

Agreement and Rider to the Splunk General Terms

This rider (Rider) to the Splunk General Terms (Exhibit A) and Exhibits B through J (collectively, the "TOS") is between Splunk Inc. a Delaware Corporation (Licensor) and the State of Oregon, acting through its Department of Administrative Services, Procurement Services (DAS PS) on behalf of state agencies (Licensee or Customer). This Rider, together with all exhibits, constitutes the complete agreement between the parties (Agreement). Capitalized terms not defined in the Rider shall be as defined in the TOS.

Licensor and DAS PS agree:

- 1. Applicability and Authority.** This Agreement pertains to the purchase of licenses and subscriptions for Splunk's Offerings offered by Licensor to Licensees under various statewide purchase agreements, including related documentation and support to be provided as a service by Licensor to Licensee under this Agreement. Licensor shall deliver Hosted Services in accordance with this Agreement, including the TOS. For the purposes of this Agreement, the "Splunk Offerings" do not include Third-Party Extensions or Third Party Products (collectively, "Third Party Offerings") as referenced in SGT (as defined below) Section 15, and no Licensee under this Agreement has authority to purchase any Third Party Offerings unless the Third Party Offering is necessary for the operation of the Splunk Offering.
- 2. Complete Agreement; Order of Precedence.** This Agreement consists of: (i) this Rider; (ii) Splunk General Terms (hereinafter, the "SGT") (Exhibit A); (iii) Specific Terms for Splunk Offerings (Exhibit B); (iv) Splunk Cloud Platform Maintenance Policy (Exhibit C); (v) Splunk Privacy Policy (Exhibit D); (vi) Splunk Websites Terms and Conditions of Use (Exhibit E); (vii) Splunk Cookie Policy (Exhibit F); Splunk Cloud Platform Security Exhibit (Exhibit G); (viii) Splunk Cloud Service Level Schedule (Exhibit H); (ix) Splunk Support Policy (Exhibit I); and (x) Splunk Data Processing Addendum (Exhibit J) .

This Rider amends and supersedes any provision to the contrary in the TOS and any Purchase Order or other ordering instrument to be issued by a Licensee (collectively referred to as "Order"). This Agreement merges all prior and contemporaneous communications with respect to the matters described in this Agreement.

In the event of any conflict between and of the above documents and an Order, the conflict will be resolved in following order:

- 1) the Rider
- 2) the TOS pursuant to its order of precedence (including updates to any policy referenced in the TOS or updates or revisions to Exhibits B-I; Splunk may update or modify Exhibits B-I, by posting an updated version at the hyperlink provided in the SGT, provided Splunk gives Licensee notice of any modification and the modification(s), if any, are consistent with SGT Section 24),
- 3) the executed Order,
- 4) any insurance requirements required by Licensee in the Order
- 5) any terms and conditions published by Licensor on or after the Effective Date of this Agreement, and

6) any terms presented to an end user in a 'click wrap' or similar end user agreement.

- 3. Effective Date and Term.** This Agreement is effective when it is fully executed and approved according to applicable laws, rules and regulations (Effective Date). This Agreement continues in effect unless terminated by either party by providing notice in the manner specified in the TOS or specified in this Rider. There is no automatic renewal for this Agreement or any Order for the services. Subject to mutual written agreement, Licensee may renew its subscription for an agreed upon term as of the anniversary date set forth in the Order.
- 3.1 Licensor may terminate or suspend the Hosted Services but may not suspend Licensee's access to Customer Content held as part of the Hosted Services if Licensee fails to pay an undisputed past-due invoice for a renewal term within 30 calendar days of Licensee's receipt of written notice from Licensor of such failure.
- 3.2 If Licensee wishes to reinstate the Hosted Services, Licensee will pay the fee(s) due for the current term at then-current prices available to similar-sized government clients in good standing. Licensee will not pay a penalty, or be obligated to pay for additional subscription terms.
- 4. Purchase and Payment.** Licensee is acquiring these products and issuing Order(s) pursuant to the provisions in the statewide price agreement referenced on the Order. Licensee's obligation to pay is set forth in the Order. All payments, if any, to Licensor are subject to ORS 293.462 and the limitations of the Statewide Travel Policy, currently found online at: <http://www.oregon.gov/das/Financial/Acctng/Documents/40.10.00.pdf>. Nothing in this paragraph shall alter Section 2(A) – Authorized Resellers and Digital Marketplaces of the SGT regarding indirect purchases of Splunk Offerings, except that Licensor's rights relative to payment remain subject to ORS 293.462 and the Statewide Travel Policy.
- 5. Confidentiality of Licensor Information.** Any obligation of Licensee to maintain the confidentiality of Licensor's proprietary information provided to Licensee is conditioned by and subject to Licensee's obligations under the Oregon Public Records Law, ORS 192.311 to 192.478 which may require disclosure of proprietary information as a "public record" unless exempt under ORS 192.345 or ORS 192.355.
- 6. Confidentiality Generally.** Licensor acknowledges that, it and its employees, subcontractors or agents in the course of this Agreement may be exposed to or acquire information that is confidential to Licensee or Licensee's clients. Customer Content is confidential information. Licensor shall maintain the confidentiality of Licensee's confidential information. The following information is not subject to the non-disclosure obligations of this agreement:
- Information that becomes part of the public domain through lawful means and without breach of any confidentiality obligation by Licensor;
 - Information subsequently and rightfully received from third parties who have the necessary rights to transfer the information without any obligation of confidentiality;

- Information that was known to Licensor prior to the Effective Date of the Agreement without obligation of confidentiality;
- Information that is independently developed by Licensor and documented in writing without use of, or reference to, any confidential information of Licensee; and
- Subject to Licensor's obligation to provide notice under Section 7, Notifications, information required to be disclosed by compulsory judicial or administrative process or by law or regulation.

6.1 Privacy and Security Training. Licensor shall ensure its employees, agents, and contractors receive periodic training on privacy and security obligations relating to this Agreement.

6.2 Limited Purposes. Licensor shall limit the use or disclosure of Customer Content to persons directly connected with the administration of this Agreement.

6.3 No Overseas Storage. Customer Content will not be stored outside of the United States or its territories. Licensee must select a cloud region in the United States or its territories for provisioning the Hosted Service, and Licensor shall not change this region unless directed by Licensee in writing to do so.

6.4 Prohibition on Data Mining. Licensor shall not capture, maintain, scan, index, share or use Customer Content, or otherwise use any data-mining technology, for any non-authorized activity, and shall not permit its agents or subcontractors to do so. For purposes of this requirement, "non-authorized activity" means data mining or processing of data, stored or transmitted by the service, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security analysis that is not explicitly authorized in this Agreement (including, but not limited to, Section 11 - Usage Data of the SGT).

6.5 Privacy Protections. The information exchanged between the parties may include Customer Content subject to specific confidentiality protections under state or federal law, and the implementing regulations of those laws. Licensor, its employees, agents, and contractors shall comply with laws and regulations applicable to the information, including as those laws and regulations may be updated from time to time. Licensor shall maintain protections required by law or this Agreement for any retained Customer Content for so long as Licensor (including through any third party) retains Customer Content. Licensee hereby represents and warrants, under its own responsibility and to the best of its knowledge, that no personal data subject to the European General Data Protection Regulation (EU/2016/679) or other data protection laws that identify Licensor as a Processor on behalf of Licensee under this Agreement. Licensee shall communicate to Licensor in writing, without undue delay, any anticipated change affecting Licensee's representation and warranty in Section above. The parties then will in good faith negotiate the provisions of a data processing agreement, to amend this Agreement, as is reasonably required (1) to reflect their obligations and risks under the GDPR and other applicable privacy laws (2) for Licensor

to provide the Services in a manner that allows Licensee and Licensor to comply with their respective obligations under such privacy laws prior to the change affecting Licensee's representation and warranty above.

6.6 Access. Licensor shall not suspend Licensee's access to Customer Content at any time during the term of this Agreement or the post-termination access period set forth in SGT Section 4(E).

6.7 Transition Services. Licensor shall, as described in SGT Section 4(E) at Licensee's option provide transition services to support a responsible and secure transition of Hosted Services and Customer Content to another service provider or to Licensee.

6.8 Sanitization. Subject to the Records Retention set forth below, Licensor shall not retain any copies of Customer Content following the post-termination access period referenced in SGT Section 4. Licensor shall not destroy Customer Content without Licensee's written authorization. Licensor shall notify Licensee of any conditions that make returning all Customer Content not feasible. Upon Licensee's written acknowledgement that returning all Customer Content is not feasible and consent, Licensor shall purge or destroy retained Customer Content ingested into the Hosted Service in all its forms (including copies of returned data) in accordance with the most current version of NIST SP 800-88 and provide Licensee with written certification of sanitization.

7. Public Records Requests and Requests for Data.

7.1 Response to Public Records Request for Agency Data. Licensee, as an executive department agency of the State of Oregon, must respond to requests for Customer Content and other public records under Oregon's Public Records laws, including ORS 192.311 to 192.478, within set timeframes. Licensor shall, in accordance with Section 4(E) of the SGT, support the ability of Licensee to respond to public records requests for Customer Content in accordance with applicable law.

7.2 Other Requests for Licensee Data. In the event Licensor receives a third party request for Customer Content, including any electronic discovery, litigation hold, or discovery searches, Licensor shall (to the extent legally permitted) first give Licensee notice and provide such information as may reasonably be necessary to enable Licensee to take action to protect its interests.

8. Security and Compliance with Laws, Regulations, and Policies. Licensor shall comply with all applicable state and federal laws and regulations, governing use and disclosure of Customer Content and access to State of Oregon information assets, as adopted or modified from time to time, including the Oregon Consumer Information Protection Act (OCIPA), ORS 646A.600 through 646A.628. For purposes of OCIPA, Licensor is a vendor.

8.1. Privacy and Security Measures. Licensor represents and warrants it has established and will maintain privacy and security measures that meet or exceed the standards set in laws, rules,

and regulations applicable to the safeguarding, security, and privacy of Customer Content. Licensor shall monitor, periodically assess, and update its physical, technical, and logical security controls and risk to ensure continued effectiveness of those controls.

8.2. Security Risk Management Plan. Licensor shall ensure the level of security and privacy protection required by this Agreement or for the Hosted Services is documented in a security risk management plan.

8.3. Reserved.

8.4. Security Logs and Reports. Licensee can review activity logs within Splunk Cloud Platform to view access to its Splunk Cloud Platform Hosted Services environment. Licensee can control the retention period of such activity logs per the Documentation and functionality of the Splunk Cloud Platform Hosted Service.

8.5. Licensee Audit Rights and Access. Licensor shall maintain records in such a manner as to clearly document its compliance with and performance under this Agreement, and provide Licensee, the Oregon Secretary of State, the federal government, and their duly authorized representatives access to:

- Determine Licensor's compliance with this Agreement, or
- documentation, information and data sufficient to show Splunk's compliance with regulatory and contractual requirements applicable to Splunk providing the Purchased Offerings to Customer, subject to the terms of Splunk's fee-based audit program.
- **Notice.** Except as stated below for security logs, access to facilities, systems, and records under this section will be granted following reasonable notice to Licensor, provided all information furnished to Licensee under this Section 8.6 does not require Licensor to provide technically sensitive, confidential or proprietary information. Records include paper or electronic form, and related system components and tools (including hardware and software), required to perform examinations and audits, and to make excerpts and transcripts, including for data forensics.

8.6. Record Retention. Licensor shall retain and keep accessible all records, with the exception of EFT authorizations, records inventories, general correspondence, cardholder data, IT status reports, market research, surveys, shipping & receiving documents, vendor lists, vendor quotes, and support tickets, for a minimum of three years, or such longer period as may be required by applicable law, following termination of the Order or this Agreement, or until conclusion of any litigation arising out of or related to any Order or this Agreement, whichever data is later.

9. Licensor Access and Audit rights. Licensor may audit Licensee's use of the Hosted Services, provided:

- 9.1. Any onsite audit will take place no more than once every 12 months, upon not fewer than 30 calendar days' written notice, during normal business hours and in a manner that does not interfere unreasonably with Licensee's operations. Licensee will provide Licensor or the independent auditor with information reasonably requested in furtherance of the verification; however, Licensor has no right of access to any locations, servers, computers, records, data, accounts, or other information protected by law from disclosure. As an alternative, Licensor can request Licensee complete a self-audit questionnaire.
- 9.2. If an agreed-upon compliance or audit report reveals that Licensee does not have sufficient subscriptions to meet its actual use, Licensee will order sufficient subscriptions at Licensee's standard list price then in effect. Licensee will not pay a penalty. Licensee may at its option purchase additional Hosted Services or subscriptions.
- 9.3. Each party will bear its own costs of any audit or compliance verification activity conducted pursuant to the TOS.

10. Licensee Liabilities and Indemnification. Licensee's liabilities under this Agreement and any Order and any Licensee obligation under the TOS or an Order to indemnify or hold Licensor harmless against claims brought by third parties against Licensor, including any payment of attorneys' fees, are subject to the limitations of Article XI, Section 7 of the Oregon Constitution and the Oregon Tort Claims Act, ORS 30.260 through 30.300. Licensee has no obligation to defend Licensor.

11. Insurance. In its Order, Licensee may request that Licensor obtain and maintain various insurance coverages.

12. Defense of Claims. To the extent Licensor is required under this Agreement to defend Licensee against claims asserted by third parties, including under Section 23 of Exhibit A, Licensee shall reasonably cooperate in good faith, at Licensor's reasonable expense, in the defense of the claim, Licensor shall select counsel reasonably acceptable to the Oregon Attorney General to defend the claim, and Licensor shall bear all costs of counsel. The Oregon Attorney General's acceptance of counsel may not be unreasonably withheld. Counsel must accept appointment as a Special Assistant Attorney General under ORS Chapter 180 before counsel may act in the name of, or represent the interests of, the State of Oregon, Licensee, its officers, employees or agents. Licensee may elect to assume its own defense with an attorney of its own choice and at its own expense any time Licensee determines important governmental interests are at stake. Licensee will promptly provide notice to Licensor of any claim that may result in an obligation on the part of Licensor to defend. Subject to these limitations, Licensor may defend a claim with counsel of its own choosing, on the condition that no settlement or compromise of any claim may occur without the consent of Licensee, which consent must not be unreasonably withheld.

13. Governing Law; Jurisdiction; Venue. This Agreement is governed by, construed, and enforced in accordance with the laws of the State of Oregon, without giving effect to its conflict of law principles, and applicable federal law. Any action or suit brought by the parties relating to this Agreement must be brought and conducted exclusively in the Circuit Court of Marion County for the State of Oregon in Salem, Oregon; provided, however, if a claim must be brought in a federal forum, then it must be brought and conducted solely and exclusively within the United States District Court for the District of Oregon. LICENSOR HEREBY CONSENTS TO THE PERSONAL

JURISDICTION OF THESE COURTS, WAIVES ANY OBJECTION TO VENUE IN THESE COURTS, AND WAIVES ANY CLAIM THAT THESE COURTS ARE INCONVENIENT FORUMS. In no way may this section or any other term of this Agreement be construed as (i) a waiver by the State of Oregon of any form of defense or immunity, whether it is sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States, or otherwise, or (ii) consent by the State of Oregon to the jurisdiction of any court.

- 14. Attorneys' Fees.** Neither party to this Agreement is entitled to obtain judgment from the other party for attorneys' fees incurred in any litigation between the parties. Except as allowable under the indemnification provisions in this Agreement.
- 15. Dispute Resolution.** Any dispute between the parties under this Agreement that is not resolved through informal discussions may be submitted to mediation upon the consent of both parties. If informal discussions or mediation are unsuccessful, either party may initiate litigation to resolve the dispute. The parties specifically disclaim any right to arbitration of disputes. Neither party waives its right to a jury trial or right to participate in class, collective, or representative claims.
- 16. Incorporation of Oregon Statutes.** ORS 279B.220, 279B.230 and 279B.235 are incorporated into this Agreement by reference to the extent applicable to Licensor's performance under this Agreement.

17. Termination.

17.1. **Additional Licensee's Rights to Terminate.** In addition to the termination rights set forth in SGT 21(B), Licensee may terminate an Order upon the following:

17.1.1. **Termination for Lack of Funding.** Nothing in this Agreement may be construed to permit any violation of Article XI, Section 7 of the Oregon Constitution or any other law regulating liabilities or monetary obligations of the State of Oregon. Licensee's payment for fees due after the last calendar day of the current State of Oregon biennium is contingent upon Licensee receiving funding, appropriations, limitations, allotments or other expenditure authority from the Oregon Legislative Assembly (including its Emergency Board) sufficient to allow Licensee, in the exercise of its reasonable administrative discretion, to continue to compensate Licensor. Licensee may immediately terminate this Agreement upon written notice if Licensee fails to receive funding, appropriations, limitations, allotments, or other expenditure authority as contemplated by Licensee's budget or spending plan and Licensee determines, in its assessment and ranking of the policy objectives explicit or implicit in its budget or spending plan, that it is necessary to terminate this Agreement.

17.1.2. **Licensee's Right to Terminate for No Cause.** Licensee may terminate this Agreement upon at least 30 calendar days' prior written notice to Licensor.

