Splunk grants access to Splunk corporate and cloud networks and systems. Pre-approval is also required before changing existing user access rights.

7.4 Splunk promptly disables application, platform and network access for terminated users upon notification of termination.

8. Password Management and Authentication Controls

8.1 Authorized users must identify and authenticate to the network, applications and platforms using their user ID and password. Splunk’s enterprise password management system requires minimum password parameters.

8.2 SSH key authentication and enterprise password management applications are utilized to manage access to the production environment.

8.3 Two-factor authentication (2FA) is required for remote access and privileged account access for Customer Content production systems.

9. Encryption and Key Management

9.1 Splunk uses industry-standard encryption techniques to encrypt Customer Content in transit. The Splunk System is configured by default to encrypt user data files using transport layer security (TLS) encryption for web communication sessions.

9.2 Splunk relies on policy controls to help ensure sensitive information is not transmitted over the Internet or other public communications unless it is encrypted in transit.

9.3 Where applicable, Splunk uses encryption at rest with a minimum encryption protocol of Advanced Encryption Standard (AES) 256-bit encryption.

9.4 Splunk uses encryption key management processes to help ensure the secure generation, storage, distribution and destruction of encryption keys.

10. Threat and Vulnerability Management

10.1 Splunk has a Threat and Vulnerability Management (TVM) program to continuously monitor for vulnerabilities that are acknowledged by vendors, reported by researchers or discovered internally through vulnerability scans, Red Team activities or personnel identification.

10.2 Splunk documents vulnerabilities and ranks them based on severity level as determined by the likelihood and impact ratings assigned by TVM. Splunk assigns appropriate team(s) to conduct remediation and track progress to resolution as needed.

10.3 For systems containing Customer Content, an external vendor conducts security penetration tests on the corporate and cloud environments at least annually to detect network and application security vulnerabilities. Critical findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation. In addition, Splunk conducts internal penetration tests quarterly and remediates findings as appropriate.

11. Logging and Monitoring

11.1 Splunk continuously monitors application, infrastructure, network, data storage space and system performance.

11.2 The Splunk Security Team reviews key reports daily and follows up on events as necessary.

12. Secure Development

12.1 Splunk's Software Development Life Cycle (SDLC) methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of software components.

12.2 For major product releases, Splunk uses a risk-based approach when applying its standard SDLC methodology, which may include such things as performing security architecture reviews, open source security scans, dynamic application security testing, network vulnerability scans and external penetration testing in the development environment. Splunk performs security code review for critical features if needed; and performs code review for all features in the development environment. Splunk scans packaged software to ensure it's free from trojans, viruses, malware and other malicious threats.

12.3 Splunk utilizes a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository are reviewed periodically and limited to authorized employees.

12.4 The SDLC methodology does not apply to free Applications developed by Splunk or to Third Party Content, including any made available on splunkbase.com. For information on the inspection process for applications available on splunkbase.com, see AppInspect.

13. Network Security

13.1 Splunk uses industry standard technologies to prevent unauthorized access or compromise of Splunk's network, servers or applications, which include such things as logical and physical controls to segment data, systems and networks according to risk. Splunk monitors demarcation points used to restrict access such as firewalls and security group enforcement points.

13.2 Remote users must authenticate with two-factor authentication prior to accessing Splunk networks containing Customer Content.

14. Vendor Security

14.1 Splunk's vendor management team assesses risks associated with new vendors prior to onboarding and thereafter manages them through its risk management program. The vendor management team employs a risk-based vendor scoring model to monitor third-party risk.

14.2 Confidential Information is shared only with those who are subject to appropriate confidentiality terms with Splunk.

14.3 Splunk uses a risk-based approach to verify on-going vendor compliance with Splunk's Security Policies.

15. Physical Security

15.1 Splunk grants physical access to Splunk facilities (including data centers where necessary) based on role. Splunk removes physical access when access is no longer required, including upon termination.
15.2 Personnel must carry, and visitors must wear, identity badges when in Splunk facilities. Visitors must always be accompanied. Splunk logs visitor access to Splunk facilities. Splunk reviews data center physical access, including remote access, on a quarterly basis to confirm that access is restricted to authorized personnel.

16. Disaster Recovery Plan
16.1 Splunk has a written Disaster Recovery Plan to manage significant disruptions to Splunk Cloud operations and infrastructure. Splunk management updates and approves the Plan annually.
16.2 Splunk personnel perform annual disaster recovery tests. Test results are documented, and corrective actions are noted.
16.3 Data backup, replication and recovery systems/technologies are deployed to support resilience and protection of Customer Content.
16.4 Backup systems are configured to encrypt backup media.

17. Asset Management and Disposal
17.1 Splunk maintains and regularly updates an inventory of Cloud infrastructure assets and reconciles the asset list monthly.
17.2 Documented, standard build procedures are utilized for installation and maintenance of production servers.
17.3 Documented data disposal policies are in place to guide personnel on the procedure for disposal of Customer Content.
17.4 Upon expiration or termination of the Agreement, Splunk will return or delete Customer Content in accordance with the terms of the Agreement. If deletion is required, Customer Content will be securely deleted, except that Customer Content stored electronically in Splunk's backup or email systems may be deleted over time in accordance with Splunk's records management practices.

18. Human Resources Security
18.1 Splunk personnel sign confidentiality agreements and acknowledge Splunk's Acceptable Use Policy during the new employee onboarding process.
18.2 Splunk conducts background verification checks for potential Splunk personnel with access to Customer Content in accordance with relevant laws and regulations. The background checksare commensurate to an individual's job duties.

19. CSA Proof of Compliance
19.1 Splunk Cloud Standard: Security Audits. At least once a year, Splunk Cloud (Standard Environment) undergoes a security audit by an independent third party that attests to the effectiveness of the controls Splunk has in place to safeguard the systems and operations where Customer Content is processed, stored or transmitted (e.g., System and Organizational Control (SOC 2), Type 2) audit in accordance with the Attestation Standards under Section 101 of the codification standards (AT 101). At a minimum, the audit covers the Security, Confidentiality, and Availability control criteria developed by the American Institute of Certified Public Accountants (AICPA). Currently, Splunk is audited against ISO 27001 and SOC 2, Type 2. Upon request, Splunk will supply Customer with a summary copy of Splunk's annual audit reports, which will be deemed Confidential Information under the Agreement.

19.2 Splunk Cloud Premium: Security Audits. For customers requiring Payment Card Industry Data Security Standards (PCI-DSS) or the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA) security standards, Splunk offers a PCI-DSS or HIPAA certified environment (Premium Environment). At least once a year, Splunk Cloud Premium Environment undergoes a security audit performed by an independent third party that attests to the effectiveness of the controls Splunk has in place to safeguard the systems and operations where Customer Content is processed, stored or transmitted.