17.1.3. **Licensee's Right to Terminate for Services Issues.** In addition to the remedies set forth in the Service Level Schedule for the Splunk Cloud Platform Hosted Service, if Licensor fails to achieve at least 98% availability for such Splunk Cloud Platform Hosted Service for two (2) consecutive quarters, Licensee may terminate the applicable Order and Licensee will receive a pro rata refund of any unused prepaid subscription fees.

Licensee acknowledges and agrees that the foregoing pro-rata refund and any applicable service level credits set forth in the Service Level Schedule are its sole and exclusive remedy for Licensor's failure to meet an applicable service level set forth in such Service Level Schedule.

17.2. **Mutual Termination.** The parties may agree to terminate this Agreement upon at least 30 calendar days' prior written agreement.

17.3. **Effect of Termination.** The effect of a termination under this Section 17 shall be in accordance with Section 21 – Term and Termination – of the SGT.

18. Independent Contractor. Licensor is at all times an independent contractor and is not an agent, employee, or representative of Licensee. Licensor has no right or authority to incur or create any obligation for or legally bind Licensee in any way. Licensor is not an "officer," "employee" or "agent" of Licensee or any other agency, office, or department of the State of Oregon, as those terms are used in ORS 30.265, and Licensor shall make no representations to third parties to the contrary. Neither party shall make any statements, representations, or commitments of any kind or to take any action binding on the other except as provided for in the Contract or authorized in writing by the party to be bound.

19. Publicity. Licensor may disclose the form and existence of this Agreement in advertising, press releases or other materials distributed to prospective customers, but shall not otherwise attempt to obtain publicity from its association with Licensee or the State of Oregon, whether or not such disclosure, publicity or association implies an endorsement by Licensee or the State of Oregon of Licensor's products and services, without the prior written consent of Licensee.

20. Counterparts. This Rider may be executed in two or more counterparts, by facsimile or otherwise, each of which is an original, and all of which together constitute one and the same instrument, notwithstanding that all parties are not signatories to the same counterpart.

21. Amendments. This Agreement may be amended, modified, or supplemented only by a written amendment that, if required by applicable law, has been approved according to applicable laws, rules and regulations. No amendment will be effective until all requisite signatures and approvals are obtained from both parties.

22. No Third Party Beneficiaries. DAS PS and Licensor are the only parties to this Agreement and are the only parties entitled to enforce its terms. Licensee is an intended beneficiary of this Agreement.

23. Subcontractors. Licensor shall disclose its subcontractors for Hosted Services under this Agreement or any Order at https://www.splunk.com/en_us/legal/sub-processors.html, and ensure all subcontractors providing services related to this Agreement or any Order comply with its applicable provisions.

24. Survival. The provisions of this Rider that by their nature survive termination do so survive.

25. Severability. The parties agree that if any term or provision of this Agreement is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and provisions will not be affected, and the rights and obligations of the parties

will be construed and enforced as if this Agreement did not contain the particular term or provision held to be invalid.

26. Non-Discrimination. If the anticipated total value of the Hosted Services to be provided under this Agreement is \$150,000 or more, Licensor certifies that it has a written policy and practice that meets the requirements described in ORS 279A.112 for preventing sexual harassment, sexual assault, and discrimination against employees who are members of a protected class. Licensor agrees, as a material condition, to maintain such policy and practice in force during the term of this Agreement.

27. Pay Equity. As required by ORS 279B.235, Licensor shall comply with ORS 652.220 and not unlawfully discriminate against any of its employees in the payment of wages or other compensation for work of comparable character on the basis of an employee's membership in a protected class. "Protected class" means a group of persons distinguished by race, color, religion, sex, sexual orientation, national origin, marital status, veteran status, disability, or age. Licensor's compliance with this section is a material term of this Agreement, and Licensor's failure to comply constitutes a breach entitling Licensee to terminate this Agreement for cause.

27.1. As required by ORS 279B.235, Licensor may not prohibit any of its employees from discussing the employee's rate of wage, salary, benefits, or other compensation with another employee or another person. Licensor shall not retaliate against an employee who discusses the employee's rate of wage, salary, benefits, or other compensation with another employee or another person.

28. NOTICES. Except as otherwise expressly provided in this Agreement, any communications between the parties or notices to be given under this Agreement must be given in writing to Licensor at the address or number set forth in Section 31, and to Licensee at the address or number set forth in Section 31, or to such other addresses or numbers as either party may hereafter indicate pursuant to this Agreement.

- Any communication or notice delivered by United States Postal Service, first class mail postage prepaid, will be deemed given five calendar days after mailing.
- Any communication or notice delivered by email will be deemed given when the recipient responds with a receipt, which may be auto-generated. To be effective against Licensee, such email transmission must be confirmed by telephone notice to the Licensee Authorized Representative (or delegate).
- Any communication or notice by personal delivery will be deemed given when actually received by the appropriate Authorized Representative (or delegate).

29. Tax Compliance. By executing this Rider, the undersigned certifies under penalty of perjury that, to the best of the individual's knowledge, Licensor has complied with the tax laws of the State of Oregon and the applicable tax laws of any political subdivision of this state, and that Licensor has no undisclosed liquidated and delinquent debt owed to this state or any political subdivision. Licensor shall, for the duration of this Agreement and any extensions, comply with all tax laws of this state and all applicable tax laws of any political subdivision of this state. For the purposes of this section, "tax laws" includes: (i) All tax laws of this state, including but not limited to axes


referenced in ORS 305.380(4), ORS 305.620 and ORS chapters 316, 317, and 318, ; (ii) Any tax provisions imposed by a political subdivision of this state that apply to Licensor, to Licensor's property, operations, receipts, or income, or to Licensor's performance of or compensation for any work performed by Licensor; (iii) Any tax provisions imposed by a political subdivision of this state that apply to Licensor, or to goods, services, or property, whether tangible or intangible, provided by Licensor; and (iv) Any rules, regulations, charter provisions, or ordinances that implemented or enforced any of the foregoing tax laws or provisions.

29.1. This Agreement will be reported to the Oregon Department of Revenue. The Department of Revenue may take any and all actions permitted by law relative to the collection of taxes and debt due to the State of Oregon or a political subdivision, including (i) garnishing Licensor's compensation under this Agreement, or (ii) exercising a right of setoff against Licensor's compensation relating to this Agreement for any amounts that may be due and unpaid to the State of Oregon or its political subdivisions for which the Department of Revenue collects debts.

30. LICENSOR, BY EXECUTION OF THIS AGREEMENT, HEREBY ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS.

Licensors:

Signature & Date

Signed by:

661D613647224C8...

07/31/2024

Printed Name and Title of

Timothy Allen

Authorized Representative

Director, Deal Strategy & Executio

Services Manager or Other Point of Contact:

Printed Name and Title

Sara Swangard, Regional Sales Manager

Mailing Address

250 Brannan Street, San Francisco, CA 94107

Physical Address

250 Brannan Street, San Francisco, CA 94107

Telephone

503/805-9006

Email

sswangard@splunk.com

State of Oregon acting by and through Department of Administrative Services

Signature & Date



08/20/2024

Printed Name and Title of

John Anglemier State Procurement Manager

Authorized Representative

DAS PS Point of Contact:

Printed Name and Title

Ashley Wenger, State Procurement Analyst

Mailing Address

1225 Ferry St SE, Salem, OR 97301

Physical Address

1225 Ferry St SE, Salem, OR 97301

Telephone

971-719-0322

Email

Ashley.V.Wenger@das.oregon.gov

APPROVED PURSUANT TO ORS291.047 BY THE DEPARTMENT OF JUSTICE:

By: Approved via email dated 7/31/24 by Karen Johnson
Senior Assistant Attorney General

**EXHIBIT A
Splunk General Terms**

These General Terms (“**General Terms**”) apply to the purchase of licenses and subscriptions for Splunk’s Offerings.

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

If you are a United States state or local government entity, including a public institute of higher education, see the **UNITED STATES STATE & LOCAL GOVERNMENT LAW EXHIBIT TO SPLUNK GENERAL TERMS** attached which *supersedes or modifies terms found elsewhere in the General Terms (including Sections 16, 22, 23, and 25)*.

Parties:

Splunk or “**we**” or “**us**” or “**our**”: Splunk Inc., a Delaware corporation, with its principal place of business at 250 Brannan Street, San Francisco, California 94107, U.S.A.; and

Customer or “**you**” or “**your**”: State of Oregon Department of Employment, with its principal place of business at 875 Union Street NE, Salem, OR, United States, 97311.

IN WITNESS WHEREOF, the parties have executed these Splunk General Terms by their duly authorized officers or representatives.

SPLUNK:

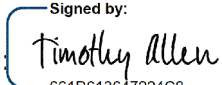
Signature:

Name:

Title:

Date:

State of Oregon Department of Employment:

Signed by:
Signature: 
661D613647224C8...

Name: Timothy Allen

Title: Director, Deal Strategy & Execution

Date: 07/31/2024

“**Effective Date**” means the date of the last signature above.

GENERAL TERMS

1. License Rights

- (A) **General Rights.** You have the nonexclusive, worldwide, nontransferable and nonsublicensable right, subject to payment of applicable Fees and compliance with the terms of these General Terms, to use your Purchased Offerings for your Internal Business Purposes during the Term and up to the Capacity purchased.
- (B) **Copies for On-Premises Products.** You have the right to make a reasonable number of copies of On-Premises Products for archival and back-up purposes.
- (C) **Splunk Extensions.** You may use Splunk Extensions solely in connection with the applicable Purchased Offering subject to the same terms and conditions for that Offering (including with respect to Term) and payment of any Fees associated with the Splunk Extensions. Some Splunk Extensions may be made available under license terms that provide broader rights than the license rights you have to the applicable underlying Offering (e.g., if the Extension is Open Source Software). These broader rights will apply to that Splunk Extension. Splunk Extensions may be installed on Hosted Services pursuant to our instructions.
- (D) **Trials, Evaluations, Beta and Free Licenses.**
- (i) **Trials and Evaluations.** Offerings provided for trials and evaluations are provided at no charge, and their use will be for a limited duration.
 - (ii) **Beta Licenses.** Some Offerings and features may be available to you as a preview, or as an alpha, beta or other pre-release version (each, a “**Beta Offering**”). All rights for Beta Offerings are solely for internal testing and evaluation. Your use of a Beta Offering will be for the term specified by us, and if no term is specified, then for the earlier of one year from the start date of the Beta Offering or when that version of the Beta Offering becomes generally available. We may discontinue the Beta Offering at any time and may decide not to make any of the features and functionality generally available.
 - (iii) **Free Licenses.** From time to time, we may make certain Offerings available for full use (i.e., not subject to limited evaluation purposes) at no charge. These free Offerings may have limited features, functions, and other technical limitations.
 - (iv) **Donated Offerings.** Donated Offerings are free limited Offerings donated to qualifying Nonprofits under a Splunk donation program. By procuring and making use of a Donated Offering, you hereby represent and warrant that you are a lawfully organized Nonprofit, and

you agree to provide verification of your nonprofit status to Splunk upon request. At Splunk's request, you agree: (a) to publish a press release and case study on your use of the Donated Offering; and (b) to be interviewed for the production of a Splunk customer video that will accompany the press release and case study. Splunk will draft and edit all content in collaboration with you and will obtain your edits and written approval (email is sufficient) prior to publication, and such approval will not be unreasonably withheld. You will allow Splunk to reference your Nonprofit and leading spokespeople in press releases with your written approval (email is sufficient). Splunk may use your name and logo on sales presentations, websites, and other marketing collateral without your prior approval.

- (E) **Test and Development Licenses.** For Offerings identified as “**Test and Development**” Offerings on your Order, you only have the right to use those Offerings up to the applicable Capacity on a non-production system for non-production uses, including product migration testing or pre-production staging, or testing new data sources, types, or use cases. Test and Development Offerings may not be used for any revenue generation, commercial activity, or other productive business or purpose.
- (F) **Limitations.** Notwithstanding anything to the contrary in these General Terms, we do not provide maintenance and support, warranties, service level commitments, or indemnification for Test and Development Offerings, trials, evaluations, or free or Beta Offerings.

2. Purchasing Through Authorized Resellers, Digital Marketplaces, and Splunk Affiliates

- (A) **Authorized Resellers and Digital Marketplaces.** If you purchase Offerings through a Splunk authorized reseller or Digital Marketplace, these General Terms will govern those Offerings. Your payment obligations for the Purchased Offerings will be with the authorized reseller or Digital Marketplace, as applicable, not Splunk. You will have no direct Fee payment obligations to Splunk for those Offerings. However, in the event that you fail to pay the Digital Marketplace for your Purchased Offerings, Splunk retains the right to enforce your payment obligations and collect directly from you.

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

- (B) **Splunk Affiliate Distributors.** Splunk has appointed certain Splunk Affiliates as its non-exclusive distributors of the Offerings (each, a “**Splunk Affiliate Distributor**”). Each Splunk Affiliate Distributor is authorized by Splunk to negotiate and enter into Orders with Customers. Where a purchase from Splunk is offered by a Splunk Affiliate Distributor, Customer will issue Orders, and

make payments, to the Splunk Affiliate Distributor which issued the quote for the Offering. Each Order will be deemed a separate contract between Customer and the relevant Splunk Affiliate Distributor and will be subject to these General Terms. For the avoidance of doubt, Customer agrees that: (i) the total liability of Splunk under these General Terms as set forth in Section 22 (Limitation of Liability) states the overall combined liability of Splunk and Splunk Affiliate Distributors; (ii) the entering into Orders by a Splunk Affiliate Distributor will not be deemed to expand Splunk and its Affiliates' overall responsibilities or liability under these General Terms; and (iii) Customer will have no right to recover more than once from the same event.

3. Your Contractors and Third-Party Providers

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

4. Hosted Services and Specific Offering Terms

- (A) **Service Levels.** When you purchase Hosted Services as a Purchased Offering, we will make the applicable Hosted Services available to you during the Term in accordance with these General Terms. The Service Level Schedules (as identified in the Specific Offering Terms referenced in Section 4(F) below) and associated remedies will apply to the availability and uptime of the applicable Hosted Service. If applicable, service credits will be available for downtime in accordance with the Service Level Schedule
- (B) **Connections.** You are responsible for obtaining and maintaining all telecommunications, broadband and computer equipment and services needed to access and use Hosted Services, and for paying all associated charges.
- (C) **Your Responsibility for Data Protection.** You are responsible for: (i) selecting from the security configurations and security options made available by Splunk in connection with a Hosted Service; (ii) taking additional measures outside of the Hosted Service to the extent the Hosted Service Offering does not provide the controls that may be required or desired by you; and (iii) routine archiving and backing up of Customer Content. You agree to notify Splunk promptly if you believe that an unauthorized third party may be using your accounts or if your account information is lost or stolen.

- (D) **Refund Upon Termination for Splunk's Breach.** If a Hosted Service is terminated by you for Splunk's uncured material breach in accordance with these General Terms, Splunk will refund you any prepaid subscription fees covering the remainder of the Term after the effective date of termination.
- (E) **Return of Customer Content.** Customer Content may be retrieved by you and removed from the Hosted Services in accordance with the applicable Documentation. We will make the Customer Content available on the Hosted Services for thirty (30) days after termination of a subscription for your retrieval. After that thirty (30) day period, we will have no obligation to maintain the storage of your Customer Content, and you hereby authorize us thereafter to, and we will, unless legally prohibited, delete all remaining Customer Content. If you require assistance in connection with migration of your Customer Content, depending on the nature of the request, we may require a mutually agreed upon fee for assistance.
- (F) **Specific Offering Terms.** Specific security controls and certifications, data policies, service descriptions, Service Level Schedules and other terms specific to a Hosted Service and other Offerings ("**Specific Offering Terms**") are set forth here: www.splunk.com/SpecificTerms, and will apply, and be deemed incorporated herein by reference.

5. Support and Maintenance

The specific Support Program included with a Purchased Offering will be identified in the applicable Order. Splunk will provide the purchased level of support and maintenance services in accordance with the terms of the Support Exhibit attached to these General Terms.

6. Configuration and Implementation Services

Splunk offers standard services to implement and configure your Purchased Offerings. These services are purchased under an Order and are subject to the payment of the Fees therein and the terms of the Configuration and Implementation Services Exhibit attached to these General Terms.

(A)

7. Data Protection for Personal Data

Splunk will follow globally recognized data protection principles and industry-leading standards for the security of personal data. Splunk will comply with the requirements and obligations set forth in Splunk's Data Processing Addendum ("**DPA**") , located at https://www.splunk.com/en_us/legal/splunk-dpa.html, which includes standard terms for the processing of personal data (including, as applicable, personal data in a Hosted Service) .

8. Security

- (A) **Security for Hosted Services: Standard Environment.** Splunk will implement industry leading security safeguards for the protection of Customer Confidential Information, including Customer Content transferred to and stored within the Hosted Services. These safeguards include commercially reasonable administrative, technical, and organizational measures to protect Customer Content against destruction, loss, alteration, unauthorized disclosure, or unauthorized access, including such things as information security policies and procedures, security awareness training, threat and vulnerability management, incident response and breach notification, and vendor risk management. Splunk's technical safeguards are further described in the Splunk Cloud Platform Security Addendum ("**SC-SA**"), located at https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html, and the Observability Suite Security Addendum ("**OS-SA**"), located at https://www.splunk.com/en_us/legal/splunk-observability-security-addendum.html, as applicable, and are incorporated herein by reference. Splunk may update the SC-SA and OS-SA from time to time provided, that updates will be subject to Section 24 below.
- (B) **Security for Hosted Services: Premium HIPAA Environment.** For Hosted Services Offerings provisioned in Splunk Cloud Platform's Premium HIPAA environment (as specified in an Order), in addition to the protections under the SC-SA and these General Terms, Splunk will comply with the requirements and obligations set forth in Splunk Business Associate Agreement found here: https://www.splunk.com/en_us/legal/splunk-baa.html.
- (C) **Additional Security for Other Hosted Services.** From time to time, Splunk may offer custom security safeguards for unique Hosted Services offerings. Any such security safeguards will be as set forth in the applicable Documentation and Specific Offering Terms.
- (D) **Security for On Premises Offerings.** Splunk will implement industry leading security safeguards for the protection of Splunk's IT systems, products, facilities and assets, and any Customer Confidential Information accessed or processed therein, e.g., customer account information, support tickets ("**Corporate Security Controls**"). Splunk's Corporate Security Controls include such things as information security policies and procedures, security awareness training, physical and environmental access controls, threat and vulnerability management, incident response and breach notification, and vendor risk management. Splunk's Corporate Security Controls are further described in Splunk's Information Security Addendum ("**ISA**"), located at https://www.splunk.com/en_us/legal/information-security-addendum.html and are incorporated herein by reference.
- (E) **Product Development Security.** Splunk will follow secure software development practices and applies an industry standard, risk-based approach to its software development lifecycle

("SDLC"), which includes, as applicable, such things as performing security architecture reviews, open source security scans, virus detection, dynamic application security testing, network vulnerability scans and external penetration testing in the development environment. Product-specific information about the SDLC in our Offerings is detailed more fully in the ISA. Splunk's Product Security Portal, located at https://www.splunk.com/en_us/product-security.html, contains detailed information about Splunk's program for managing and communicating product vulnerabilities. Splunk categorizes product vulnerabilities in accordance with the Common Vulnerability Scoring System ("Medium," "High," or "Critical") and uses commercially reasonable efforts to remediate vulnerabilities depending on their severity level in accordance with industry standards.

- (F) **Maintaining Protections.** Notwithstanding anything to contrary in these General Terms, or any policy or terms referenced herein via hyperlink (or any update thereto), Splunk may not, during a Term materially diminish the security protections set forth in these General Terms, any Specific Offering Terms, or the applicable security addendum.

9. Use Restrictions

Except as expressly permitted in an Order, these General Terms or our Documentation, you agree not to (nor allow any user or Third Party Provider to): (a) reverse engineer (except to the extent specifically permitted by statutory law), decompile, disassemble or otherwise attempt to discover source code or underlying structures, ideas or algorithms of any Offering; (b) modify, translate or create derivative works based on the Offerings; (c) use an Offering to ingest, monitor or analyze the machine, IT system or application data of any third party; (d) resell, transfer or distribute any Offering; (e) access or use any Offering in order to monitor its availability, performance, or functionality for competitive purposes; (f) attempt to disable or circumvent any license key or other technological mechanisms or measures intended to prevent, limit or control use or copying of, or access to, Offerings; (g) separately use any of the applicable features and functionalities of the Offerings with external applications or code not furnished by Splunk or any data not processed by the Offering; (h) exceed the Capacity purchased or (i) use any Offering in violation of all applicable laws and regulations (including but not limited to any applicable privacy and intellectual property laws).

10. Our Ethics, Compliance and Corporate Responsibility

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

- (B) **Anti-Corruption.** We implement and maintain programs for compliance with applicable anti-corruption and anti-bribery laws. Splunk policy prohibits the offering or soliciting of any illegal or improper bribe, kickback, payment, gift, or thing of value to or from any of your employees or agents in connection with these General Terms. If we learn of any violation of the above, we will use reasonable efforts to promptly notify you at the main contact address provided by you to Splunk.
- (C) **Export.** We certify that Splunk is not on any of the relevant U.S. or EU government lists of prohibited persons, including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. Export information regarding our Offerings, including our export control classifications for our Offerings, is found here: https://www.splunk.com/en_us/legal/export-controls.html.

11. Usage Data

From time to time, Splunk may collect Usage Data generated as a by-product of your use of Offerings. Usage Data does not include Customer Content. We collect Usage Data for a variety of reasons, such as to identify, understand, and anticipate performance issues and the factors that affect them, to provide updates and personalized experiences to customers, and to improve the Splunk Offerings. Details on Splunk's Usage Data collection practices are set forth in Splunk's Privacy Policy found here: https://www.splunk.com/en_us/legal/privacy/privacy-policy.html.

12. Capacity and Usage Verification

- (A) **Certification and Verification.** At Splunk's request, you will furnish Splunk a certification signed by your authorized representative verifying that your use of the Purchased Offering is in accordance with these General Terms and the applicable Order. For On-Premises Products, we may also ask you from time to time, but not more frequently than once per calendar period, to cooperate with us to verify usage and adherence to purchased Capacities. If Splunk requests a verification process, you agree to provide Splunk reasonable access to the On-Premises Product installed at your facility (or as hosted by your Third-Party Provider). If Splunk does any verification, it will be performed with as little interference as possible to your use of the On-Premises Product and your business operations. Splunk will comply with your (or your Third-Party Providers') reasonable security procedures.
- (B) **Overages.** If a verification or usage report reveals that you have exceeded the purchased Capacity or usage rights for your Purchased Offering (e.g., used as a service bureau) during the period reviewed, then we will have the right to invoice you using the applicable Fees at list price then in effect, which will be payable in accordance with these General Terms. Without limiting Splunk's

foregoing rights, with respect to Hosted Services, Splunk may work with you to reduce usage so that it conforms to the applicable usage limit, and we will in good faith discuss options to right size your subscription as appropriate. Notwithstanding anything to the contrary herein, Splunk will have the right to directly invoice you for overages, regardless of whether you purchased the Purchased Offering from an authorized reseller or Digital Marketplace. See the Specific Offering Terms for any additional information related to overages for a Hosted Service.

13. Our Use of Open Source

Certain Offerings may contain Open Source Software. Splunk makes available in the applicable Documentation a list of Open Source Software incorporated in our On-Premises Products as required by the respective Open Source Software licenses. Any Open Source Software that is delivered as part of your Offering and which may not be removed or used separately from the Offering is covered by the warranty, support and indemnification provisions applicable to the Offering. Some of the Open Source Software may have additional terms that apply to the use of the Offering (e.g., the obligation for us to provide attribution of the specific licensor), and those terms will be included in the Documentation; however, these terms will not (a) impose any additional restrictions on your use of the Offering, or (b) negate or amend any of our responsibilities with respect to the Offering.

14. Splunk Developer Tools and Customer Extensions

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

You have a nonexclusive, worldwide, nontransferable, nonsublicensable right, subject to the terms of these General Terms, to use Splunk Developer Tools to develop your Customer Extensions, including to support interoperability between the Offering and your system or environment. Splunk proprietary legends or notices contained in the Splunk Developer Tools may not be removed or altered when used in or with your Customer Extension. You retain title to your Customer Extensions, subject to Splunk’s ownership in our Offerings and any materials and technology provided by Splunk in connection with the Splunk Developer Tools. You agree to assume full responsibility for the performance and distribution of Customer Extensions.

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

(A) **Third-Party Extensions on Splunkbase.** Splunk makes Extensions developed and/or made available by a third-party on Splunkbase (“**Third-Party Extension**”) available for download or access as a convenience to its customers. Splunk makes no promises or guarantees related to any

Third-Party Extension, including the accuracy, integrity, quality, or security of the Third-Party Extension. Nothing in these General Terms or on Splunkbase will be deemed to be a representation or warranty by Splunk with respect to any Third-Party Extension, even if a particular Third-Party Extension is identified as “certified” or “validated” for use with an Offering. We may, in our reasonable discretion, block or disable access to any Third-Party Extension at any time. Your use of a Third-Party Extension is at your own risk and may be subject to any additional terms, conditions, and policies applicable to that Third-Party Extension (such as license terms, terms of service, or privacy policies of the providers of such Third-Party Extension). Third-Party Extensions may be installed on Hosted Services pursuant to our instructions.

- (B) **Third-Party Content.** Hosted Services may contain features or functions that enable interoperation with Third-Party Content that you, in your sole discretion, choose to add to a Hosted Service. You may be required to obtain access separately to such Third-Party Content from the respective providers, and you may be required to grant Splunk access to your accounts with such providers to the extent necessary for Splunk to allow the interoperation with the Hosted Service. By requesting or allowing Splunk to enable access to such Third-Party Content in connection with the Hosted Services, you certify that you are authorized under the provider’s terms to allow such access. If you install or enable (or direct or otherwise authorize Splunk to install or enable) Third-Party Content for use with a Hosted Service where the interoperation includes access by the third-party provider to your Customer Content, you hereby authorize Splunk to allow the provider of such Third-Party Content to access Customer Content as necessary for the interoperation. You agree that Splunk is not responsible or liable for disclosure, modification or deletion of Customer Content resulting from access to Customer Content by such Third-Party Content, nor is Splunk liable for any damages or downtime that you may incur or any impact on your experience of the Hosted Service, directly or indirectly, as a result of your use of and/or reliance upon, any Third-Party Content, sites or resources.
- (C) **Splunk As a Reseller.** When you purchase third party products ("**Third Party Products**") from Splunk as specified in an Order (which products shall include third party software, but not any support which Splunk itself has contracted to provide), the following provision applies. Splunk acts solely as a reseller of Third Party Products, which are fulfilled by the relevant third party vendor ("**Third Party Vendor**"), and the purchase and use of Third Party Products is subject solely to the terms, conditions and policies made available by such Third Party Vendor. Consequently, Splunk makes no representation or warranty of any kind regarding the Third Party Products, whether express, implied, statutory or otherwise, and specifically disclaims all implied terms, conditions and warranties (including as to quality, performance, availability, fitness for a particular purpose or non-infringement) to the maximum extent permitted by applicable law. You will bring any claim in relation to Third Party Products against the applicable Third Party Vendor directly. In no event will Splunk be liable to you for any claim, loss or damage arising out of the use, operation or

availability of Third Party Product (whether such liability arises in contract, negligence, tort, or otherwise).

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

16. Your Compliance

- (A) **Lawful Use of Offerings.** When you access and use an Offering, you are responsible for complying with all laws, rules, and regulations applicable to your access and use. This includes being responsible for your Customer Content and users, for your users’ compliance with these General Terms, and the accuracy, lawful use of, and the means by which you acquired your Customer Content. You may not transmit and/or store PHI Data, PCI Data or ITAR Data within a Hosted Services unless you have specifically purchased a Purchased Offering for that applicable regulated Hosted Services environment (as identified in an Order).
- (B) **Registration.** You agree to provide accurate and complete information when you register for and use any Offering and agree to keep this information current. Each person who uses any Offering must have a separate username and password. For Hosted Services, you must provide a valid email address for each person authorized to use your Hosted Services, and you may only have one person per username and password. Splunk may reasonably require additional information in connection with certain Offerings (e.g., technical information necessary for your connection to a Hosted Service), and you will provide this information as reasonably requested by Splunk. You are responsible for securing, protecting, and maintaining the confidentiality of your account usernames, passwords and access tokens.
- (C) **Export Compliance.** You will comply with all applicable export laws and regulations of the United States and any other country (“**Export Laws**”) where your users use any of the Offerings. You certify that you are not on any of the relevant U.S. government lists of prohibited persons, including the Treasury Department’s List of Specially Designated Nationals and the Commerce Department’s List of Denied Persons or Entity List. You will not export, re-export, ship, transfer or otherwise use the Offerings in any country subject to an embargo or other sanction by the United States, including,

without limitation, Iran, Syria, Cuba, the Crimea Region of Ukraine, Sudan and North Korea, and you will not use any Offering for any purpose prohibited by the Export Laws.

- (D) **GovCloud Services.** If you access or use any Hosted Services in the specially isolated Amazon Web Services (“AWS”) GovCloud (US) region (including without limitation any Hosted Services that are provisioned in a FedRAMP authorized environment within the AWS GovCloud (US) region)), you hereby represent and warrant that: (i) you are a “US Person” as defined under ITAR (see 22 CFR part 120.62); (ii) you have and will maintain a valid Directorate of Defense Trade Controls registration, if required by ITAR; (iii) you and your end users are not subject to export control restrictions under US export control laws and regulations (i.e., users are not denied or debarred parties or otherwise subject to sanctions); (iv) you will maintain an effective compliance program to ensure compliance with applicable US export control laws and regulations, including ITAR, as applicable; and (v) you will maintain effective access controls as described in the Specific Offering Terms for the applicable Hosted Services. You are responsible for verifying that any user accessing Customer Content in the Hosted Services in the AWS GovCloud (US) region is eligible to access such Customer Content. The Hosted Services in the AWS GovCloud (US) region may not be used to process or store classified data. You will be responsible for all sanitization costs incurred by Splunk if users introduce classified data into the Hosted Services in the AWS GovCloud (US) region. You may be required to execute additional addendums to this agreement prior to provisioning of selected Hosted Services.
- (E) **Acceptable Use.** Without limiting any terms under these General Terms, you will also abide by our Hosted Services acceptable use policy: <https://www.splunk.com/view/SP-CAAAMB6>.

17. Confidentiality

- (A) **Confidential Information.** Each party will protect the Confidential Information of the other. Accordingly, Receiving Party agrees to: (i) protect the Disclosing Party’s Confidential Information using the same degree of care (but in no event less than reasonable care) that it uses to protect its own Confidential Information of a similar nature; (ii) limit use of Disclosing Party’s Confidential Information for purposes consistent with these General Terms, and (iii) use commercially reasonable efforts to limit access to Disclosing Party’s Confidential Information to its employees, contractors and agents or those of its Affiliates who have a bona fide need to access such Confidential Information for purposes consistent with these General Terms and who are subject to confidentiality obligations no less stringent than those herein.
- (B) **Compelled Disclosure of Confidential Information.** Notwithstanding the foregoing terms, the Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled (i) by law enforcement agencies or regulators or (ii) due to its obligations under applicable public records, “sunshine,” or similar statute to do so, provided the Receiving Party gives the Disclosing Party prior

notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a Party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

18. Payment

The payment terms below only apply when you purchase Offerings directly from Splunk. When you purchase from an authorized reseller or Digital Marketplace, the payment terms are between you and the authorized reseller or Digital Marketplace. However, a breach of your payment obligations for an Offering with a Digital Marketplace will be deemed a breach of this Section 18.

- (A) **Fees.** You agree to pay all Fees specified in the Orders. Fees are non-cancelable and non-refundable, except as otherwise expressly set forth in these General Terms. Without limiting any of our other rights or remedies herein, overdue charges may accrue interest monthly at the rate of 1.5% of the then-outstanding unpaid balance, or the maximum rate permitted by law, whichever is lower. Fees are due and payable either within 30 days from the date of Splunk's invoice or as otherwise stated in the Order.
- (B) **Credit Cards.** If you pay by credit, or debit card you: (i) will provide Splunk or its designated third-party payment processor with valid credit or debit card information; and (i) hereby authorize Splunk or its designated third-party payment processor to charge such credit or debit card for all items listed in the applicable Order. Such charges must be paid in advance or in accordance with any different billing frequency stated in the applicable Order. You are responsible for providing complete and accurate billing and contact information and notifying Splunk in a timely manner of any changes to such information.
- (C) **Taxes.** All Fees quoted are exclusive of applicable taxes and duties, including any applicable sales and use tax. You are responsible for paying any taxes or similar government assessments (including, without limitation, value-added, sales, use or withholding taxes). We will be solely responsible for taxes assessable against us based on our net income, property, and employees.

19. Splunk's Warranties

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

- (B) **General Corporate Warranty.** Splunk warrants that it has the legal power and authority to enter into these General Terms.
- (C) **Hosted Services Warranty.** Splunk warrants that during the applicable Term: (i) Splunk will not materially decrease the overall functionality of the Hosted Services; and (ii) the Hosted Services will perform materially in accordance with the applicable Documentation. Our sole and exclusive liability, and your sole and exclusive remedy for any breach of these warranties, will be your right to terminate the applicable Hosted Services Purchased Offering, and we will refund to you any prepaid but unused Fees for the remainder of the Term.
- (D) **On-Premises Product Warranty.** Splunk warrants that for a period of ninety (90) days from the Delivery of an On-Premises Product, the On-Premises Product will substantially perform the material functions described in the applicable Documentation for such On-Premises Product, when used in accordance with the applicable Documentation. Splunk's sole liability, and your sole remedy, for any failure of the On-Premises Product to conform to the foregoing warranty, is for Splunk to do one of the following (at Splunk's sole option and discretion) (i) modify, or provide an Enhancement for, the On-Premises Product so that it conforms to the foregoing warranty, (ii) replace your copy of the On-Premises Product with a copy that conforms to the foregoing warranty, or (iii) terminate the Purchased Offering with respect to the non-conforming On-Premises Product and refund the Fees paid by you for such non-conforming On-Premises Product.
- (E) **Disclaimer of Implied Warranties.** Except as expressly set forth above, the Offerings are provided "as is" with no warranties or representations whatsoever express or implied. Splunk and its suppliers and licensors disclaim all warranties and representations, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, noninfringement, or quiet enjoyment, and any warranties arising out of course of dealing or trade usage. Splunk does not warrant that use of Offerings will be uninterrupted, error free or secure, or that all defects will be corrected..