19.2(i) PCI-DSS. In the case of PCI-DSS, Splunk offers cloud services as a Level 1 PCI service provider. Splunk complies with the most recent version of PCI-DSS to the extent PCI-DSS is applicable to the Services provided under the Agreement (e.g., if Splunk accesses, collects, uses, retains, discloses, processes, stores or transmits any Customer cardholder data as defined under PCI-DSS or any other data protected or subject to PCI-DSS), or if any part of such services impacts the security of the PCI Data environment.

19.2(ii) HIPAA. In the case of HIPAA, Splunk complies with the HIPAA security rule standards for the processing of protected health information (PHI).

Upon request, Splunk will supply Customer with proof of Splunk's compliance with PCI-DSS or HIPAA, as applicable.

EXHIBIT C
SPLUNK PRIVACY POLICY

Below is the Splunk's Privacy Policy as of the Effective Date, the most current policy is available at http://www.splunk.com/view/SP-CAAAAAG.

Updated: May 2019

This Privacy Policy explains how Splunk Inc. ("Splunk") collects, uses, and discloses information you provide to us or which we otherwise collect in providing products or services to you ("Information"), including "Personal Data" by which we mean information that allows us to determine your identity when you engage with us.

Notwithstanding anything in this Exhibit C, the "Splunk Cloud Data Processing Addendum" ("Cloud DPA") is attached hereto as Attachment 1. Anything in this Agreement or in this Exhibit C is deemed to be in addition to the Cloud DPA. In the event that anything in this Agreement or in this Exhibit conflicts with the Cloud DPA, the Cloud DPA shall govern the obligations of the parties regarding the processing of Personal Data.

The use of our products and services ("Splunk Offerings") is subject to the terms of the applicable customer agreement, the use of our website is subject to the **Splunk Website Terms and Conditions of Use**, and the terms of this Privacy Policy are incorporated into each and form part of those agreements.

Data Collection
What We Collect Via Your Interactions
How We Use Information Collected From Interactions
Exercising Your Rights In Europe
Opting Out Of Marketing Emails
What We Collect Via Splunk Offerings And How We Use It
Other Collection Practices
Data Collection Practices Associated With Apps
How Splunk Shares Your Information
Lawful Basis For Transferring Your Data
How We Secure Your Information
Splunk Also Observes The Following Practices
Updates To This Privacy Policy
Contact Splunk
Links to Related Agreements, Policies and Information

Data Collection. There are two primary ways in which Splunk collects Information from you: through Interactions and through Splunk Offerings.

Interactions

When you interact online or offline with Splunk, we may receive your Information, including your Personal Data. For example, we receive your Information when you:

- Visit and use Splunk's websites
- Download materials through the websites
- Provide or update account information through the websites

- Register or attend Splunk-hosted or sponsored events (such as promotional events, webcasts, contests or hackathons)

We collect Information about you from other sources such as public databases, joint marketing partners, social media platforms, conference/event hosts, and partners when you interact with them.

We refer collectively to these contacts as “Interactions” and we explain below how we use the Information we collect through them.

Splunk Offerings

We also collect Information, including Personal Data, when necessary to provide our Splunk Offerings to you or to fulfill our legitimate interests, as described below. We may ask you for this data directly, or in some cases, we may collect it when certain features are enabled in our Splunk Offerings. For example, we collect your Information when you (or someone you work with):

- Trial or order any of our Splunk Offerings
- Interact with Splunk online or offline, including when you request support services
- Use Splunk Offerings to process information

What We Collect Via Your Interactions

We (or others acting on our behalf) may collect your Information, including your Personal Data, through the Interactions described above. Categories of Personal Data we collect include such things as:

- Name
- Email address
- Physical address, including country
- Employer
- Title/Position
- Payment details
- Phone number
- User name / user ID
- IP address

We collect Personal Data in various ways, such as when you manually key in your Personal Data to our website forms or provide it to us or others from whom we receive marketing leads. IP addresses are collected on an automated basis through your use of the website services using cookies, web beacons, and like technologies. We may infer your location from your IP address. For more on the use of cookies and like technologies, see our **Splunk Cookie Policy**.

How We Use Information Collected From Interactions

Splunk uses the Information it collects from your Interactions to deliver services to you in accordance with our terms, to satisfy our legal obligations, or to satisfy our legitimate interests, as described below. We take seriously the need to balance our legitimate interests with your privacy rights and summarize for you here how we use your Information, including Personal Data.

We use your Information to:

- Fulfill your orders or respond to your requests for information

To satisfy your requests for website materials such as marketing collateral or white papers, we collect and use your name and email address.

- Improve and develop the website services
  We collect Information via cookies and like technologies as set forth in our Splunk Cookie Policy to help us fulfill our legitimate interest in improving our website services and make them more relevant to you.
- Issue you Splunk accounts for access to online communities and forums
  When you join our online communities and forums, we collect your Personal Data so you can participate. The guidelines associated with those communities and forums recommend not sharing private or proprietary information on them, as many aspects of them are public.
- Send administrative information
  We may need to notify you (or we may choose to inform you) when we make updates to our terms or policies or make changes to our website services. We will use your name and email address to send these administrative notices to you, which due to their nature are treated differently from marketing communications from which you can opt out.
- Manage your Splunk account
  In order to perform the services under the contract between you and Splunk, we need to collect certain Information from you such as your contact and payment details. Without this Information, we may not be able to deliver the services or comply with our legal obligations.
- Send you marketing communications
  Where we have your consent to do so (if required), we will email you product announcements, educational materials or information about special offers or upcoming online or offline events, such as SplunkLive or .conf. In accordance with applicable law, we give you the choice to opt out of receiving these materials.
- Invite you to participate in surveys, studies, and assessments of Splunk Offerings
  We use your Personal Data to request feedback from you about our Splunk Offerings so that we can fulfill our legitimate interest in improving them and continue to grow our business. Your participation in user surveys is voluntary and subject to your consent, the terms of your agreements with us, and this Privacy Policy.
- Personalize your experience
  We use your Personal Data to satisfy our legitimate interest in presenting you with content tailored to your interests using cookies, web beacons, and like technologies. (For more information see the Splunk Cookie Policy.) We may also receive your location information in connection with certain services. You can update your device location setting permissions at any time to disable collection.
- Diagnose and fix technical issues, monitor for security, and otherwise protect our property
  We do this to satisfy our legitimate interest in anticipating and recognizing potential threats to the operation and security of our website services to help keep them online and secure. We may process your Personal Data, in particular your IP address, for this purpose.
- To comply with any applicable law, regulation, legal process, or governmental request, or to protect our legal rights
- For any other purpose disclosed to you in connection with our website services from time to time

If we process your Personal Data for a purpose other than that set out above, we will provide you with information prior to such processing.