20. Ownership

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

- (B) **Customer Content.** You own and reserve all right, title and interest in your Customer Content. By sending Customer Content to a Hosted Service, you grant us a worldwide, royalty free, non-exclusive license to access and use the Customer Content for purposes of providing you the Hosted Service.
- (C) **Feedback.** You have no obligation to provide us with ideas for improvement, suggestions, or other feedback (collectively, “**Feedback**”) in connection with an Offering, unless otherwise expressly set forth in the applicable Order. If, however, you provide any Feedback, you hereby grant to Splunk a non-exclusive, transferable, irrevocable, worldwide, royalty-free license (with rights to sublicense) to make, use, sell, offer to sell, reproduce, modify, distribute, make available, publicly display and perform, disclose and otherwise commercially exploit the Feedback.

21. Term and Termination

- (A) **Term and Renewal.** These General Terms will commence upon the Effective Date and will remain in effect until the expiration of all applicable Purchased Offerings, unless earlier terminated pursuant to this Section. Termination of a specific Purchased Offering will not affect the Term of any other Purchased Offering. Termination of these General Terms will have the effect of terminating all Purchased Offerings. Grounds for terminating a Purchased Offering (e.g., for non-payment), that are specific to the Purchased Offering, will not be grounds to terminate Purchased Offerings where no breach exists. The Term of a Purchased Offering will not renew without mutual agreement of the parties.
- (B) **Termination.** Either party may terminate these General Terms, or any Purchased Offering, by written notice to the other party in the event of a material breach of these General Terms, or the specific terms associated with that Purchased Offering, that is not cured within thirty (30) days of receipt of the notice. Upon any expiration or termination of a Purchased Offering, the rights and licenses granted to you for that Purchased Offering will automatically terminate, and you agree to immediately (i) cease using and accessing the Offering, (ii) return or destroy all copies of any On-Premises Products and other Splunk materials and Splunk Confidential Information in your possession or control, and (iii) upon our request, certify in writing the completion of such return or destruction. Upon termination of these General Terms or any Purchased Offering, Splunk will have no obligation to refund any Fees or other amounts received from you during the Term. Notwithstanding any early termination above, except for your termination for our uncured material breach, you will still be required to pay all Fees payable under an Order.
- (C) **Survival.** The termination or expiration of these General Terms will not affect any provisions herein which by their nature survive termination or expiration, including the provisions that deal with the following subject matters: definitions, ownership of intellectual property,

confidentiality, payment obligations, effect of termination, limitation of liability, privacy, and the “Miscellaneous” section in these General Terms.

- (D) **Suspension of Service.** In the event of a material breach or threatened material breach of this Agreement, Splunk may, without limiting its other rights and remedies, suspend your use of the Hosted Service until such breach is cured or Splunk reasonably believes there is no longer a threat, provided that, we will give you at least five (5) days’ prior notice before suspension. Suspension of a Hosted Service will have no impact on the duration of the Term of the Purchased Offering, or the associated Fees owed.

22. Limitation of Liability

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

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

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

The limitation of liability herein will not apply to a party’s infringement of the other party’s intellectual property rights, indemnification obligations, or the fraud, gross negligence or willful misconduct of a party.

The foregoing disclaimers of damages will also not apply to the extent prohibited by law. Some jurisdictions do not allow the exclusion or limitation of certain damages. To the extent such a law applies to you, some or all of the exclusions or limitations set forth above may not apply to you, and you may have additional rights.

23. Indemnity

- (A) **Our Indemnification to You.** Splunk will defend and indemnify you, and pay all damages (including attorneys' fees and costs) awarded against you, or that are agreed to in a settlement, to the extent a claim, demand, suit or proceeding is made or brought against you or your Affiliates by a third party (including those brought by a government entity) alleging that a Purchased Offering infringes or misappropriates such third party's patent, copyright, trademark or trade secret (a "**Customer Claim**"). Splunk will have no obligation under the foregoing provision to the extent a Customer Claim arises from your breach of these General Terms, your Customer Content, Third-Party Extension, or the combination of the Offering with: (i) Customer Content; (ii) Third-Party Extensions; (iii) any software other than software provided by Splunk; or (iv) any hardware or equipment. However, Splunk will indemnify against combination claims to the extent (y) the combined software is necessary for the normal operation of the Purchased Offering (e.g., an operating system), or (z) the Purchased Offering provides substantially all the essential elements of the asserted infringement or misappropriation claim. Splunk may in its sole discretion and at no cost to you: (1) modify any Purchased Offering so that it no longer infringes or misappropriates a third party right, (2) obtain a license for your continued use of the Purchased Offering, in accordance with these General Terms, or (3) terminate the Purchased Offering and refund to you any prepaid fees covering the unexpired Term.
- (B) **Your Indemnification to Us.** Unless expressly prohibited by applicable law, you will defend and indemnify us, and pay all damages (including attorneys' fees and costs) awarded against Splunk, or that are agreed to in a 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 your Customer Content or Customer Extensions infringes or misappropriates such third party's patent, copyright, trademark or trade secret, or violates another right of a third party; or (ii) alleges that your Customer Content or your use of any Offering violates applicable law or regulation.
- (C) **Mutual Indemnity.** Each party will defend, indemnify and pay all damages (including attorneys' fees and costs) awarded against the other party, or that are agreed to in a settlement to the extent that an action brought against the other party by a third party is based upon a claim for bodily injury (including death) to any person, or damage to tangible property resulting from the negligent acts or willful misconduct of the indemnifying party or its personnel hereunder, and will pay any reasonable, direct, out-of-pocket costs, damages and reasonable attorneys' fees attributable to such claim that are awarded against the indemnified party (or are payable in settlement by the indemnified party).
- (D) **Process for Indemnification.** The indemnification obligations above are subject to the party seeking indemnification to: (i) provide the other party with prompt written notice of the specific claim; (ii)

give the indemnifying party sole control of the defense and settlement of the claim (except that the indemnifying party may not settle any claim that requires any action or forbearance on the indemnified party's part without their prior consent, which will not unreasonably withhold or delay); and (iii) gives the indemnifying party all reasonable assistance, at such party's expense.

24. Updates to Offerings

Our Offerings and policies may be updated over the course of our relationship. From time to time, Splunk may update or modify an Offering and our policies, provided that: (a) the change and modification applies to all customers generally, and are not targeted to any particular customer; (b) no such change or modification will impose additional fees on you during the applicable Term or additional restrictions on your use of the Offering, (c) no such change will override or supersede the allocation of risk between us under these General Terms, including without limitation the terms under Sections 22 (Limitation of Liability) and 23 (Indemnity); (d) no such change or modification will materially reduce the security protections or overall functionality of the applicable Offering; and (e) any such change or modification will apply only prospectively, and will not apply to any breach or dispute that arose between the parties prior to the effective date of the change or modification. In the event of any conflict between these General Terms and the policies incorporated herein by reference, these General Terms will control.

25. Governing Law

These General Terms will be 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. Any legal action or proceeding arising under these General Terms 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.

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

26. Use of Customer Name

You agree that we may add your name to our customer list and identify you as a Splunk customer on Splunk's websites. Any further public use of your name in connection with Splunk marketing activities (e.g., press releases) will require your prior approval.

27. Miscellaneous

- (A) **Different Terms.** Splunk expressly rejects terms or conditions in any Customer purchase order or other similar document that are different from or additional to the terms and conditions set forth in these General Terms. Such different or additional terms and conditions will not become a part of the agreement between the parties notwithstanding any subsequent acknowledgement, invoice or license key that Splunk may issue.
- (B) **No Future Functionality.** You agree that your purchase of any Offering is not contingent on the delivery of any future functionality or features, or dependent on any oral or written statements made by Splunk regarding future functionality or features.
- (C) **Notices.** Except as otherwise specified in these General Terms, all notices related to these General Terms will be sent in writing to the addresses set forth in the applicable Order, or to such other address as may be specified by either party to the other party, and will be effective upon (i) personal delivery, (ii) the second business day after mailing, or (c), except for notices of termination or an indemnifiable claim (“**Legal Notices**”), which shall clearly be identifiable as Legal Notices, the day of sending by email. Billing-related notices to Customer will be addressed to the relevant billing contact designated by Customer. All other notices to Customer will be addressed to the relevant system administrator designated by Customer.
- (D) **Assignment.** Neither party may assign, delegate, or transfer these General Terms, in whole or in part, by agreement, operation of law or otherwise without the prior written consent of the other party, however Splunk may assign these General Terms in whole or in part to an Affiliate or in connection with an internal reorganization or a merger, acquisition, or sale of all or substantially all of Splunk’s assets to which these General Terms relates. Any attempt to assign these General Terms other than as permitted herein will be null and void. Subject to the foregoing, these General Terms will bind and inure to the benefit of the parties’ permitted successors and assigns.
- (E) **U.S. Government Use Terms.** Splunk provides Offerings for U.S. federal government end use solely in accordance with the following: Government technical data and rights related to Offerings include only those rights customarily provided to the public as defined in these General Terms. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software) and, for Department of Defense transactions, DFARS 252.227-7015 (Technical Data–Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Commercial Computer Software Documentation). If a government agency has a need for rights not conveyed under these terms, it must negotiate with Splunk to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

- (F) **Waiver; Severability.** The waiver by either party of a breach of or a default under these General Terms will not be effective unless in writing. The failure by either party to enforce any provisions of these General Terms will not constitute a waiver of any other right hereunder or of any subsequent enforcement of that or any other provisions. If a court of competent jurisdiction holds any provision of these General Terms invalid or unenforceable, the remaining provisions of these General Terms will remain in full force and effect, and the provision affected will be construed so as to be enforceable to the maximum extent permissible by law.
- (G) **Integration; Entire Agreement.** These General Terms along with any additional terms incorporated herein by reference, constitute the complete and exclusive understanding and agreement between the parties and supersedes any and all prior or contemporaneous agreements, communications and understandings, written or oral, relating to their subject matter. Except as otherwise expressly set forth herein, any waiver, modification, or amendment of any provision of these General Terms will be effective only if in writing and signed by duly authorized representatives of both parties.
- (H) **Force Majeure.** Neither party or its Affiliates, subsidiaries, officers, directors, employees, agents, partners and licensors will (except for the obligation to make any payments) be liable for any delay or failure to perform any obligation under these General Terms where the delay or failure results from any cause beyond their reasonable control, including, without limitation, acts of God, labor disputes or other industrial disturbances, electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockades, embargoes, riots, acts or orders of government, acts of terrorism, or war.
- (I) **Independent Contractors; No Third-Party Beneficiaries.** The parties are independent contractors. These General Terms do not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the parties. There are no third-party beneficiaries of these General Terms. Neither party has the authority to bind or act on behalf of the other party in any capacity or circumstance whether by contract or otherwise.

General Terms Definitions Exhibit

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

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

“CCPA” means the California Consumer Privacy Act of 2018.

“Confidential Information” means all nonpublic information disclosed by a party (“**Disclosing Party**”) to the other party (“**Receiving Party**”), whether orally or in writing, that is designated as “confidential” or that, given the nature of the information or circumstances surrounding its disclosure, should reasonably be understood to be confidential. Notwithstanding the foregoing, “Confidential Information” does not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

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

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

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

“Digital Marketplace” means an online or electronic marketplace operated or controlled by a third party where Splunk has authorized the marketing and distribution of its Offerings.

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

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

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

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

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

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

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

“Internal Business Purpose” means your use of an Offering for your own internal business operations, based on the analysis, monitoring or processing of your data from your systems, networks, and devices. Accordingly, Internal Business Purpose does not include monitoring or servicing the systems, networks and devices of third parties.

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

“Nonprofit” means a U.S. Federal 501(c)(3), tax-exempt, nonprofit corporation or association (or other nonprofit entity organized in accordance with the laws of where your nonprofit entity is registered) that has qualified for a free, donated Offering in connection with a Splunk donation program.

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

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

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

“Orders” means Splunk’s quote or ordering document (including online order form) accepted by you via your purchase order or other ordering document submitted to Splunk (directly or indirectly through an authorized reseller or Digital Marketplace) to order Offerings, which references the Offering, 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 your purchase order or other terms on a purchase order that are additional or inconsistent with the terms of these General Terms.

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

“PHI Data” means any protected health data, as defined under HIPAA.

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

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

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

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

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

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

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

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

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

UNITED STATES STATE & LOCAL GOVERNMENT LAW EXHIBIT TO SPLUNK GENERAL TERMS

This exhibit (the “**Exhibit**”) forms an integral part of the Splunk General Terms. In the event of any conflict between the General Terms and this Exhibit, this Exhibit will prevail and control. **This Exhibit is applicable only if you are a United States state or local government entity, including a public institute of higher education.**

1. **Your Compliance.** A new Section 16 (F) of the General Terms is added as follows:

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

2. **Limitation of Liability.** Section 22 of the General Terms is replaced in its entirety with the following:

22. Limitation of Liability

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

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

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

The limitation of liability herein will not apply to a party’s infringement of the other party’s intellectual property rights, indemnification obligations, Customer’s breach of sections 9(i) or 16(F), or the fraud, gross negligence or willful misconduct of a party.

The foregoing disclaimers of damages will also not apply to the extent prohibited by law. Some jurisdictions do not allow the exclusion or limitation of certain damages. To the extent such a law applies to you, some or all of the exclusions or limitations set forth above may not apply to you, and you may have additional rights.

3. **Indemnity.** Section 23 of the General Terms is replaced in its entirety with the following:

23. Indemnity

- (A) **Our Indemnification to You.** Splunk will defend and indemnify you, and pay all damages (including attorneys' fees and costs) awarded against you, or that are agreed to in a settlement, to the extent a claim, demand, suit or proceeding is made or brought against you or your Affiliates by a third party (including those brought by a government entity) alleging that a Purchased Offering infringes or misappropriates such third party's patent, copyright, trademark or trade secret (a "**Customer Claim**"). Splunk will have no obligation under the foregoing provision to the extent a Customer Claim arises from your breach of these General Terms, your Customer Content, Third-Party Extension, or the combination of the Offering with: (i) Customer Content; (ii) Third-Party Extensions; (iii) any software other than software provided by Splunk; or (iv) any hardware or equipment. However, Splunk will indemnify against combination claims to the extent (y) the combined software is necessary for the normal operation of the Purchased Offering (e.g., an operating system), or (z) the Purchased Offering provides substantially all the essential elements of the asserted infringement or misappropriation claim. Splunk may in its sole discretion and at no cost to you: (1) modify any Purchased Offering so that it no longer infringes or misappropriates a third party right, (2) obtain a license for your continued use of the Purchased Offering, in accordance with these General Terms, or (3) terminate the Purchased Offering and refund to you any prepaid fees covering the unexpired Term. Further, Splunk will defend, indemnify and pay all damages (including attorneys' fees and costs) awarded against you, or that are agreed to in a settlement to the extent that an action brought against you by a third party is based upon a claim for bodily injury (including death) to any person, or damage to tangible property resulting from the negligent acts or willful misconduct of Splunk or its personnel hereunder, and will pay any reasonable, direct, out-of-pocket costs, damages and reasonable attorneys' fees attributable to such claim that are awarded against you (or are payable in settlement by you).
- (B) **Process for Indemnification.** The indemnification obligations above are subject to the party seeking indemnification to: (i) provide the other party with prompt written notice of the specific claim; (ii) give the indemnifying party sole control of the defense and settlement of the claim to the maximum extent permissible under applicable law (except that the indemnifying party may not settle any claim that requires any action or forbearance on the

indemnified party's part without their prior consent, which will not unreasonably withhold or delay); and (iii) gives the indemnifying party all reasonable assistance, at such party's expense.

4. **Governing Law.** Section 25 of the General Terms is replaced in its entirety with the following:

25. Governing Law

These General Terms will be 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. Any legal action or proceeding arising under these General Terms 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. **Notwithstanding the foregoing, if you are a United States state or local government entity, including a public institute of higher education, the Agreement is governed by the laws of your state, excluding its conflict of laws principles. These General Terms do not affect statutory rights that cannot be waived or changed by contract.**

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

Support Exhibit to Splunk General Terms

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

1. Support Programs

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

2. Support Services

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

3. Support Policy

Our Support Policy, provided here: https://www.splunk.com/en_us/legal/splunk-software-support-policy.html (**"Support Policy"**) describes the duration of our Support Services for certain Splunk On-Premises Products and other policies associated with our Support Services.

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

4. Case Priority

Each Support Program offers different support levels for your case priority levels. When submitting a case, you will select the priority for initial response by logging the case online, in accordance with the

priority guidelines set forth under your Support Program. When the case is received, we may in good faith change the priority if the issue does not conform to the criteria for the selected priority. When that happens, we will provide you with notice (electronic or otherwise) of such change.

5. Exclusions

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

6. Support for Splunk Extensions

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

7. Authorized Support Contacts

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

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

We only take support requests from, and communicate with, your Support Contacts in connection with support cases. We strongly recommend that your Support Contact(s) are trained on the applicable

Offering. In order to designate Support Contacts, you must provide the individual's primary email address and Splunk.com login ID.