Exercising Your Rights in Europe

If you are in the European Union or the United Kingdom, you have the right to: request access to and correction of your Personal Data; restrict or object to the processing of your Personal Data; and request your Personal Data be "forgotten" (technically erased). If you would like to exercise these rights, contact us at: **datasubjectrequests@splunk.com**. Please describe the nature of your request and the Personal Data it relates to, and we will comply as soon as reasonably practicable, consistent with applicable law. We will verify your identity before we comply with your request, and therefore, ask for your cooperation with our identity verification process.

If we process your Personal Data based on your consent, you may withdraw your consent at any time. We will let you know if we are seeking to rely on your consent at the time we collect your information.

Opting Out of Marketing Emails

If you no longer want to receive marketing-related emails from Splunk on a go-forward basis, please send an email to that effect to: **marketingops@splunk.com**. Alternatively, you may use the "unsubscribe" feature in our email messages.

What We Collect Via Our Splunk Offerings and How We Use It

On-premises Product Data. We collect and process different types of product data (as described below) when you deploy the Splunk Offerings on-premises ("Splunk On-premises Offerings") to serve our legitimate interest of improving our products and services. We work hard to help ensure a balance between our legitimate interests and your privacy rights.

- ***License Usage Data*** is Information that allows us to identify your account entitlements, such as license consumption and license type, in our systems through an assigned license ID.
- ***Aggregated Usage Data*** Is Information about your operating environment and session, such as your network and systems architecture, page loads and views, and searches by type. We aggregate this Information to analyze usage patterns. Once we verify that the data received is from a valid Splunk product, we discard the license ID. We hash user IDs connected to page view activity before analysis by Splunk. For more on Aggregated Usage Data, see **Splunk's Documentation (Share Performance Data)**.

  Splunk uses Aggregated Usage Data to fulfill our legitimate interest in enhancing the Splunk Offerings. For example, we may use this data to:
  - Better understand how our users configure and use Splunk On-premises Offerings
  - Determine which configurations or practices optimize performance (e.g., best practices)
  - Benchmark key performance indicators ("KPIs")
  - Perform data analysis and audits
  - Identify, understand, and anticipate performance issues and the factors that affect them
  - Improve the operation of the Splunk Offerings
  - Develop new features and functionality
- ***Support Usage Data*** is Aggregated Usage Data, but the license ID persists so that the Information can be linked to your account. We use this data to analyze performance information, troubleshoot issues, personalize your experience, suggest other Splunk Offerings that may be of interest to you, or provide guidance to help you optimize your use of your Splunk On-premises Offering.

In our paid Splunk On-premises Offerings, you have the option of configuring your settings to opt out of providing License Usage, Aggregated Usage and Support Usage Data. For opt-out instructions, see **Splunk's Documentation (Share Performance Data)**.

Splunk Cloud Offerings Service Data. We collect and process data generated by your use of Splunk's cloud-based offerings, such as the Splunk Cloud and VictorOps services ("Splunk Cloud Offerings"). We collect this data to help fulfill our contractual obligations to you and to serve our legitimate interest in improving the service. We work hard to help ensure a balance between our legitimate interests and your privacy rights.

Service Data is Information generated by your use of the Splunk Cloud Offerings such as page views, interactions, errors, number of active and licensed users, number of searches, source types and format (e.g., json, xml, csv), and app workflows. Splunk uses Service Data to provide and enhance the Splunk Offerings. For example, we may use this data to:

- Help analyze and troubleshoot issues
- Personalize your experience and suggest other Splunk Offerings that may be of interest to you
- Provide guidance to help you optimize your usage
- Analyze behavior and performance across deployments
- Benchmark KPIs (data aggregated and pseudonymized)
- Perform data analysis and audits
- Identify, understand, and anticipate performance issues and the factors that affect them
- Improve the operation of Splunk Offerings
- Develop new features and functionality

Service Data is collected by Splunk as part of the Splunk Cloud Offering, including free or trial offers, and may contain incidental pieces of identifying information necessary to monitor the health, performance or security of your deployment. Splunk restricts access to this information, and where feasible, aggregates and pseudonymizes it.

Location Data is data we collect in certain Splunk Offerings ("apps" and "add-ons", as discussed below) that associates your end users' mobile device with an identifier for your app to help us improve the user experience and personalize your services and content. Depending on your configuration of the Splunk Offerings, it may be that location information on your end users is shared with Splunk, however, you can disable this function if you so choose (or advise your end users about how to disable it) through the location setting on their mobile device.

For more information about the data collected through use of your Splunk Offerings, see our **Documentation** for the relevant Splunk Offering (e.g., **Share Performance Data** for Splunk Enterprise).

Other Collection Practices

We also collect Personal Data from you to fulfill our contractual commitments to you. For example, we collect contact information such as name, address (email and physical) and phone number to enter you into our customer database systems and manage your account. This may also include Information about billing and payments, customer service, support services, or software updates.

We share this Information with our affiliates, vendors and partners who help us service your account and with whom we have written agreements protecting the confidentiality, privacy and security of your Information. We do not sell this Information.

Data Collection Practices Associated with Apps

The Splunk Offerings are extendible using software applications commonly called “apps”, “add-ons” or “technical add-ons” that we offer through splunkbase.splunk.com. We refer to these collectively as “Apps”. These Apps are versatile and have access to a broad set of web technologies that can be used to collect and use your Information. This Privacy Policy only applies to Apps developed by Splunk.

Splunk requires other App developers to comply with applicable privacy and data protection laws, but cannot guarantee that they do so. You should familiarize yourself with the privacy policies and license agreements that apply to those Apps regardless of whether they are available on splunkbase.splunk.com, third-party marketplaces (e.g., AWS Marketplace) or packaged with a Splunk Offering.

Splunk collects data generated from the use and performance of Apps that interoperate with Splunk Offerings, such as crash information, version, session duration, user engagement, and number of downloads, active/licensed users, and log ins. We may share this information with App developers so they can improve and enhance the performance of their Apps.

How Splunk Shares Your Information

Splunk may disclose Information to third parties in the following ways:

- ***Affiliates***. We may disclose Information to our affiliates subject to this policy in order for them to help administer or service the Splunk Offerings. Splunk is the party responsible for the management of jointly-used Personal Data. Splunk maintains intragroup agreements with its affiliates covering the use of Personal Data within the Splunk family of companies.
- ***Service Providers***. We may disclose Information to our service providers (e.g., infrastructure as a service, order fulfillment, professional/customer/support services), pursuant to written agreements with confidentiality, privacy and security obligations. Splunk maintains a list of its sub-processors who process Personal Data as part of the Splunk Offerings, which Splunk updates, as needed.
- ***App Developers.*** We may disclose Information about App use and performance with App developers so that they can improve and enhance the performance of their Apps. App developers will be identified to you when you download and use their Apps pursuant to their license terms, including their privacy policies.
- ***Partners and Sponsors.*** We may disclose contact and account Information to our partners and event sponsors (identified at time of registration or event participation) pursuant to written agreements with confidentiality, privacy and security obligations. They may use the Information to assess your interest in Splunk Offerings, conduct user research and surveys, or send you marketing communications, subject to the terms of their privacy policies. We may also share On-premises Product Data and Service Data from Splunk Cloud Offerings with partners who provide you with support services.
- ***Compliance and Safety.*** We may disclose Information as necessary or appropriate under applicable laws (including laws outside your country of residence) to: comply with legal process or requirements; respond to requests from public and government authorities (including those outside your country of residence); enforce our terms and conditions; and

protect our operations or those of any of our affiliates; and our rights, privacy, safety, or property, and/or that of our affiliates, you or others.

- ***Merger, Sale, Etc.*** We may disclose Information in the event of a proposed or actual reorganization, merger, sale, joint venture, corporate transaction, assignment, transfer, or other disposition of all or any portion of Splunk business, assets or stock (including Information regarding any bankruptcy or similar proceedings).
- ***Other Users****.* We may disclose Information to other users of the service in aggregated format, provided it does not include Personal Data. This may include "best practices" tips, KPIs, benchmark data or other such aggregated information useful to the user community.

Lawful Basis for Transferring Your Data

Splunk is committed to uphold the privacy principles articulated in the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield Frameworks ("Privacy Principles") regarding the collection, use, and retention of personal information transferred from the European Union, the EEA, the United Kingdom, and/or Switzerland, as applicable, to the United States in reliance on Privacy Shield. Splunk has self-certified to the Department of Commerce that it adheres to the Privacy Principles with respect to such information. If there is any conflict between the terms in this Privacy Policy and the Privacy Principles, the Privacy Principles will govern. Splunk's certifications to these Privacy Shield Frameworks may be found **here**.

How We Secure Your Information

Splunk takes reasonable technical and organizational measures to safeguard Personal Data against loss, theft, and unauthorized access, disclosure, alteration, misuse, or destruction. Unfortunately, no data transmission, software, or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of an account has been compromised), please notify us immediately in accordance with the "Contact Splunk" section below. If Splunk learns of a breach of its systems, Splunk may notify you or others consistent with applicable law and/or as agreed in our contract with you. Splunk may communicate with you electronically regarding security, privacy, and administrative issues relating to your use of the Splunk Offerings and the Information you provide to us.

Splunk Also Observes the Following Practices

Retention Period. We retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required or not prohibited by applicable law. Information you store in our Splunk Cloud Offerings is portable by you at the end of the term of your agreement with Splunk. We retain your contract information for the duration of your contract with us and thereafter as required or permitted by law. See **Data Retention Policies** for further details.

Use of Splunk Offerings by Minors. The Splunk Offerings are not directed to individuals sixteen (16) and under or those not of the age of majority in your jurisdiction, and we request that these individuals not provide Personal Data through the Splunk Offerings.

Cross-border Transfers. Your Personal Information may be stored and processed in any country where we have facilities or in which we engage service providers which are located outside of your country of residence, including to the United States. Different data protection rules than those applicable in your country may therefore apply. As indicated above, Splunk has certified to the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield Frameworks for the transfer of Personal Data from the EEA, the United Kingdom, and Switzerland to the U.S. We put in place adequacy mechanisms to protect your Personal Data in our agreements with our service providers.

Links to Other Parties. The Splunk Offerings may contain links to or facilitate access to other websites or online services. This Privacy Policy does not address, and Splunk is not responsible for the privacy, information, or practices of other parties, including any App developer, App provider, social media platform provider, operating system provider, wireless service provider, or device manufacturer. The inclusion of a link within the Splunk Offerings does not imply endorsement of the linked site or service by us or our affiliates. Splunk encourages you to review the privacy policies and learn about the privacy practices of those companies whose websites you choose to visit. We list below links to resources about many of the other parties with whom we interact as described in this Privacy Policy:

- For partners
- For App developers/providers listed on Splunk's app ecosystem, Splunkbase
- For other marketplaces where Splunk Apps may be found
- For industry content providers (such as providers of research, white papers, etc.)
- For industry award providers (such as those listed on Splunk.com)
- For resources (such as source code repositories, sample data sources, customers, etc.) mentioned in blogs and press releases
- For other providers, sponsors, or speakers at events in which Splunk is involved
- For social media platform providers (such as Twitter, LinkedIn, YouTube, or Facebook)

Updates to this Privacy Policy. We may change this Privacy Policy from time to time and will post our updates **here**. We will also communicate any material changes of the Privacy Policy to you.

Contact Splunk

If you have any questions or comments about this Privacy Policy, the information practices of the Splunk Offerings, or your dealings with Splunk, you can contact us at any time:

Splunk Inc.
Attention: Legal Dept.
San Francisco, CA headquarters
DPO@splunk.com

Splunk UK
Attention: Legal Dept.
Paddington area United Kingdom office
PrivacyShield@splunk.com

Splunk Germany
Attention: Legal Dept.
Munich area Germany office
PrivacyShield@splunk.com

If your request or concern is not satisfactorily resolved by us, you may approach your **local data protection authority**.

EXHIBIT D
Data Ingestion and Daily License Usage

Below is Splunk's data ingestion and daily license usage policy as of the Effective Date, the most current policy is available at http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DataPolicies#Data_ingestion_and_daily_license_usage.

Your Splunk Cloud license governs how much data you can load into your Splunk Cloud deployment per day (GMT). To see current and past daily data ingestion information in Splunk Web, use the Monitoring Console app. To do this, choose **Apps**, click **Cloud Monitoring Console** and navigate to the License Usage page. Splunk recommends you set up alerts in the system to monitor your license usage.

You can exceed your purchased daily index volume a maximum of five times in a calendar month. If you exceed your daily limit more than five times in a calendar month, what happens depends on the type of Splunk Cloud deployment you have, as follows:

- **Managed Splunk Cloud**: Your Splunk sales representative may work with you to help you reduce your usage to stay within the purchased limit or to purchase the necessary increase. If you are unable or unwilling to abide by the applicable usage limit, you will pay any invoice for excess usage in accordance with your Terms of Service.
- **Self-service Splunk Cloud deployments:** Your Splunk Cloud instance is locked. You can reset a locked instance three times in a 90-day period. To reset a locked instance, go to your Splunk customer portal and click the **Unlock License** button. To unlock your instance, your Splunk user must have administrator and instance owner level privilege.

If you consistently exceed your licensed limit, contact Splunk Sales to do a benchmark assessment to determine your volume needs and purchase an appropriate plan to handle your volume.

EXHIBIT E
Splunk App Support Types

Below is information on Splunk Apps as of the Effective Date, the most current information is available at https://docs.splunk.com/Documentation/Splunkbase/splunkbase/Splunkbase/Appsupporttypes.