8. Defect Resolution

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

9. Your Assistance

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

10. Changes to Support Programs

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

Configuration and Implementation Services Exhibit to Splunk General Terms

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

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

1. Services and Statements of Work

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

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

2. Our Personnel

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

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

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

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

3. Our Background Checks, Security and Compliance Obligations

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

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

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

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

4. Your Materials

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

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

- (A) **C&I Services Materials.** The C&I Services we perform (e.g., configuration of our Offerings), and the C&I Services Materials we offer, create, and deliver to you in connection with the C&I Services, are generally applicable to our business, and therefore we require the right to be able to re-use the C&I Services Materials we create for one customer in connection with all of our customers. For the avoidance of doubt, our use of the C&I Services Materials created for you in connection with C&I Services will comply with our ongoing obligations and restrictions with respect to your Customer Materials and your Confidential Information, and we will not identify you in any way in connection with our further use of such C&I Services Materials.
- (B) **Customer Owned Work Product.** However, in the unlikely event that the parties agree that C&I Services Materials for a project are custom work product unique to your business, and not applicable to other customers generally, we will transfer ownership to those agreed C&I Services Materials to you under the applicable Statement of Work. C&I Services Materials must be expressly identified as “**Customer Owned Work Product**” under a Statement of Work for ownership to pass to you. Subject to payment of applicable Fees under the Statement of Work, we hereby assign to you all rights, title and interest (including all Intellectual Property Rights therein) in and to all C&I Services Materials identified as Customer Owned Work Product (but excluding all Splunk Preexisting IP incorporated into the Customer Owned Work Product). At your request and expense, we will assist and cooperate with you in all reasonable respects and will execute documents and take such further acts reasonably requested by you to enable you to acquire, transfer, maintain, perfect, and enforce your ownership rights in such Customer Owned Work Product.
- (C) **Our Ownership.** Subject to your ownership rights in Customer Owned Work Product and Customer Materials, we will own all rights in and to all C&I Services Materials.
- (D) **License Rights.** For those C&I Services Materials that are not Customer Owned Work Product, you will have the right to access and use those C&I Services Materials in connection with your applicable Offerings, and those rights will be of the same scope and duration as your rights to the underlying Offering.

6. C&I Services Warranty

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

7. Your Cooperation

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

8. Insurance

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

- (i) Commercial General Liability Insurance with a limit of not less than \$1,000,000 per occurrence and a general aggregate limit of not less than \$2,000,000.
- (ii) Business Auto Insurance with a limit of not less than \$1,000,000 combined single limit. Such Insurance will cover liability arising out of “hired and non-owned” automobiles.
- (iii) Worker’s Compensation Insurance as required by workers’ compensation, occupational disease and occupational health and safety laws, statutes, and regulations.
- (iv) Technology Errors & Omissions Insurance with a limit of not less than \$3,000,000 per occurrence and general aggregate.
- (v) Umbrella/Excess Insurance with a limit of not less than \$3,000,000 per occurrence and general aggregate.

9. Change Order Process

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

10. Expenses

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

11. Prepaid C&I Services

Unless otherwise expressly stated in a Statement of Work, all prepaid C&I Services must be redeemed within twelve (12) months from the date of purchase/invoice. At the end of the twelve (12) month term, any remaining pre-paid unused C&I Services will expire; no refunds will be provided for any remaining pre-paid unused C&I Services. Unless otherwise specifically stated in a Statement of Work, Education is invoiced and payable in advance.

Configuration and Implementation Services Definitions Exhibit

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

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

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

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

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

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

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

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

EXHIBIT B

Specific Terms for Splunk Offerings

SPECIFIC TERMS FOR SPLUNK OFFERINGS

Last updated: June 2024

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

Splunk Offerings Terms

Splunk Cloud Platform

1. Service Description

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

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

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

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

3. Service Level Schedule – Splunk Cloud Platform

Splunk’s Splunk Cloud Service Level Schedule, set forth at https://www.splunk.com/en_us/legal/splunk-cloud-service-level-schedule.html, will apply to the

availability and uptime of the Splunk Cloud Platform, subject to planned downtime and any unscheduled emergency maintenance according to Splunk's Maintenance Policy referenced in the Splunk Service Level Schedule. Customer will be entitled to service credits for downtime in accordance with the applicable Service Level Schedule.>

4. Data Usage Policy for Splunk Cloud Platform

For Subscriptions based on Maximum Daily Indexing Volume, Customer is entitled to periodically exceed the daily volume purchased by Customer in accordance with Splunk's data ingestion and daily license usage policy set forth

at [http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DataPolicies#Data ingestion and daily license usage](http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DataPolicies#Data%20ingestion%20and%20daily%20license%20usage).

EXHIBIT C

Splunk Cloud Platform Maintenance Policy

SPLUNK CLOUD PLATFORM MAINTENANCE POLICY

GENERAL

In order to operate in an efficient and secure manner as well as deliver the latest features set for our customers and users, the Splunk Cloud Platform has three classes of Splunk initiated changes:

- Service Updates
- Routine Maintenance
- Emergency Maintenance

Splunk will take no more than two maintenance windows for Service Updates and/or Routine Maintenance changes per calendar month.

Splunk will notify your Operational Contacts at least 14 days in advance for Service Updates and Routine Maintenance. For additional information regarding operational aspects of Splunk initiated changes or customer initiated maintenance, refer [here](#). Please contact Splunk Support by opening a case on the Splunk Customer Portal if you have any questions or concerns. For other Splunk hosted offerings, please refer to the corresponding service description pages.

CHANGE FREEZE

- Customers may request for a Change Freeze i.e., suspension of maintenance for Service Updates during specific dates or periods in the calendar month. Splunk will however review requests in view of the criticality of the change/update and make commercially reasonable efforts to honor those requests. Change Freezes are not guaranteed.
 - Change Freeze requests will only be considered for customer Splunk Cloud Platform stacks on a version released within the last 12 months.
- Change Freeze requests cannot be made for emergency maintenance or routine maintenance, and Splunk may override any previously approved Change Freeze requests to perform such maintenance.
- Splunk has a standing Change Freeze in effect for Splunk-Initiated Changes during the holiday period from December 15th to January 15th.
 - If you need additional Change Freeze time in addition to the holiday period please submit a Change Freeze request for a holiday extension.

- Only Emergency Maintenance updates will be performed during a holiday Change Freeze period.
- Opted-in Auto-updates will proceed as normal during any Change Freeze.
 - Examples can be found in this [blog](#).

SERVICE UPDATES

- Splunk will notify customer Operational Contacts at least 14 days prior to the Service Updates. Our communications will provide specifics about any required customer actions, such as updates to data ingestion mechanisms or applications.
- During Service Updates, ingest, login and search services may be degraded or unavailable for a short period of time within the maintenance window. Our communications will provide specifics about which services may be degraded or unavailable.
- Customers can change their assigned routine maintenance window date up to 72-hours prior to their scheduled window.

ROUTINE MAINTENANCE

Splunk will notify customer Operational Contacts at least 14 days prior to the Routine Maintenance. Our communications will provide specifics about any required customer actions, such as updates to data ingestion mechanisms or applications. Splunk may override any Change Freezes to perform routine maintenance.

- During Routine Maintenance, ingest, login and search services may be degraded or unavailable for a short period of time within the maintenance window. Our communications will provide specifics about which services may be degraded or unavailable.
- If requested at least 72-hours prior to the scheduled maintenance window, Splunk will make commercially reasonable efforts to honor change requests.

EMERGENCY MAINTENANCE

- Emergency Maintenance is performed in circumstances that require immediate attention. We expect these Emergency Maintenance windows to be rare and by its very nature not scheduled. Splunk will make commercially reasonable efforts to notify customer Operational Contacts. Our communications will provide specifics about any required customer actions, such as updates to data ingestion mechanisms or applications. Splunk may override any Change Freezes to perform emergency maintenance.

- During Emergency Maintenance, ingest, login and search services may be degraded or unavailable for a short period of time within the window. Our communications will provide specifics of any services that may be degraded or unavailable.

Please contact Splunk Support by opening a case on the [Support Portal](#) if you have any questions or concerns.

EXHIBIT D
Splunk Privacy Policy

Splunk Privacy Statement (“Privacy Policy”)

Updated: March 2024

This Privacy Policy explains how Splunk Inc. and its subsidiaries ("Splunk") collect, use, and disclose information you provide to us or which we otherwise collect (“Information”), including “Personal Data” by which we mean Information about an identified or reasonably identifiable individual.

This Privacy Policy applies to Offerings (as defined in the Splunk General Terms), splunk.com and to other websites Splunk operates that link to this Privacy Policy. This Privacy Policy does not apply to Personal Data processed by Splunk as a processor or to Splunk as an employer.

From time to time, Splunk acquires companies that may operate under their own privacy policies. You will continue to be presented with those companies’ privacy policies on their offerings and websites until the integration with Splunk is complete and those offerings and websites are linked to this Privacy Policy.

The use of our Offerings is also subject to the terms of the applicable customer agreement. The use of our website is subject to the [Splunk Websites Terms and Conditions of Use](#), and the terms of this Privacy Policy are incorporated into and form part of that agreement.

Data Collection

There are two primary ways in which Splunk collects Information about you: through [Interactions](#) and through [Offerings](#) as set forth below.

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 Splunk's websites or offices

Download materials through our websites

Provide or update account or contact details through our websites

Register for, attend, speak at or otherwise participate in Splunk-hosted or sponsored events (including, but not limited to, conferences, promotional events, webcasts, contests, or hackathons)

Participate in community programs and Splunk-related repositories on third-party open-source platforms Communicate with us (including by email, phone, text, online chat, or social media)

Provide testimonials or feedback

We collect Information about you from other sources such as public databases, commercial data sources, joint marketing partners, resellers, managed services providers and other partners, social media platforms, industry groups, and conference/event hosts We refer collectively to these contacts as "Interactions" and we explain below how we use the Information we collect through them.

What We Collect via Your Interactions

We (or others acting on our behalf) may collect your Information, including your Personal Data, through Interactions. The Personal Data we collect includes such things as:

Name or alias

Email address

Physical address, including country

Employer

Industry group

participation Title / position

Payment details

Phone number

Username / user ID

IP address

MAC address (or other device identifiers automatically assigned to your device when you access the internet including browser or device type)

Images and related metadata (for example, when visiting our offices or attending an event) Content of your communications and files you input, upload, or create

Videos (for example, when you provide a product testimonial)

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. From time to time, we offer virtual private networks (VPNs) for attendees at Splunk events or visitors

to our offices. If you access a Splunk-provided VPN, we may collect Personal Data from you, such as IP and MAC addresses, when we monitor the VPNs for security or performance.

IP addresses are also 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 the [Splunk Cookie Policy](#) and [How We Use Information Collected from Interactions](#).

When you make purchases through our website, we use third-party payment processors to collect credit card or other financial data. Splunk does not store the credit card data you provide, only payment confirmation information.

How We Use Information Collected from Interactions

Splunk uses the Information we collect from your Interactions to deliver Offerings to you in accordance with our terms, to fulfill our contractual and legal obligations, or to pursue legitimate business interests, as described below. Here is a summary of the purposes for which we use your Information, including Personal Data, to:

- Fulfill your orders or respond to your requests for information and other inquiries. For example, to satisfy your requests for website materials such as marketing collateral or whitepapers, we collect and use your name and email address.
- Operate, enhance, and personalize your experience on our websites. We collect Information via cookies and other information-gathering technologies (with your consent, where required) as stated in the [Splunk Cookie Policy](#) to fulfill our legitimate interest in operating our website, making it easy to navigate, and enriching the available content and offering information tailored to your interests. In doing so, we may receive your location Information, which you can disable by configuring the location sharing permissions in your device.
- Issue you Splunk accounts and provide you access to, and/enable your participation in, online communities and forums or to provide you with access to certain Offerings. Certain Offerings that display the Splunk name but present you with their own privacy notice are subject to such privacy notice and not this Privacy Policy.

- When you join our online communities and forums, including blogs and Splunk-branded business communication and streaming platform channels (collectively, “Online Forums”), we collect your Personal Data to enable your access and provide an interactive experience when you participate. The guidelines associated with those Online Forums recommend not sharing private or proprietary Information on them, as many of their aspects are public. If you choose to submit content to online forums, such content will be considered public and will not be subject to the privacy protections set forth in this Privacy Policy unless expressly required by law. Online Forums that display the Splunk name but present you with their own privacy notice are subject to such privacy notice and not this Privacy Policy.

- Send you administrative notices

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 or Offerings. We will use your name and email address to send such 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

To perform the services under the contract between you and Splunk, we need to collect certain Information from you such as your contact information and payment details. Without this Information, we may not be able to deliver the services or comply with our contractual or legal obligations.

- Advertise and market to you

With your consent or to pursue our legitimate interests as a business, we may contact you with announcements about our Offerings, educational materials, announcements about special offers, or information about upcoming or ongoing online/offline events, such as .conf, and related offers.

If required by applicable law, we will ask you for your consent before sending such communications and/or give you the choice to opt out of receiving these communications.

- Administer prize promotions and events

We use your Information to administer prize promotions and events based on the terms of the promotion or event. For example, if you enter into a prize promotion, we may use your data for winner selection and to provide the prize to you, if you win. Registration for a coding workshop or other events, may require adding your name to the list of expected attendees. If selected, we may seek your consent to announce you as a winner, which you may withdraw at any time. However, we will retain information collected in connection with your enrollment with the prize promotion or event.

- Invite you to participate on customer advisory boards or in surveys, studies, and assessments of Offerings or potential future Offerings

We use your Personal Data to register you to participate on advisory boards (such as our Customer Advisory Boards, Product Advisory Councils, or Developer Advisory Boards) or to request feedback from you about our Offerings or potential future Offerings. We use your feedback to fulfill our legitimate interest in improving our current and future Offerings and growing our business. Your participation is voluntary and subject to the terms of your agreements with us and this Privacy Policy.

- Diagnose and fix technical issues, monitor for security, and otherwise protect our property We do this to satisfy our legitimate interest in assessing actual or potential technical issues or threats to our facilities, attendees at Splunk-sponsored events, our IT systems and networks, Offerings, and website services. We may process your Information, in particular your IP address, for this purpose.

- Comply with law

We may use your Information to comply with any applicable laws, regulations, legal process, or governmental requests, or to protect our legal rights or those of others.

- For any other purpose disclosed to you in connection with our Offerings, website services, or other third-party platforms from time to time.

If we process your Personal Data for other purposes, we will provide you with information about such processing, and if required, obtain your consent.

Opting Out of Marketing Emails

If you no longer want to receive marketing emails from Splunk on a go-forward basis, please submit your request through our online [opt-out form](#). Alternatively, you may use the "unsubscribe" feature in our marketing email messages to opt-out of receiving marketing email messages.

Offerings

We also collect Information, including Personal Data, when providing our Offerings. We may ask you for this Information directly, or in some cases, we may collect it as you use our Offerings. For example, we collect Information from or about you when you (or someone you work with):

- Order or sign up for a trial of our Offerings
- Interact with Splunk online or offline, including when you request support services
- Log into or use our Offerings

What We Collect via Our Offerings We collect and process different types of data (described below) when you deploy our Offerings to fulfill our contractual and legal obligations, to operate our business, or fulfill other legitimate interests. The type of data we collect via our Offerings is Usage Data, which is data generated from the usage, configuration, deployment, access and performance of an Offering. We summarize for you here the types of usage data collected and the purposes for which we use this data below.

Usage Data Collected

Data about your operating environment and configuration, user interactions, and sessions related to your use of our Offerings. This may include information and related metadata about your network and systems architecture and configurations, OS and Offering versions, Offering configurations, installed applications, feature utilizations and frequencies, page loads and views, number and types of searches, errors, number of active and licensed users, source, source types and formats (e.g., json, xml, and csv), web browser details, http referrer page, and app workflows.

Data that allows us to identify account entitlements, such as license entitlement consumption, license capacity, or license type in our systems through an assigned license ID.

A combination of the above two, to provide account support including features used, deployment topology, performance metrics and license ID. The Information is user/customer-identifiable so that we can help address your specific issue and personalize your experience.

If you use a mobile device to access an Offering via an application “Apps” or “App”, as discussed below, that associates your mobile device with an identifier for your App. We may also receive information that your mobile device sends when you use our Apps, such as a device identifier or OS. Depending on a customer’s configuration of our Offerings, location information about users may be shared with Splunk. You can disable location sharing using the location-setting features on your mobile device.

For more information about the data collected through our Offerings, see the [Offering-specific documentation](#) (e.g., [Share data in Splunk Enterprise](#) in the Splunk Enterprise Admin Manual).

How We Use Usage Data We Collect via Our Offerings

We use the data and Information described above to fulfill our contractual obligations in providing the Offerings to you and to fulfill our legitimate interest in supporting and enhancing them. For example, we may use this data and Information to:

- Troubleshoot issues, provide support, and update our Offerings
- Provide guidance to help you optimize your configuration, security, and usage of our Offerings
- Better understand how our users use and configure our Offerings
- Determine which configurations or practices optimize performance (e.g., best practices)
- Benchmark key performance indicators (“KPIs”)
- Recommend enhancements
- Perform data analysis and audits
- Identify, understand, and anticipate performance issues and the factors that affect them

- Identify product security issues that may affect you and inform you of them
- Improve and develop new features and functionality
- Monitor the health, performance, and security of our Offerings
- Validate accounts, automate license verification, and offer enhancements
- Offer accelerated troubleshooting, notices of patches/upgrades, tips to optimize usage, security, configurations and/or performance, and suggestions about other Offerings that may be of interest to you
- Analyze usage trends, such as by data type, environment size, scale and architecture, and industry or sector, to develop and prioritize product enhancements (e.g., bug fixes or new features)
- To help us improve the user experience and personalize your services and content
- For any other purpose disclosed to you in connection with our Offerings or other third-party platforms from time to time

In certain paid on-premises products, the level of participation can be selected and changed. For more details on what we collect and participation options, see [Splunk's Documentation](#).

Other Collection Practices

We also collect Information 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 databases and manage your account. We also collect billing and payment Information and information about how you use our Offerings, including Information such as browser type, version number and operating system (OS), to administer your account, respond to customer service/support inquiries, and provide you with information about software updates via alerts or other “push” notifications. We may share this Information as described in [How Splunk Shares Your Information](#). We do not sell this Information.

Data Collection Practices Associated with Apps

Splunk's Offerings are extendible using software applications commonly called “apps,” “add-ons,” “widgets,” or “technical add-ons” we offer through splunkbase.splunk.com or other websites that may link to this Privacy Policy. 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 built by or on behalf of Splunk. It does not apply to Apps developed by others (“App Developers”), including those built by Splunk Works and Splunk Labs, which may be available through splunkbase.splunk.com, third-party marketplaces or repositories (e.g., AWS Marketplace, Google Play Store, and GitHub), or that are otherwise interoperable with our Offerings. Apps developed by App Developers are subject to their privacy notices.

Splunk requires App Developers to comply with applicable privacy and data protection laws but cannot guarantee that they do so. Before you use Apps created by App Developers, you should familiarize yourself with their privacy policies and license agreements.

Splunk collects Information generated from the use and performance of Apps that interoperate with its Offerings, such as crash data, version, session duration, and user engagement (e.g., number of downloads, active/licensed users, and logins). We may share this data with App Developers so they can improve and enhance the performance of their Apps.

How Splunk Shares Your Information

Splunk may disclose your Information to others in the following ways:

Subsidiaries. We may disclose Information to our [subsidiaries](#) subject to this Privacy Policy so that they can help market, sell, and service our Offerings. Splunk is the party responsible for the management of jointly used Personal Data. Splunk maintains intragroup agreements 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.

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. With your consent, we may also disclose your Information to App Developers to help support the performance of their Apps. App Developers will be identified to you when you download and use their Apps pursuant to their license and other terms.

Partners and Sponsors. We may disclose account and contact details to our [partners](#) and event hosts/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 our Offerings, conduct user research and surveys, or send you marketing communications, subject to the terms of their privacy policies. We may also share Usage Data with partners when they manage your Offering for you.

Internet Activity Service Providers. As described further in the [Splunk Cookie Policy](#), we may disclose internet or other electronic network activity Information, including, but not limited to, browsing history, search history, and Information regarding a consumer's interaction with a website, or advertisement if you enable or do not disable advertising cookies.

Online Forums. When you take certain actions on blogs and Splunk-branded business communication and streaming platform channels ("Online Forums") that are public or intended to be public in nature, such as when you broadcast content, participate in a chat room, post profile Information, or follow a channel, that Information may be collected, used, or disclosed by other participants in the Online Forums. In addition, some features of Online Forums are designed to provide others with Information about user activity, such as the subscription status of users for a given channel.

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 or government authorities (including those outside your country of residence); enforce our terms and conditions; and protect our operations and rights and safety of you and others, as needed. For more information about data we disclose in response to requests from law enforcement and other government agencies, please see the [Splunk Data Request Guidelines](#).

Merger, Sale, etc. We may disclose Information in the event of a proposed or actual

corporate or financing transaction, such as a reorganization, merger, sale, joint venture, acquisition, assignment, transfer, or 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 our Offerings in aggregated format, provided it does not include Personal Data. This may include “best practices” tips, key performance indicators (KPIs), benchmarking data or other such aggregated information useful to the user community. For select Offerings, we may share Information you provide, such as security artifacts that may contain Personal Data (e.g., IP address) with other subscribers, but only if required as part of the Offering, as set forth in the relevant terms.

Cookie Preferences

Splunk honors Global Privacy Control (GPC) signals that you enable on your browser. If you do not have GPC enabled on your browser or device, and depending on your location, we will seek your consent or provide an opportunity for you to select which cookies you would like to enable or disable. If you wish to change previously selected cookie preferences, please consult the [Splunk Cookie Policy](#).

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 is guaranteed to be 100% secure. If you have reason to believe that your Personal Data may no longer be secure (for example, if you feel that the security of an account has been compromised), please notify us immediately via the communication channels in 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 privacy and security issues affecting Information collected through your Interactions or use of our Offerings.

How Long We Store Your Information

Retention Period. We retain your 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 Splunk cloud environments 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 agreement with us and thereafter as required or permitted by law. We keep a record of your data requests, including your requests to opt out of marketing communications, to honor them in the future. See the [Splunk Data Retention Policy](#) for additional details.

Minors

Use of Offerings by Minors. Our Offerings, splunk.com and other websites Splunk operates are not directed to individuals 16 and under or those not of the age of majority in your jurisdiction, and we request that these individuals, or others on their behalf, not provide us with their Information.

Your Rights

In certain locations, you may have rights under data protection law, such as to request access to or correction, deletion, or transfer of your Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our [data request form](#), and we will respond as soon as reasonably practicable consistent with applicable law. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

European Economic Area, the UK, and Switzerland

We rely on a variety of legal bases to process Personal Data, including your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with a legal obligation. 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 of collection.

In Europe, Splunk Services UK Limited co-controls Personal Data required for contracts and accounts as described above in [Offerings](#) and [Other Collection Practices](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under [Contact Splunk](#) below. If your request or concern is not satisfactorily resolved by us, you can approach your local data protection authority. You can find your local data protection authority in the EU [here](#), in the UK [here](#), and in Switzerland [here](#).

Your Rights

Individuals located in the UK or European Economic Area are granted certain rights related to Personal Data, including the ability to:

- Ask whether we process Personal Data about you, and if we do, to access the Personal Data and certain information about how we use it and who we share it with;
- Request that we delete the Personal Data we hold about you in certain limited circumstances;
- Request that we stop processing the Personal Data we hold about you;
- Request that your Personal Data be provided to you or another organization in a structured, commonly used and machine-readable format;
- Object to our processing of data about you, including in relation to processing your Personal Data for marketing purposes; and
- Withdraw consent if processing of your Personal Data is based on consent.

If you or a designated third-party agent would like to exercise these rights, please submit the request through our [data request form](#), and we will respond in accordance with our legal obligations. We will verify your identity, and the identity of any third-party agent acting on your behalf, before we comply with the request and ask for your cooperation with our identity verification process.

Lawful Basis for Transferring Your Data: Cross-border Transfers

Your Personal Data may be stored and processed in any country where Splunk, its subsidiaries, partners, sub-processors, and third-party service providers conduct business or host events. These locations may be outside of your country of residence, including in the United States, where different data protection laws may apply. When we transfer Personal Data, we implement safeguards for protection of the transferred Personal Data, such as standard contractual clauses. We put in place appropriate terms to protect your Personal Data in our agreements with our service providers, processors, and sub-processors.

EU-U.S. Data Privacy Framework

Splunk has certified to the Department of Commerce that we adhere to the Data Privacy Framework Principles (“Principles”) of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, as further described in the [Splunk Data Privacy Framework Notice](#), and Splunk complies with all its obligations under the Principles. However, Splunk does not currently rely on the frameworks for transfers of Personal Data from the EU/EEA/Switzerland and the UK to the United States in its role as a controller. Instead, we continue to rely on standard contractual clauses. To learn more about the Data Privacy Framework program, please visit <https://www.dataprivacyframework.gov/>, where you can view Splunk’s certifications.

California

Capitalized terms in this section are as defined in the California Civil Code.

If you are a California Consumer, California law provides you with specific rights regarding your Personal Information, subject to certain exceptions. These the rights include:

the right to know the categories of Personal Information a business collects about you, the purposes for which such Information is collected or used, whether the Information is sold or shared, and the length of time a business intends to keep the Information;

the right to request deletion of Personal Information a business collects from you; the right to request correction of inaccurate Personal Information;

the right to request disclosure of Information collected, including specific pieces of Personal Information collected about you;

the right to request disclosure of Information Sold or Shared;

the right to opt-out of the Sale or Sharing of Personal Information; and the right to non-discrimination for exercising your rights.

If you or a designated third-party agent would like to exercise these rights, please submit the request through our [data request form](#) or via our toll-free number 1-888-914-9661 PIN #: 587261, and we will respond in accordance with our legal obligations. We will verify your identity, and the identity of any third-party agent acting on your behalf, before we comply with the request, and ask for your cooperation with our identity verification process.

Splunk may collect the following categories of Personal Information from California Consumers for purposes outlined in [How We Use Information Collected from Interactions](#) and [What We Collect via Our Offerings and How We Use It](#):

Identifiers or other elements of Personal Information under [California Civil Code Section 1798.80](#) and 1798.140 such as those described in [What We Collect via Your Interactions](#). Identifiers are retained 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.

Characteristics of protected class Information about veteran's status if you applied for a veteran's discount on educational credits. Splunk does not collect this Information directly. We use service providers to confirm eligibility. Eligibility status is retained 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.

Characteristics of protected class Information to verify disability status to grant reasonable accommodations for Splunk Certification testing. This Information is not stored by Splunk, only whether an accommodation was granted.

Commercial Information about products or services as described in [Other Collection Practices](#). This commercial Information is retained 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. Internet or other electronic network activity when you interact with Splunk's website as described in [What We Collect via Your Interactions](#), [What We Collect via Our Offerings and How We Use It](#), and the [Splunk Cookie Policy](#). Internet or other electronic network activity data is retained for the period necessary to fulfill the purposes outlined in this Privacy Policy and within the [Splunk Cookie Policy](#) unless a longer retention period is required or not prohibited by applicable law. You may change your cookie preferences at any time via the [Splunk Cookie Policy](#). The categories of third parties that receive this cookie data are outlined in Splunk's cookie banner and the [Splunk Cookie Policy](#). A full list of cookies and their sources are identified on [Splunk's Cookie Appendix](#). Geolocation data such as IP address as described in [What We Collect via Your Interactions](#), [What We Collect via Our Offerings and How We Use It](#), and the [Splunk Cookie Policy](#).

Geolocation data is retained for the period necessary to fulfill the purposes outlined in this Privacy Policy and within the [Splunk Cookie Policy](#) unless a longer retention period is required or not prohibited by applicable law. You may change your cookie preferences at any time via the [Splunk Cookie Policy](#). The categories of third parties that receive this cookie data are outlined in Splunk's cookie banner and the [Splunk Cookie Policy](#). A full list of cookies and their sources are identified on [Splunk's Cookie Appendix](#).

Inferences drawn from any of the Information identified in 1798.140. Any such inferences will be retained for the period necessary to fulfill the purposes outlined in this Privacy Policy and within the [Splunk Cookie Policy](#) unless a longer retention period is required or not prohibited by applicable law.

Within the scope of this Policy, Splunk does not collect or process Sensitive Personal Information

about California Consumers.

Splunk did not – in the preceding 12 months – and does not Sell or Share Personal Information of California Consumers. Splunk will seek your consent for use of cookies that are not strictly necessary and you can select which cookies to enable. If you wish to change previously selected cookie preferences, please consult the [Splunk Cookie Policy](#).

The source of each of these categories of Personal Information are outlined in this Privacy Policy in the [Interactions](#) and [Offerings](#) sections respectively.

The categories of Third Parties to whom Personal Information may be disclosed are outlined in this Privacy Policy in the [How Splunk Shares your Information](#) section. We may have disclosed any of the above categories of Personal Information pursuant to an individual's consent or under a written contract with a Service Provider for a Business Purpose.

Other U.S. States with Data Privacy Laws

The categories of Personal Data processed, the purposes of processing Personal Data, the categories of Personal Data shared with third parties and the categories of third parties with whom Splunk shares Personal Data are as outlined above.

Consumers in US states with privacy laws have privacy rights, such as to request access to or correction, deletion, or transfer of their Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you, or a person you have authorized, would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our [data request form](#), and we will respond in accordance with our legal obligations. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

In the event Splunk declines to take action on your request, we will respond with the legally-required information, including where applicable, instructions for how to submit your appeal. Once an appeal is received, Splunk will respond to the appeal in compliance with applicable

law.

Splunk does not sell your Personal Data. Splunk will seek your consent for use of cookies that are not strictly necessary and you can select which cookies to enable. If you wish to change previously selected cookie preferences, please consult the [Splunk Cookie Policy](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under [Contact Splunk](#) below.

Links to Other Parties

Our 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 without limitation any App Developer, social media platform provider, wireless service provider, or device manufacturer. The inclusion of a link within the Offerings does not imply endorsement of the linked site or service by Splunk. Splunk encourages you to review the privacy policies and learn about the privacy practices of the companies whose websites you choose to visit or Apps you choose to use. 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 listed on [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 other 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](#), [GitHub](#), [Twitch](#), [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 or Splunk's privacy practices, you can contact us at any time at dpo@splunk.com or by mail as provided below:

Splunk Inc.

Office of the Data Protection

Officer 250 Brannan Street

San Francisco, CA 94107

Splunk Services UK Limited

Office of the Data Protection

Officer Brunel Building 1 & 2

Canalside Walk London W2 1DG

England

Splunk Services Germany

GmbH Office of the Data

Protection Officer Mies-van-

der-Rohe-Straße 6

80335

München

Germany

Splunk Data Retention Policy

Updated: November 2021

Type of data	Retention timeframe*
License Usage Data - Splunk	5 years
Usage Data - Splunk	5 years
Usage Data - Splunk On-Call**	2 years
Usage Data - Splunk Observability***	13 months
Support Usage Data - Splunk	5 year
Mobile Device Data	5 years
Support diagnostic files provided by Customers (Splunk On-prem Only)	Up to 180 days

*Cloud log and event stream data excluded.

** Formerly VictorOps.

***Formerly SignalFx.

EXHIBIT E
Splunk Websites Terms and Conditions of Use

Splunk Websites Terms and Conditions of Use

LAST UPDATED: May 8, 2024

Splunk Inc., a Delaware corporation with a principal place of business at 250 Brannan Street, San Francisco, California, and its affiliates and subsidiaries (collectively, “**Splunk**”) makes information, products, and services available on this website (the “**Site**”), subject to the following terms and conditions of use (“**Terms**”). Before using this Site, please read these Terms carefully. Throughout these Terms, “we”, “us” and “our” refer to Splunk, and “you” or “your” refer to you personally (i.e., the individual who reads and agrees to be bound by these Terms), and, if you access this Site on behalf of a corporation or other legal entity, you and such corporation or other legal entity on whose behalf you access the Site. If you have entered into another agreement with us concerning specific services or products, then the terms of that agreement control where it conflicts with these Terms.

1. ACCEPTANCE OF TERMS

By using the Site, you agree to be bound by these Terms. If you do not agree to these Terms, please do not use the Site. Splunk provides the information, products and services on the Site to you, conditioned upon your acceptance, without modification, of these Terms contained herein. Your use of the Site constitutes your agreement with such Terms.

We reserve the right to change these Terms, in whole or in part, in our own discretion at any time. You can determine when these Terms were last revised by referring to the “LAST UPDATED” legend at the top of these Terms. Such modifications shall be effective immediately upon the linking of modified Terms to the Site, and, if you possess an account through the Site for which you have provided an email address (“**Account**”), by communicating the modifications to you either (i) when you log in to the Site or (ii) by sending the modifications to the email address that you have provided to us. You agree to comply with, and be bound by, any such modifications (i) by continuing to use or access the Site after modified Terms are posted to the Site or (ii) if you possess an Account, by not requesting to terminate your Account within seven (7) days after receiving a notice of modifications as described above.

In addition, your use of a particular Splunk service may be subject to specific guidelines or rules

(“Service-specific Rules”) posted from time to-time and incorporated by this reference into these Terms. If you do not accept our Terms or any Service-specific Rules, you should refrain from accessing the Site and its services. If we change any Service-specific Rules, we will post the changed version on the location where those Service-specific Rules normally appear, reference the change on the primary page for that service and include a link to the previous version of the terms or rules. Splunk reserves the right at any time and from time-to-time to modify or discontinue, temporarily or permanently, the Site or any service (or any part thereof). Splunk shall not be liable to any user or other third party for any such modification, suspension or discontinuance except as expressly provided herein.