Splunkbase apps can have the following types of support.

Type	Description
Splunk supported	Applies to apps and add-ons published by Splunk Inc. that are supported and maintained by Splunk. Splunk will provide customers with active support subscriptions an initial response and acknowledgement to any support request for these apps or add-ons in accordance with P3 terms. Splunk will also ensure compatibility of Splunk Supported apps and add-ons with future releases of applicable Software. Splunk ensures this compatibility for any Splunk Supported apps or add-ons installed in Splunk Cloud before commencing Splunk Cloud upgrades. Splunk does not provide support or maintenance for apps or add-ons published by any party other than Splunk Inc., including third-party developers.
Developer supported	Applicable only to apps and add-ons published by parties other than Splunk Inc. Any support or maintenance for these apps and add-ons are provided by the developer, whose contact information can be found on the download page. Splunk reserves the right to remove the Developer Supported classification of third-party apps and add-ons if the developer is not, in Splunk's determination, fulfilling reasonable obligations for support and maintenance. For example, failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable Splunk Software will result in reclassification to Not Supported. Customers are responsible for engaging directly with the developer of Developer Supported apps and add-ons to ensure proper functionality and version compatibility with the applicable Splunk Software. If functional or compatibility issues that may arise are not resolved, customers may be required to uninstall the app or add-on from their Splunk environment in order for Splunk to fulfill support obligations. For Splunk Cloud customers, the Service Level Commitment and Service Level Credit in the Splunk Service Level Schedule will not apply for any issues caused by Developer Supported apps or add-ons.
Not supported	Applicable to applications and add-ons published by Splunk or third-party developers. Indicates that no support or maintenance are provided by the publisher. Information from the user community might be available from sources such as Splunk Answers. Customers are solely responsible for ensuring proper functionality and version compatibility of Not Supported apps and add-ons with the applicable Splunk software. If unresolvable functional or compatibility issues are encountered, customers may be required to uninstall the app or add-on from their Splunk environment in order for Splunk to fulfill support obligations. For Splunk Cloud customers, the Service Level Commitment and Service Level Credit in the Splunk Service Level Schedule will not apply to issues caused by Not Supported apps or add-ons.

EXHIBIT F
Splunk Acceptable Use Policy for Cloud Offerings

Below is the Splunk Acceptable Use Policy for Cloud Offerings as of the Effective Date. The most current policy is available at https://www.splunk.com/view/SP-CAAAMB6.

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 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. If Customer violates this Policy or authorizes or assists others in doing so, Splunk may suspend or terminate Customer's use of the Splunk Service.

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. Splunk may remove, disable access to or modify any content or resource that violates this Policy or any other agreement between Customer and Splunk. 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 G
SUPPORT TERMS FOR SPLUNK CLOUD SERVICES

Below are Splunk's support terms as of the Effective Date, the most current support terms are available at http://www.splunk.com/goto/cloud_support.

Splunk provides telephone support (for most products), online documentation, web forums, email and a web-based portal for submitting cases and tracking case status. Support cases are handled based on case priority levels as described below. When submitting a case, Customers will select the priority for initial response by logging the case online, in accordance with the priority guidelines set forth below. When the case is received, Splunk Customer Support may change the priority if the issue does not conform to the criteria for the selected priority and will provide Customers with notice (electronic or otherwise) of such change. Splunk will respond to Splunk support requests in accordance with the guidelines set forth below. Customers of Splunk Light delivered as a cloud service are entitled to the support indicated below with *Splunk Light designations.

Case Priority Levels
Case priorities are assigned based on the technical importance of the problem.
P1 = Splunk Cloud Service is completely inaccessible.
P2 = One or more key features of Splunk Cloud Service are unusable.
P3 = Any other case where a Splunk Cloud Service is not operating as documented or when a Splunk Cloud Service is being used within the purchased aggregate volumes and storage periods, and there is a material degradation in the performance of the Splunk Cloud Service.
P4 = All enhancement requests.

Response Times
Initial Response & Acknowledgment, by case priority
P1: 2 hours
P2: Next business day
P3: Two business days (*Splunk Light)
P4: Two business days

Escalation, by case priority
P1: Manager: Immediate / VP: 1 business day
P2: Manager: 1 business day / VP: 1 week
P3: VP Product Management reviews all open bugs quarterly
P4: VP Product Management reviews all enhancement requests quarterly
*Splunk Light: Manager: monthly reviews / Director or VP: quarterly reviews

Email Status Updates for Open Cases, by case priority
P1: Daily
P2: Weekly
P3: None
P4: None
*Splunk Light: 5 business days

Authorized Support Contacts
Support will be provided solely to the individual(s) authorized by the Customer to receive such support from Splunk ("Support Contacts"). Splunk strongly recommends that Support Contact(s) be trained on the applicable Splunk Cloud Service(s). The Customer's Order Document(s) will indicate a maximum number of authorized Support Contacts for the Customer's license level. The Customer will be asked to designate Support Contacts, including email address and Splunk.com login ID, following Splunk's acknowledgment of the Customer's Order Document(s).

Support Hours
Support is provided via telephone, email and web portal. Support will be delivered by a member of Splunk's technical support team during the regional hours of operation listed below.
P1: 24 x 7
P2: Monday through Friday during standard business hours (8 am to 5 pm Pacific); excluding Splunk holidays
P3: Monday through Friday during standard business hours (8 am to 5 pm Pacific); excluding Splunk holidays (*Splunk Light)
P4: Monday through Friday during standard business hours (8 am to 5 pm Pacific); excluding Splunk holidays

Customer's Obligation to Assist
Should a Customer report a purported defect in a Splunk Cloud Service, Splunk may require Customer's reasonable cooperation. The Customer's failure to provide the requested cooperation may prevent Splunk from identifying and fixing that purported defect.

EXHIBIT H
Splunk Cloud Data Policies

Below are policies related to the volume of data storage Customer purchases as of the Effective Date, as listed in the Order. The most current policies are available at http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DataPolicies and http://docs.splunk.com/Documentation/SplunkCloud/latest/User/Manageindexes.

Splunk Cloud administers your data according to the policies described below.

Notwithstanding anything in this Exhibit H, the "Splunk Cloud Data Processing Addendum" ("Cloud DPA") is attached hereto as Attachment 1. Anything in this Agreement or in this Exhibit H is deemed to be in addition to the Cloud DPA. In the event that anything in this Agreement or in this Exhibit conflicts with the Cloud DPA, the Cloud DPA shall govern the obligations of the parties regarding the processing of Personal Data.

Data retention

When you send data to Splunk Cloud, it is stored in **indexes**. Splunk Cloud retains data based on index settings that enable you to specify when data is to be deleted or moved to self storage. To configure different data retention settings for different sources of data, store the data in separate indexes according to the desired retention policy.