2. U.S.-BASED WEBSITE

The Site is controlled and operated by Splunk from the United States, and, except as expressly set forth herein, is not intended to subject Splunk to the laws or jurisdiction of any state, country or territory other than that of the United States. Splunk does not represent or warrant that the Site or any part thereof is appropriate or available for use in any particular jurisdiction other than the United States. In choosing to access the Site, you do so on your own initiative and at your own risk, and are responsible for complying with all local laws, rules and regulations. You are also subject to U.S. export controls and are responsible for any violations of such controls, including any U.S. embargoes or other federal rules and regulations restricting exports. Splunk may limit the Site’s availability, in whole or in part, to any person, geographic area or jurisdiction Splunk chooses, at any time and in Splunk’s sole discretion. By using the Site, you hereby certify that: (a) you are not: (i) a citizen or permanent resident of any country on which the United States has embargoed goods, technology and/or services (e.g., Cuba, Iran, North Korea, Sudan, Syria, or Crimea), or (ii) on any of the relevant U.S. Government Lists of prohibited or restricted 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; and (b) your use of Splunk products and services is in compliance with the applicable U.S. export control and economic sanctions laws and regulations. For further information on the export controls and sanctions laws see, <http://www.bis.doc.gov/index.htm> and <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>

3. REGISTRATION AND USER INFORMATION

You may be required to register with Splunk in order to access certain areas of the Site. Your submission of registration and other personal data through the Site is governed by [Splunk’s Privacy Policy](#) (the “**Privacy Policy**”) and is hereby incorporated into these Terms by this reference. By

accepting these Terms, you agree to our collection, use, and disclosure of your information as described in the Privacy Policy. In the course of registration, you must: (a) provide true, accurate, current and complete information on the registration form and (b) maintain and promptly update such registration information as necessary. If, after investigation, we have reasonable grounds to suspect that your information is untrue, inaccurate, not current or incomplete, we may suspend or terminate your account and prohibit any and all current or future use by you of the Site (or any portion thereof). You may not use a user name (or email address) that is already being used by someone else; that may be construed as impersonating another person; that belongs to another person; that violates the intellectual property or other rights of any person; that is offensive; or that Splunk rejects for any other reason in its sole discretion. Your user name and password are for your personal use only, and not for use by any other person. You are responsible for maintaining the confidentiality of any password you may use to access the Site, and agree not to lend or transfer your password or user name, or lend or otherwise transfer your use of or access to the Site, to any third party. You are fully responsible for all interactions with the Site that occur in connection with your password or user name. You agree to notify Splunk immediately of any unauthorized use of your password or user name or any other breach of security related to your account or the Site, and to log off/exit from your account with the Site (if applicable) at the end of each session. Splunk is not liable for any loss or damage arising from your failure to comply with this Section, including any loss or damage arising from your failure to (a) immediately notify Splunk of any unauthorized use of your password or account or any other breach of security and (b) ensure that you log off/exit from your account at the end of each session.

4. PROPRIETARY RIGHTS; LICENSE GRANTS

4.1. Software. Any software that is made available to access or download by or through this Site (“**Software**”) is the copyrighted work of Splunk, its suppliers and/or its licensors. Your rights to access, download, and use any Software made available for download or access from the Site will be subject to your agreement to the terms and conditions of the software license agreement or other service agreement identified on the Site and/or in the Software (each, a “**License Agreement**”). You may not install or use any Software that is accompanied by or includes a License Agreement unless you have agreed to the applicable License Agreement. Except to the extent expressly permitted in any applicable License Agreement, or expressly authorized under applicable law overriding any of the following restrictions, you agree that you will not sell, lease, lend, convey, transmit, modify, adapt, translate, prepare derivative works from, decompile, reverse engineer, disassemble or attempt to derive source code from the Software. Any reproduction, redistribution or other use or exploitation of the Software not in accordance with the License Agreement and/or these Terms is expressly prohibited by law, and may result in civil and criminal penalties.

4.2. Content. Unless otherwise specifically noted, the information, content, data, text, graphics, images, videos, documents and other materials made available through the Site ("**Content**") are and shall remain the property of Splunk, its licensors and/or suppliers, and are protected by copyright, trademark, patent, and/or other proprietary rights and laws. To the extent that you acquire any rights in Content, you hereby assign all such worldwide intellectual property rights to Splunk. Subject to your compliance with these Terms, solely for so long as you are permitted by Splunk to access and use the Site, and provided that you keep intact all copyright and other proprietary notices, you may (a) view any Content on any single computer solely for personal, informational, non-commercial purposes, and (b) download and print one (1) copy of materials that Splunk specifically makes available for downloading (such as white papers or user documentation) from this Site solely for personal, informational, non-commercial purposes, provided that such Content may not be modified or altered in any way. Unless otherwise specifically permitted for any particular Content, you may not use, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, rent, lease, modify, loan, sell, distribute, or create derivative works based on, the Site or any Content, in whole or in part, without the express prior written authorization of Splunk.

4.3. Community Content. Your rights to access, use, copy and distribute any user- and community-generated information or content (including other users' Contributions, as defined below, or third-party apps or content made available on splunkbase.splunk.com, dev.splunk.com or community.splunk.com, collectively "**Community Content**") is subject to the relevant terms and conditions or license agreement attached to such Community Content. If there are no specific terms and conditions or license agreement attached to such Community Content, the licenses and restrictions under Section 4.2 "**Content**" will apply.

4.4. Proprietary Rights. Elements of the Site are protected by copyright, trade dress, trademark, unfair competition, and/or other laws and may not be copied or imitated in whole or in part. No logo, graphic, sound, or image from the Site may be copied or retransmitted unless expressly permitted in writing by Splunk. Nothing contained on the Site should be construed as granting, by implication, estoppel or otherwise, any license or right to use any of Splunk's or its suppliers' trade names, trademarks or service marks without Splunk's express prior written consent. "Splunk" and other Splunk logos, trademarks, service marks, and product and service names are the intellectual property of Splunk.

5. INFORMATION SUBMITTED THROUGH THE SITE

Unless otherwise specifically agreed to by you and Splunk, by uploading, emailing, posting, publishing or otherwise transmitting information, sample data, event types, tags, comments, suggestions, feedback, content or other materials to the Site or Splunk (each a **“Contribution”**), you hereby acknowledge that such Contribution is non-confidential and grant (or warrant that the owner of such rights has expressly granted) to Splunk a perpetual, irrevocable, worldwide, non-exclusive, sublicensable, fully paid-up and royalty-free license to use, make, have made, offer for sale, sell, copy, distribute, perform, display (whether publicly or otherwise), modify, adapt, publish and transmit such Contributions in any form, medium, or technology now known or later developed, and to grant to others rights to do any of the foregoing. In addition, you warrant that all so-called moral rights in the content have been waived. For each Contribution, you represent and warrant that you have all rights necessary for you to grant the licenses granted in this Section, and that such Contribution, and your provision thereof to and through the Site, comply with all applicable laws, rules and regulations.

Splunk will not pre-screen or review Contributions, but Splunk reserves the right to refuse or delete any Contributions in its discretion. You acknowledge and agree that Splunk reserves the right (but has no obligation) to do one or more of the following in its discretion, without notice or attribution to you: (i) monitor Contributions as well as your access to the Site; (ii) alter, remove, or refuse to post or allow to be posted any Contribution; and/or (iii) disclose any Contributions, and the circumstances surrounding their transmission, to any third party in order to operate the Site, in order to protect Splunk, its suppliers or licensees and their respective employees, officers, directors, shareholders, affiliates, agents, representatives, and the Site’s users and visitors; to comply with legal obligations or governmental requests; to enforce these Terms; or for any other reason or purpose. Splunk disclaims any responsibility for the Contributions displayed on its Site. Splunk assumes no responsibility for the timeliness, deletion, mis-delivery or failure to store or publish any Contributions or other user information or personalization settings.

Splunk does not control the Community Content, identified in section 4.3 (**“Community Content”**) posted on the Site and, as such, does not guarantee the accuracy, integrity or quality of such Community Content. Under no circumstances will Splunk be liable in any way for any Community Content, including, but not limited to, liability for any errors or omissions in any content or for any loss or damage of any kind incurred as a result of the use of such content. By using the Site, you may be exposed to Community Content that is offensive, indecent or objectionable. You must evaluate, and bear all risks associated with, the use of such content, including any reliance on the accuracy, completeness, or usefulness of such content.

6. PURCHASES

If you wish to purchase our products and services, for your convenience, we may provide links on the Site to a web store or e-commerce platform where you can make such purchases. Please be aware that the web store or e-commerce platform may be hosted, operated or managed by a third party, and may be governed by such third-party's website terms and conditions and privacy policy. We encourage you to read carefully those third-party terms and conditions and privacy policy prior to making any purchases. These Terms do not govern, and we are not responsible or liable for, your interaction with such third-party managed web store or e-commerce platform.

7. RULES OF CONDUCT

While using the Site you will comply with all applicable laws, rules and regulations. In addition, Splunk expects you to respect the rights and dignity of others. Your use of the Site is conditioned on your compliance with the rules of conduct set forth in this Section; any failure to comply may also result in termination of your access to the Site pursuant to Section 13 ***“Termination”***. You agree that you will not:

- Post, transmit, or otherwise make available, through or in connection with the Site:
- Anything that is or may be (a) threatening, harassing, degrading or hateful; (b) defamatory; (c) fraudulent or tortious; (d) obscene, indecent or otherwise objectionable; or (e) protected by copyright, trademark or other proprietary right without the express prior written consent of the owner of such right.
- Any material that would give rise to criminal or civil liability or that encourages conduct that constitutes a criminal offense.
- Any virus, worm, Trojan horse or other computer code, file, or program that is harmful or invasive or may or is intended to damage or hijack the operation of any hardware or software.
- Any unsolicited or unauthorized advertising, promotional materials, “junk mail,” “spam,” “chain letter,” “pyramid scheme”, “phishing”, or investment opportunity, or any other form of solicitation.
- Use the Site for any fraudulent or unlawful purpose.
- Harvest or collect personally identifiable information or personal information or personal data (as defined in various data protection regulations such as the General Data Protection

Regulation (EU) 2016/679 and the California Consumer Protection Act of 2018 (CCPA)) about other users of the Site.

- Impersonate any person or entity, including any representative of Splunk; falsely state or otherwise misrepresent your affiliation with any person or entity; or express or imply that Splunk endorses any statement you make.
- Interfere with or disrupt the operation of the Site or the servers or networks used to make the Site available, including disrupting or threatening the integrity or security of the Site; or violate any requirements, procedures, policies or regulations of such networks.
- Restrict, disrupt, interfere, or inhibit any other person from using the Site (including by hacking or defacing any portion of the Site, threatening, intimidating, or harassing others).
- Use the Site to advertise or offer to sell or buy any goods or services without Splunk's express prior written consent.
- Reproduce, duplicate, copy, sell, resell or otherwise exploit for any commercial purposes, any portion of, use of, or access to the Site (including any content, Software and other materials available through the Site).
- Modify, adapt, create derivative works of, translate, reverse engineer, decompile or disassemble any portion of the Site (including any content, Software and other materials available through the Site), except as and solely to the extent expressly authorized under applicable law overriding any of these restrictions.
- Remove any copyright, trademark or other proprietary rights notice from the Site or content, Software and other materials originating from the Site.
- Frame or mirror any part of the Site without Splunk's express prior written consent.
- Create a database by systematically downloading and storing all or any Site content.
- Use any robot, spider, site search/retrieval application or other manual or automatic device to retrieve, index, "scrape," "data mine" or in any way reproduce or circumvent the navigational structure or presentation of the Site, without Splunk's express prior, written consent.

8. LINKS

You may find links to other websites on the Site. Those links will let you leave Splunk's site. Splunk exercises no control whatsoever over such third-party websites and any contents or web-based resources found on those third-party sites and is not responsible or liable for the availability thereof or the content, advertising, products or other materials thereon or any updates or changes thereto. Splunk is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement by Splunk of any linked sites. Splunk shall not be responsible or liable, directly or indirectly, for any damage or loss incurred or suffered by any user in connection therewith. Your access and use of those websites, including your use of any content, information, data, advertising, products, or other materials on or available through such websites, is solely at your own risk is subject to the terms and conditions of use and privacy policy(ies) applicable to such sites and resources. The Splunk Privacy Policy is applicable only when you are on the Site. Once you choose to be directed to another website, you should read that website's privacy statement before disclosing any personal data.

9. DISCLAIMER OF WARRANTIES

YOUR USE OF THE SITE IS AT YOUR OWN RISK. THE SITE AND ANY CONTENT, INFORMATION, PRODUCTS OR SERVICES MADE AVAILABLE ON OR THROUGH THE SITE ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTY OF ANY KIND. SPLUNK AND/OR ITS SUPPLIERS AND LICENSORS HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS SITE OR ANY INFORMATION, CONTENT, PRODUCTS OR SERVICES CONTAINED THEREIN, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. SPECIFICALLY, SPLUNK MAKES NO WARRANTY THAT (I) THE SITE WILL MEET YOUR REQUIREMENTS, (II) YOUR ACCESS TO THE SITE WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE, (III) THE QUALITY OF ANY CONTENT, PRODUCTS, SERVICES, INFORMATION OR OTHER MATERIAL OBTAINED THROUGH THE SITE WILL MEET YOUR EXPECTATIONS, AND (IV) ANY ERRORS IN THE SOFTWARE WILL BE CORRECTED. THE SITE, THE PRODUCTS AND SERVICES AVAILABLE THROUGH THE SITE AND THE INFORMATION, CONTENT, SOFTWARE, DOCUMENTS, AND RELATED GRAPHICS PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES, ERRORS, OR OMISSIONS. THE DISCLAIMERS OF WARRANTY AND LIMITATIONS OF LIABILITY APPLY, WITHOUT LIMITATION, TO ANY DAMAGES OR INJURY CAUSED BY THE FAILURE OF PERFORMANCE, ERROR, OMISSION, INTERRUPTION, DELETION, DEFECT, DELAY IN OPERATION OR TRANSMISSION, COMPUTER VIRUS, COMMUNICATION LINE FAILURE, THEFT OR DESTRUCTION OR UNAUTHORIZED ACCESS TO, ALTERATION OF OR USE OF ANY ASSET, WHETHER ARISING OUT OF BREACH OF CONTRACT, TORTIOUS BEHAVIOR, NEGLIGENCE OR ANY OTHER COURSE OF ACTION BY SPLUNK.

10. LIMITATION OF LIABILITY

IN NO EVENT SHALL SPLUNK AND/OR ITS SUPPLIERS/LICENSORS AND ITS AND THEIR OFFICERS, DIRECTORS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING OUT OF OR IN CONNECTION WITH YOUR USE OF THE SITE OR THESE TERMS INCLUDING, WITHOUT LIMITATION, ANY DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS OR OTHER INTANGIBLES, USE OF PERSONAL OR CONFIDENTIAL DATA, LOSS OF SECURITY OF INFORMATION YOU HAVE PROVIDED IN CONNECTION WITH YOUR USE OF THE SITE (HOWEVER ARISING, INCLUDING CONTRACT, EQUITY, NEGLIGENCE OR OTHER TORTIOUS ACTION) EVEN IF ADVISED IN ADVANCE OF SUCH DAMAGES OR LOSSES. THE MAXIMUM LIABILITY OF SPLUNK AND ITS OFFICERS, DIRECTORS, EMPLOYEES, AND LICENSORS/SUPPLIERS TO YOU OR ANY THIRD PARTIES IN ANY CIRCUMSTANCE SHALL BE THE TOTAL AMOUNT, IF ANY, PAID BY YOU TO SPLUNK TO ACCESS AND USE THE SITE. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

11. RELEASE

In the event that you have a dispute with one or more Site users, you release Splunk (and our officers, directors, agents and employees) from claims, demands and damages (actual and consequential) of every kind and nature, known and unknown, suspected and unsuspected, disclosed and undisclosed, arising out of or in any way connected with such disputes. If you are a California resident, you waive California Civil Code 1542, which says: "A general release does not extend to claims that the creditor or releasing party does not know or suspect to exist in his or her favor at the time of executing the release and that, if known by him or her, would have materially affected his or her settlement with the debtor or released party."

12. INDEMNITY

To the fullest extent permitted by law, you shall indemnify, defend and hold harmless Splunk, its licensors/suppliers and their respective officers, directors, employees and agents from any and all claims (including without limitation any proceeding, investigation or claim by a self-regulatory organization, state or federal securities agency or commission), demands, damages, costs and liabilities, including reasonable attorneys' fees, arising out of or in connection with: (1) any of your Contributions, including an assertion that the information, content, or other materials or services provided or made available by you or the use thereof, may infringe any copyright, trademark, or other intellectual property rights of any individual or entity, invade the privacy rights of any

individual, or misappropriate any individual or entity's trade secret, or contain any libelous, defamatory, disparaging, pornographic, or obscene materials; (2) any breach by you of your obligations under these Terms including the Rules of Conduct set forth in Section 7; (3) your unlawful and/or unauthorized use of, or activities in connection with this Site. The foregoing indemnities shall survive expiration or termination of these Terms.

13. TERMINATION

Splunk may, in its sole discretion, at any time for any reason or no reason, terminate your access to this Site and any account(s) you may have in connection with this Site, including if Splunk believes that you have violated or acted inconsistently with the letter or spirit of these Terms or if it is required by applicable law, regulation, court or governing agency order.

This termination may be effected without notice and, on such termination, we may immediately deactivate your account and/or bar any further access to such files, and your right to use the Site will immediately cease. Splunk shall not be liable to you or any third party for any termination of your access to the Site or account hereunder.

14. CLAIMS OF COPYRIGHT INFRINGEMENT

Splunk respects the intellectual property rights of others and asks that you do the same. The Digital Millennium Copyright Act (the "DMCA") provides recourse for copyright owners who believe that material appearing on the Internet infringes their rights under U.S. copyright law. If you believe in good faith that materials available on the Site infringe your copyright, you (or your agent) may send Splunk a notice requesting that we remove the material or block access to it. If you believe in good faith that someone has wrongly filed a notice of copyright infringement against you, the DMCA permits you to send Splunk a counter-notice. Notices and counter-notices must meet the then-current statutory requirements imposed by the DMCA. See <http://www.copyright.gov/> for details. Notices and counter-notices should be sent to:

Copyright Agent
Splunk Inc.
250 Brannan St
San Francisco, CA 94107
dmca@splunk.com
+1 415.848.8400

We encourage you to consult your legal advisor before filing a notice or counter-notice.