By default, data is retained for a maximum of 90 days. If you want to retain data for more than 90 days, contact Splunk Sales to purchase additional storage.

Each index uses two settings to determine when to delete or move your data:

- The maximum size of the index (specified in the **Max data size (GB)** field on the Indexes page)
- The maximum age of events in the index (specified in the **Retention (days)** field on the Indexes page)

When the index reaches the specified maximum size or events reach the specified maximum age, the oldest data is deleted or moved to self storage.

For example, suppose the maximum size of the index is set to 100 GB, and the maximum age of events in the index is set to 15 days. If you send 100 GB every day, then data will never be more than one day old, because every day the index reaches its maximum size and the oldest data is deleted or moved. However, if you send only 1 GB every day, the index never reaches its maximum size, so deletion is controlled by the maximum age. Data is never more than 15 days old and the size of the index remains around 15 GB.

Index data is stored in directories called **buckets**. Data is deleted by deleting entire buckets, not individual events. Buckets have their own settings that limit their size and the age of events in them. A bucket is not deleted until every event in the bucket meets the deletion settings for the index. If you use data self storage, the bucket is not deleted until the data is successfully moved to your self storage location.

For example, suppose the maximum size of the index is set to 10 GB and the maximum age of events in the bucket is set to 15 days. If you send 1 GB every day to that bucket, then on day 10 the bucket reaches its size limit, and only then are the index settings for deletion respected. If the maximum size of the index is set to 1 GB, the bucket still grows to 10 GB, at which point the bucket is closed and the index retention settings are applied. Because the index exceeds its limit of 1 GB, the 10 GB bucket is deleted.

Because of this logic, you cannot guarantee that data is deleted on a precise schedule by default. If you require data to be deleted on a precise schedule, contact Splunk Technical Support to discuss the options.

To modify your data retention policy, work with Splunk Technical Support to request modifications to the `maxTotalDataSizeMB` and `frozenTimePeriodInSecs` attributes.

Backup policy

Splunk Cloud maintains a seven-day backup of data and configuration files. Backups run continuously.

Manage Splunk Cloud indexes

Indexes store the data you have sent to your Splunk Cloud deployment. To manage indexes, Splunk Cloud administrators can perform these tasks:

- Create, update, delete, and view properties of indexes.
- Monitor the size of data in the indexes to remain within the limits of a data plan or to identify a need to increase the data plan.
- Modify data retention settings for individual indexes.
- Delete data from indexes.
- Optimize search performance by managing the number of indexes and the data sources that are stored in specific indexes.
- Delete indexes. **Caution:** This function deletes all data from an index and removes the index. The operation is final and cannot be reversed.
- Move expired data from indexes to self storage or a Splunk archive (Dynamic Data Active Archive). Data from the index is not deleted until it is successfully moved to the storage location. Archived data can be restored to Splunk Cloud for searching. Data from a self storage location can no longer be searched from Splunk Cloud. However, it can be restored to a Splunk Enterprise instance for searching if necessary.

Best practices for creating indexes

Consider these best practices when creating indexes:

- Create separate indexes for long-term and short-term data. For example, you might need to keep security logs for one year but web access logs for only one month. Using separate indexes, you can set different data retention times for each type of data.
- Apply logical or role-based boundaries for indexes. For example, create separate indexes for different departments.
- Devise a naming convention to easily track, navigate, and organize indexes.
- To configure your data retention settings, see the best practice listed here: Manage Data Retention Settings.

The Indexes page

To view the **Indexes** page, select **Settings**>**Indexes**. The **Indexes** page lists the indexes in a Splunk Cloud deployment and allows administrators to create, update, delete, and modify the properties of indexes. To modify settings for an index, click its name.

From this page you can:

- Create an index.
- View index details such as the following.
  - **Index name**: The name specified when the index was created.
  - **Current size (GB)**: The approximate amount of data currently stored in the index.
  - **Max size (GB)**: The maximum amount of raw data (in TB, GB, or MB) retained in the index.
  - **Event count**: The number of events in the index.
  - **Earliest event**: The earliest event found in the index.
  - **Latest event**: The most recent event found in the index.
  - **Searchable Retention (Days)**: The maximum age of events retained in the index.
  - **Status:** Enabled or disabled. Data in a disabled index is ignored in searches.
  - **Storage Type**: The storage settings for expired data from a given index. Can be self storage, archive, or no additional storage.
  - Delete an index. **Caution:** Deletes all data from an index and removes the index. The operation is final and cannot be reversed.

Create a Splunk Cloud index

Splunk Cloud administrators create indexes to organize data, apply role-based access permissions to indexes that contain relevant user data, fine-tune data, specify how long to retain data in indexes, and so on.

1. Select **Settings** > **Indexes**.
2. Click **New.**
3. In the **Index Name** field, specify a unique name for the index. Names must begin with a lowercase letter or a number and can include uppercase letters, hyphens, and underscores.
4. In the **Max data size** field, specify the maximum amount of data allowed before data is removed from the index.
5. In the **Retention (Days)** field, specify the number of days before an event is removed from an index.
6. In the **Dynamic Data Storage** field, select **Splunk Archive** to send data to the Splunk Dynamic Data Active Archive, or choose **Self Storage** to move expired data to your own self-storage area. If you don't want to maintain expired Splunk data, leave **No additional storage** selected.
7. If you enabled data self storage, select a location for data self storage. Or, click **Edit self storage locations** to add a new self storage location. For more information about data self storage and instructions for configuring a data self storage location, see Store expired Splunk Cloud data.
8. If you enabled Dynamic Data Active Archive, configure retention settings for the archive. For more information, see Archive expired Splunk Cloud data.
9. Click **Save**.

The index appears after you refresh the page. Retention settings are applied to individual indexes, and data retention policy settings apply to all of the data that is stored in your Splunk Cloud deployment. Monitor and verify that the data retention settings for all indexes does not meet or exceed the values set in the data retention policy. For more information, see Splunk Cloud data policies.

Manage data retention settings

Each index uses two settings to determine when to delete data:

- The maximum size of the index (GB) (specified in the **Max Size of Entire Index** field)
- The maximum age of events in the index (specified in the **Retention (days)** field)

When the index reaches the specified maximum size or events reach the specified maximum age, the oldest data is deleted or is moved to an archive or self-storage location (depending on your configuration).

For example, you ingest data from a particular data source at a rate of 10 GB per day, and you want to retain and search against the last 90 days worth of data. Given your search and data retention requirements, you should set the values so that the **Retention (days**) value is reached before the **Max Size of Entire Index** threshold is reached. Given the above parameters, you might configure the retention settings to the following.

- **Max Size of Entire Index** set to 1800 GB
- **Retention (days)** set to 90

These values together account for both your ingestion rate and the time you want to retain the data. You will need to consider these factors for each index that you create.

Finally, it's a good idea to check your data retention in the Cloud Monitoring Console to ensure you estimated your ingestion rate correctly and your storage consumption is within your entitlement. If you did not correctly estimate your ingestion rate, you might have a shorter retention period than expected. For more information, see Splunk Cloud data policies.

Splunk Cloud administrators can specify the settings that determine when data is removed from a specific index as follows.

For more information about data self storage and instructions for configuring a data self storage location, see Store expired Splunk Cloud data. For more information about archiving data, see Archive expired Splunk Cloud data. The new data retention settings appear after you refresh the page.

Disable a Splunk Cloud index

Splunk Cloud administrators can disable an index. The data in a disabled index is not queried during searches.

1. Select **Settings** > **Indexes**.
2. From the **Indexes** page, click **Disable** under the **Status** column.
3. Click **OK** to disable the index.

The index status changes to **Disabled** after you refresh the page. **Note:** You cannot disable default indexes and third-party indexes from the **Indexes** page.

Enable a Splunk Cloud index

Splunk Cloud administrators can enable an index. Data in an enabled index can be queried during searches.

1. Select **Settings** > **Indexes**.

2. Click **OK** to enable the index.

The index status changes to **Enabled** after you refresh the page.

Delete index data and the index from Splunk Cloud
Splunk Cloud administrators can delete an index.

Caution: This function deletes all data from an index and removes the index. The operation is final and cannot be reversed.

1. Select **Settings** > **Indexes**.
2. Identify the index and click **Delete** from the **Action** column.
3. Click **OK** to confirm that you want to delete the data and index from Splunk Cloud.

The data and index are deleted from Splunk Cloud and cannot be restored. **Note:** You cannot delete default indexes and third-party indexes from the **Indexes** page.

ATTACHMENT 1
Splunk Cloud Data Processing Addendum

THIS DATA PROCESSING ADDENDUM ("**DPA**") is made as of the Effective Date (defined below) BETWEEN

(1) Customer Systems Inc.-Corporate Headquarters whose principal place of business at 170 W. Tasman Dr., San Jose, CA ("**Customer**"); and

(2) **Splunk Inc.**, whose principal place of business is at 270 Brannan St., San Francisco, CA 94107 ("**Splunk**").

Each a "**Party**" and together, the "**Parties**."

This DPA is incorporated into and forms part of the Splunk Cloud Terms of Service between Splunk and Customer for the purchase of Splunk Services ("**Agreement**").

This DPA will become effective as of the date the Agreement ("**Effective Date**"). This DPA will be deemed legally binding upon receipt by Splunk of a fully executed copy and supersedes any prior agreements between Customer and Splunk concerning the processing of Personal Data.

HOW THIS DPA APPLIES

In the event of any conflict or inconsistency between the Agreement and this DPA, the latter shall prevail, but only to the extent of the conflict or inconsistency. Any terms which are not defined in this DPA are as defined in the Agreement.

Subject to the terms of the Agreement, the below terms and conditions apply to the processing of Personal Data.

1. PROCESSING OF PERSONAL DATA

1.1 Roles and Responsibilities. Customer is the Data Controller and Splunk is the Data Processor. Customer grants a general authorization to: (a) Splunk to appoint any Splunk Affiliate as a subprocessor; and (b) Splunk and any Splunk Affiliate to appoint third-party sub-processors to support the performance of the Services as provided below.

1.2 Splunk Processing Activities. Splunk agrees that it will: (a) only process Personal Data to provide the Services in accordance with the Agreement and pursuant to Customer's written instructions as set forth in this DPA; and (b) take reasonable steps to ensure that only authorized personnel who are under written obligations of confidentiality have access to such Personal Data. Splunk further agrees that it will comply with the Data Protection Law applicable to Splunk in the provision of Services under the Agreement and this DPA.

1.3 Customer Processing Activities. Customer may in its use of the Services submit Personal Data to Splunk. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer or any relevant third-party acquired Personal Data. Unless specifically identified in an Order, Customer agrees to not transmit or store within the Services any prohibited Personal Data as set forth in the Agreement.

1.4 Details of Processing Activities. The nature and extent of Personal Data processed by Splunk to deliver the Services is determined and controlled solely by Customer. Appendix A sets out the duration, nature and purpose of the processing of Personal Data. The categories of Data and Data Subjects whose Personal Data that may be processed by Splunk are also set forth in Appendix A.

2. SUB-PROCESSING

2.1 Current Sub-processors. A list of sub-processors current through the Effective Date is attached hereto at Appendix B, and Splunk also makes available its then current list of sub-processors through a link on its website Privacy Policy.

2.2 Right to Object to New Sub-processors. If Customer has a reasonable objection to any new sub-processor, it shall notify Splunk of such objection in writing. Within thirty (30) days after receipt of such notification by Splunk, the parties will seek to resolve the matter in good faith. If Splunk is able to provide the Services to Customer in accordance with the Agreement without using the sub-processor and decides in its discretion to do so, then Customer will have no further rights under this Section 2.2 with regard to the proposed use of the subprocessor. If Splunk requires use of the sub-processor and is unable to satisfy Customer as to: (a) the suitability of the sub-processor or (b) the documentation and protections in place between Splunk and the sub-processor, within sixty (60) days from the date of Customer's written objection, Customer may terminate the Agreement only with respect to the Services to which the proposed new sub-processor's processing relates or would relate by providing written notice to Splunk. Termination will be effective thirty (30) days after receipt by Splunk. Customer agrees to pay all fees as required under the Agreement incurred up to and including the date of termination.

2.3 Obligations of and Liability for Sub-processors. Splunk will take steps to require that any subprocessor it engages to provide Splunk Cloud Services on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on Splunk in this DPA. Splunk agrees to be liable for the acts or omissions of its third-party sub-processors to the same extent as Splunk would be liable if performing the services of the sub-processors under the terms of the Agreement.

3. SUBJECT ACCESS REQUESTS

In the event Splunk receives a Data Subject Request from Customer's Data Subject, Splunk will not respond to such Data Subject Request without Customer's prior written consent except to confirm that such request relates to Customer to which Customer hereby agrees. To the extent Customer does not have the ability to address a Data Subject Request using the functionalities available to Customer within the Splunk Cloud Service, Splunk will upon Customer's request provide reasonable assistance to facilitate a Data Subject Request to the extent Splunk is able to consistent with applicable law and provided Customer pays Splunk's charges for providing such assistance at Splunk's then-current professional services rates.

4. ASSISTANCE

Splunk will provide reasonable assistance to Customer as Customer reasonably requests (taking into account the nature of processing and the information available to Splunk) in relation to Customer's obligations under Data Protection Law with respect to: (a) data protection impact assessments (as such term is defined in the GDPR); and (b) Customer's compliance with its obligations under the GDPR with respect to the security of processing.

5. DELETION OR REMOVAL OF PERSONAL DATA

Upon termination of the Service, Customer may at its sole option and expense, delete or remove Customer data, including any Personal Data contained therein, from the Splunk Cloud environment as provided in the Agreement.

6. INSPECTIONS AND AUDIT

6.1 Splunk will make available to Customer such information in its possession or control as Customer may reasonably request to demonstrate Splunk's compliance with its obligations as a Data Processor under Data Protection Law. Requests for assistance from Splunk under this Section 6 (Inspections and Audits) or Section 3 (Subject Access Requests) above should be made to: Sec-Compliance@splunk.com or such other location as Splunk may make available on its website from time to time.

6.2 Customer may exercise its right of inspection and audit under Data Protection Law, through Splunk providing: (a) a certificate not older than 18 months by a registered and independent external auditor demonstrating that Splunk's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard such as ISO 27001 or SOC 2 Type (II); and (b) additional information in Splunk's possession or control to an EU supervisory authority when it requests or requires additional information with regard to the data processing activities carried out by Splunk under this DPA.

6.3 In the event that Customer is entitled under Data Protection Laws to request additional information pursuant to 6.2(b) above, such further information (including any on-site inspections) will be provided and/or conducted at Splunk's then-current professional services rates, taking into account the amount of resources and time required. Customer and Splunk will mutually agree upon the scope, timing and duration of any on-site inspection, including with respect to any third-party inspector selected by the Customer. Customer will promptly notify Splunk of any non-conformance discovered during the course of an on-site audit.

7. TECHNICAL AND ORGANIZATIONAL MEASURES

Splunk provides the technical and organizational measures required under applicable Data Protection Law for the security of the Personal Data it processes as set forth the Agreement.

8. INTERNATIONAL DATA TRANSFERS

Splunk is certified under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and is committed to the Privacy Shield Principles, including with respect to onward transfer. Customer acknowledges that Splunk will process Personal Data outside the EEA (and the U.K.) including in the United States.

9. PERSONAL DATA BREACH

9.1 Personal Data Breach Notification. Splunk will notify Customer without undue delay after becoming aware of a Personal Data Breach. Where appropriate in respect of any Personal Data which has been the subject of a Personal Data Breach, Splunk will provide reasonable assistance to Customer to the extent required for Customer to comply with GDPR, which may include assistance in notifying the relevant supervisory authority, and a description of the Personal Data Breach, if customer determines such notification is needed under GDPR.

9.2 Customer Notification to Splunk. If Customer determines that a Personal Data Breach must be notified to any supervisory authority and/or data subjects and/or the public or portions of the public pursuant to the GDPR, Customer will notify Splunk before the communication is made and supply Splunk with copies of any written documentation to be filed with the supervisory authority and of any notifications Customer proposes to make (whether to any supervisory authority, data subjects, the public or portions of the public) which reference Splunk, its security measures and/or role in the Personal Data Breach, whether or not by name. Subject to customer's compliance with any mandatory notification deadlines under the GDPR, Customer will consult with Splunk in good faith and take account of any clarifications or corrections Splunk reasonably requests to such notifications and which are consistent with the GDPR and applicable guidance under GDPR.

10. GENERAL

10.1 Splunk will inform Customer, as soon as reasonably practicable upon becoming aware, if in Splunk's opinion any instructions provided by Customer under this DPA infringe the GDPR.

10.2 Splunk's liability to Customer arising out of or related to the DPA will be subject to the same limitations and exclusion of liability as apply under the Agreement.

10.3 The Parties agree that Splunk will be a Data Controller of: (a) Customer business contact information that is Personal Data required to administer the Services; and (b) any personal data contained within Service Data as described in the Agreement, and terms of the DPA relating to the obligations of a Data Processor will not apply. Customer is responsible for ensuring its employees’ and authorized third-parties’ compliance with these terms.

11. DEFINITIONS

"Data Controller" as defined under the GDPR;

"**Data Processor**" as defined under the GDPR;

"**Data Protection Law**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom, applicable to the processing of Personal Data under this Agreement, including 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)("**GDPR**") and all national legislation implementing or supplementing the foregoing as updated, amended or replaced from time to time;

"Data Subject" as defined under the GDPR;

"Data Subject Request" means a request from or on behalf of a Data Subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or an objection from or on behalf of a Data Subject to the processing of its Personal Data;

"**Personal Data**" means all data which is defined as 'personal data' under Data Protection Law and which is provided by a Customer to Splunk (directly or indirectly), and accessed, stored or otherwise processed by Splunk as a Data Processor as part of its provision of the Service to a Customer and to which Data Protection Law applies from time to time; and

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthoried disclosure of, or access to, Personal Data while being transmitted, stored or otherwise processed by Splunk.

The Parties' authorized signatories have duly executed this DPA:

CUSTOMER		**SPLUNK INC.**	
By:	DocuSigned by: Cathy Hilling BCD941D0892246E	By:	DocuSigned by: Tim Emanuelson 1B08ABB9F5E6465...
Name:	Cathy Hilling Full Name	Name:	**Tim Emanuelson**
Title:	Contract Negotiator	Title:	**VP, Worldwide Corporate Controller**

APPENDIX A

DATA SUBJECTS

Customer may submit Personal Data to the Splunk Service, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners, vendors and their respective employees or contractors (who are natural persons)
- Customers' assigned users of the Splunk software and services
- Customers' employees, agents, contractors or advisors (who are natural persons)

CATEGORIES OF DATA

Customer may submit Personal Data to the Splunk Service, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Business contact information (e.g., company email, phone, physical business address)
- Personal contact information (e.g., email, mobile phone, address)
- ID data
- Connection data
- Location data

SUBJECT-MATTER

Customer determines the subject-matter of the processing and Splunk processes Personal Data as required to deliver the Services.

DURATION

Personal Data will be processed for the duration of the Services as determined by the Customer and as required by Splunk to administer the Services to the Customer.

NATURE AND PURPOSE

Customer determines the nature and purpose of the processing and Splunk handles Personal Data as required to deliver the Services.

APPENDIX B

Entity	Type of Service	Location
Amazon Web Services, Inc.	Infrastructure-as-a-Service	U.S. (East & West Coast) EU (Ireland and Germany)
Blue Ocean Contact Centers Inc.	Support	Canada
Salesforce.com, Inc.	Enterprise Services	U.S.
Spencer Rose Limited	Staffing Services and Support	U.K.
P.S. Computer Services Ltd.	IT Staffing Services	U.K.
iOPEX Technologies, Inc.	Technical Support Services	U.S. India
The Kinney Group	IT Infrastructure and Data Center Solution Services	U.S.
TEKsystems, Inc.	Technical Support	U.S.
Crest Data Systems, Inc. and Private LTD	Technical Support	U.S. India
Gary D. Nelson Associates, Inc.	Staffing Services	U.S.
Praecipio Consulting	Support Services	U.S.