15. FORWARD-LOOKING STATEMENTS

Some of the information on this Site may contain projections or other forward-looking statements regarding future events or the future financial performance of Splunk. We wish to caution you that these statements are only predictions and actual events or results may differ materially. Such statements include those that (a) use the words “believes,” “expects,” “anticipates,” “estimates” or words of similar importance or meaning; (b) are specifically identified as forward-looking; (c) describe any of Splunk’s plans, objectives or goals for future operations and products; or (d) concern the characteristics and growth of Splunk’s markets or customers or Splunk’s expected liquidity and capital resources. Factors that could cause actual results to differ materially include economic, competitive, governmental and technological influences affecting Splunk’s operations, markets, products, services and prices. Further information on potential factors that could affect the actual financial results of Splunk are included in Splunk’s filings with the Securities and Exchange Commission; specifically, Splunk’s most recent reports on Form 10-K and Form 10-Q. Splunk does not assume any obligation to update any forward-looking statement to reflect events that occur or circumstances that exist after the date on which they were made.

16. GENERAL

These Terms constitute the entire agreement between you and Splunk with respect to your use of this Site and supersede all prior or contemporaneous communications and proposals, whether electronic, oral or written, between you and Splunk with respect to this Site. These Terms and the relationship between you and Splunk shall be governed by the laws of the State of California without regard to its conflict of law provisions and you shall submit to the personal and exclusive jurisdiction of the courts located within the county of San Francisco, California. If any provision of these Terms is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties’ intentions as reflected in the provision, and the other provisions of these Terms remain in full force and effect. A party may only waive its rights under these Terms, by a written document executed by both parties. Any failure to enforce any provision of these Terms shall not constitute a waiver thereof or of any other provision hereof. You may not assign, transfer or sublicense any or all of your rights or obligations under these Terms without Splunk’s express prior written consent. No provision of these Terms is intended for the benefit of any third party, and the parties do not intend that any provision should be enforceable by a third party either under the Contracts (Rights of Third Parties) Act 1999 or otherwise.

17. FORCE MAJEURE

Neither party or its affiliates, subsidiaries, officers, directors, employees, agents, partners and licensors will (except for the obligation to make any payments) be liable for any delay or failure to perform any obligation under these Terms where the delay or failure results from any cause beyond their reasonable control, including, without limitation, acts of God, epidemics, labor disputes or other industrial disturbances, electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockades, embargoes, riots, acts or orders of government, acts of terrorism, or war.

18. CONTACT; NOTICES

If you have any general question, comment or complaint regarding the Site, please send an e-mail to sitefeedback@splunk.com. Formal notices to Splunk under these Terms (including a report of any violation of these Terms by any user) shall be sufficient only if in writing and transmitted via personal delivery or delivered by a major commercial rapid delivery courier service or by certified or registered mail, return receipt requested, to: Splunk Inc., Attention: Legal Department, 250 Brannan Street, San Francisco, California 94107, with a copy to legal@splunk.com. Notices to you may be made via posting to the Site, by email, or by regular mail, in Splunk's discretion. Without limitation, you agree that a printed version of these Terms and of any notice given in electronic form shall be admissible in judicial or administrative proceedings based upon or relating to these Terms to the same extent and subject to the same conditions as other business documents and records originally generated and maintained in printed form.

SERVICE SPECIFIC RULES: SPLUNK SEARCH POWERED BY AI ("AI SEARCH")

Your use of the AI Search services is considered part of the Site and is governed by the Splunk Website Terms and Conditions of Use ("Website Ts&Cs") and these Service-Specific Rules.

For the avoidance of doubt, the AI Search services are considered part of the "Content" under the Website Ts&Cs. Any text, instructions, content, information or other materials you input into the AI Search services ("Inputs") are owned by you but are deemed "Contributions" under the Website Ts&Cs. As the AI Search services primarily summarize, search and create content from Splunk-originated source documents, any content, information, materials, recommendations or other outputs generated by the AI Search services based on your Inputs ("Outputs") is Content under the Website Ts&Cs and owned by Splunk.

The AI Search services uses generative artificial intelligence ("genAI"). Outputs may not be unique and other users of AI Search may generate the same or similar output. As a genAI system, the AI Search services may hallucinate, provide inaccurate, incomplete or irrelevant information, generate Outputs that are harmful or that are not fit for use (including from a legal and/or business perspective). Splunk does not offer any representation or warranties, express or implied, that Outputs are accurate or free from error or bias. You should independently evaluate, through human review, the Outputs, including to make sure that such Outputs are accurate, lawful, and otherwise appropriate and permissible under the Website Ts&Cs and that you have adequate rights to use such Outputs, before relying on them. You shall ensure that your use of any Output does not violate the intellectual property or proprietary rights of Splunk or any third party.

In addition to the "Rules of Conduct" section of the Website Ts&Cs, you must not include any sensitive or confidential information in any Input. As specified in the Website Ts&Cs we do not guarantee the confidentiality or security of any Input you may input into AI Search or Outputs. AI Search may include safety features to block harmful content, such as content that violates the "Rules of Conduct" section of the Website Ts&Cs. You may not attempt to bypass these protective measures or use content that violates these Service-Specific Rules. You may not use AI Search to develop machine learning models, related technology, or to create any competing products or services.

The AI Search services may not be used for medical, legal, financial, or other professional advice. Any Outputs regarding those topics should not be relied upon. You must not use any Output relating to a person for any purpose that could have a legal or material impact on that person, such as making credit, educational, employment, housing, insurance, legal, medical, or other important decisions about them.

For the avoidance of doubt, the "Rules of Conduct," "Disclaimer of Warranties," "Limitation of Liability," and "Indemnity" sections of the Website Ts&Cs applies to your use of AI Search services. Furthermore, by using the AI Services you agree to defend, indemnify and hold harmless Splunk from and against any claims, causes of action, demands, recoveries, losses, damages, fines, penalties or other costs or expenses arising from or in connection with your use of the AI Search services, including arising from or in connection with Outputs.

EXHIBIT F Splunk Cookie Policy

Splunk Cookie Statement (“Cookie Policy”)

Updated: March 2024

Splunk Inc. and our subsidiaries (collectively, “Splunk”) created this Cookie Policy to help you learn about how we use browser cookies, web beacons, tags, and other web analytics or identifying technologies (collectively, “Cookies”) when you interact with us on our websites (“Services”).

As we explain below, we use Cookies to receive and store certain types of information whenever you interact with us to improve our performance, distinguish you from other users, and enhance your user experience.

You can manage the Cookies that Splunk uses (including disabling them if you choose) by following the instructions in [How to Select or Change Cookie Preferences](#).

What Are Cookies?

Cookies are small text files that are sent to and stored on your browser, mobile device, or computer hard drive (but do not access its contents) when you visit our Services. They contain information that may identify you, your devices, or your preferences whenever you return to our Services.

Web beacons (also known as clear gifs, page tags, or pixel tags) are tiny graphics with a unique identifier that help us deliver or communicate with Cookies, track, and measure Service performance, and evaluate the effectiveness of marketing campaigns. Web beacons are typically embedded invisibly on web pages or in an email.

How Splunk Uses Cookies

Splunk uses Cookies on our Services (with your consent, where required) for security and online tracking purposes, to facilitate navigation, better display information, monitor the success of our Services and ad campaigns, and deliver more relevant advertising throughout your online experience. We also use Cookies to gather information about your use of the Services. We do this to improve the user experience and the design and functionality of our Services. Sections of our websites are deployed on third-party platforms, and those platforms may use cookies.

Cookies Used on Splunk Services

A summary of cookies used on Splunk Services is outlined below. For a detailed list of the Cookies used on our Services (including first and third party Cookies), please consult our Cookie Policy Appendix.

1. STRICTLY NECESSARY COOKIES

Strictly Necessary Cookies allow you to move around our Services more freely and securely. For example, they collect session ID and user authentication information, which allows registered users to perform multiple actions within the same Service visit without having to repeatedly re-enter log-in details each time they navigate to a new webpage or perform a new function. These Cookies also help ensure that you can access registered user-only pages, load web pages faster, and improve overall Service performance, like being able to easily share content. These Cookies also help to verify compliance with our terms and conditions. We do not gather information about you that could be used for marketing or advertising purposes or remember where you have been on the internet. We set the applicable Strictly Necessary Cookies when you visit our Services because you will not be able to use our Services properly without them. As a result, these cookies cannot be disabled and are enabled by default regardless of location.

2. PERFORMANCE COOKIES

Performance Cookies track how individuals use our Services, such as counting the number of visitors, how individuals use or move around our Services (e.g., which pages they visit and for how long), what items they select, how they navigate to and within them, and whether they experience any errors. The information collected by these Cookies is used to help us improve our Services, better understand user interests, and measure the effectiveness of our advertising generally. We may also use Performance Cookies to help perform market research and revenue tracking, and to optimize functionality. If you do not enable or disable these Cookies, we will not be able to learn how you use our Services in order to improve them.

3. FUNCTIONAL COOKIES

Functional Cookies allow us to manage and control variations of Services and provide enhanced functionality, like being able to watch a video, comment on a blog, or notify you of updates you have requested. Splunk also uses Functional Cookies to collect information regarding your preferences on our Services, including your preferences for language, currency, text size, fonts, and any other parts of our Services that are customizable. If you do not enable or disable these Cookies, we will not be able to remember your Service preferences, and you will have to reset them each time you visit.

4. ADVERTISING COOKIES

Like many companies, Splunk uses Cookies to track the efficiency of our online advertising campaigns and marketing communications, and to deliver advertisements that are relevant to you. These Cookies include ad tracking functionality that collects data about when you visit our Services, including what advertisements you view and how you interact with them. They may also track your

internet journey beyond our Services so that we may present you with Splunk advertisements when you navigate to other websites. If you do not enable or disable these Cookies, you may still receive advertisements, but they won't be tailored to your interests.

How to Select or Change Cookie Preferences

If you have browser Cookies enabled and you visit one of our Services, we may store one or more browser Cookies on your computer or device to remember you for the next time you visit. These Cookies do not persist and eventually expire; however, you can update your Cookie settings to delete them before they expire by deleting your browser Cookies using your internet browser settings.

If you do not want to accept browser Cookies, you may in some cases simply configure your browser settings so that your browser declines them automatically or gives you the choice of declining or accepting them from a Service. You may also want to "limit ad tracking" by configuring your settings on your mobile device directly.

In addition, Splunk websites recognize the Global Privacy Control (GPC) signal available in some web browsers. For more information on the GPC and how to use a browser or browser extension incorporating the GPC signal, see <https://globalprivacycontrol.org/>.

We also provide a Cookie Preference Center where you can Customize the different categories of browser Cookies described above or change previously selected choices.

If you reject browser Cookies, our Services may be disabled, their functionality may be impaired, and we may not be able to send you relevant communications or advertising. You will continue to receive advertisements from third parties (and possibly even from Splunk) but they would not be customized to reflect your interests in Splunk.

Strictly Necessary Cookies cannot be disabled via the Privacy Preference Center because these Cookies are necessary for the Services to function. If your browser rejects Strictly Necessary Cookies, you may not be able to log in, download materials and products, or use single sign-on to access the Splunk support portal, partner portal, or Splunk Answers sections of our website, among other Services.

For more on how to disable or block Cookies from your browser or mobile device see AllAboutCookies.org or YourOnlineChoices.eu.

Third-party Providers and Their Services

With your consent, where required, we may use third party services to deliver targeted communications to you during your online experience. We set out a detailed list of those additional third-party tools in our [Cookie Policy Appendix](#), including a summary of how they work.

We work with these third parties to deliver targeted communications to you and others who visit their platforms and who may be interested in our Services. If you don't want to receive these communications, you should update your ad preferences with the third-party platform in addition to adjusting your cookie preferences as described above.

If you do not change your ad preferences with the third-party platform, you may still see our non-targeted advertisements while you are online if your interest settings on such third-party platforms are aligned to an audience segment (pre-defined by the third-party platforms) associated with our business. We do not control whether these ads are displayed to you. Please see the relevant links in our [Cookie Policy Appendix](#) to learn more and manage ad settings.

Likewise, we have no control over, and are not responsible for, the Cookies, tracking technologies, or advertising processes of third-party providers that you may visit, including the use of any of our partners or advertising affiliates. If you would like more information about the Cookies used on third-party services, or if you would like to disable Cookies from any third-party service, please refer to the privacy policy or cookie information provided by the relevant third-party service.

Updates to This Cookie Policy

We may change this Cookie Policy from time to time. Please look at the "Updated" legend at the top of this page to see when this Cookie Policy was last revised. Your acceptance of Cookies following the "Updated" date means that you accept the Cookie Policy as revised as of that date.

Contact Splunk

If you have any questions or comments about this Cookie Policy, you can contact us at any time at dpo@splunk.com or by mail as provided below:

Please note that email communications are not always secure, so please do not include any sensitive information in your emails to us.

Splunk Inc.
Office of the Data Protection
Officer
250 Brannan Street
San Francisco, CA 94107

Splunk Services UK Limited
Office of the Data
Protection Officer
Brunel Building
1 & 2 Canalside Walk
London W2 1DG
England

SplunkServices
Germany GmbH
Office of the Data Protection
Officer
Mies-van-der-Rohe-Straße 6
80807
München
Germany

EXHIBIT G
Splunk Cloud Platform Security Exhibit

SPLUNK CLOUD PLATFORM SECURITY EXHIBIT

This Splunk Cloud Platform Security Exhibit (CSE) sets forth the administrative, technical and physical safeguards Splunk takes to protect Confidential Information, including Customer Content, in Splunk Cloud Platform (Security Program). Splunk may update this CSE 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 CSE is made a part of your Splunk General Terms (Agreement) with Splunk 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 CSE, this CSE will control. This CSE does not apply to Splunk Cloud Platform subscriptions purchased or acquired through Splunk.com, including without limitation Trial or Beta Services , or to on-premise component(s) of hybrid offerings.

1. Purpose

1.1 This CSE describes the information security standards that Splunk maintains to protect Confidential Information, including Customer Content, in addition to any requirements set forth in the Agreement.

1.2 The CSE is designed to protect the confidentiality, integrity and availability of Confidential Information, including 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 designed to protect the confidentiality, integrity and availability of Confidential Information, including Customer Content; and (c) is appropriate to the nature, size and complexity of Splunk's business operations.

2.2 Security Policies, Standards and Methods. Splunk maintains security policies, standards and methods (collectively, Security Policies) designed to safeguard the processing of Confidential Information, including Customer Content, by employees and contractors in accordance with this CSE.

2.3 Security Program Office. Splunk's Chief Information Security Officer (CISO) leads Splunk's Security Program and the CISO Office develops, reviews and approves, together with appropriate stakeholders, 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 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 & 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 manages cybersecurity risks in accordance with its Risk Assessment Method, which defines how Splunk identifies, prioritizes and manages risks to its information assets and the likelihood and impact of them occurring.

3.2 Splunk management reviews documented risks to understand their potential impact to the business, determine appropriate risk levels and treatment options. Mitigation plans are implemented to address material risks to business operations, including data protection.

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 Platform 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 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, if a 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 CSE 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 audits are performed as part of our certification process (further below) to validate the ongoing governance of control operations and their 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 to critical systems 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 Authorized users are required to change passwords at pre-defined intervals consistent with industry standards.

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

8.4 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 (currently, TLS 1.2+) 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 discovered internally through vulnerability scans, offensive exercises (red team), and employees; or externally reported by vendors, researchers or others.

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 An external vendor conducts security penetration tests on the corporate and Splunk Cloud Platform environments annually to detect network and application security vulnerabilities. Findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation based on severity level. In addition, Splunk conducts internal penetration tests quarterly on its Splunk Cloud Platform infrastructure and remediates findings as appropriate.

11. Logging and Monitoring

11.1 Monitoring tools and services are used to monitor systems across Splunk for application, infrastructure, network and storage events, performance and utilization

11.2 Event data is aggregated and stored using appropriate security measures designed to prevent tampering. Logs are stored in accordance with Splunk's data retention policy.

11.3 The Splunk Security Team continuously reviews alerts and follows up on suspicious events as appropriate.

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 and minor product releases, Splunk uses a risk-based approach when applying its standard SDLC methodology, which includes such things as performing security architecture reviews, open source security scans, code review, dynamic application security testing, network vulnerability scans and external penetration testing. 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 Users must authenticate with two-factor authentication prior to accessing Splunk networks containing Customer Content.

14. Vendor Security

14.1 Splunk conducts security due diligence and risk assessments of its vendors prior to onboarding and thereafter manages vendor security through its risk management program.

14.2 Splunk management reviews the documented risks associated with vendors to understand the potential impact to the business. Mitigation plans are implemented to address material risks to business operations, including data protection.

14.3 Splunk's agreements with vendors impose security obligations on them which are necessary for Splunk to maintain its security posture as set forth in this CSE. Confidential Information is shared only with those who are subject to appropriate confidentiality terms with Splunk.

14.4 Splunk uses a risk-based approach to monitor vendor security practices and compliance with their agreements with Splunk.

15. Physical Security

15.1 Splunk grants physical access to Splunk facilities (including Splunk-operated data centers where applicable) based on role. Splunk removes physical access when access is no longer required, including upon termination.

15.2 Employees and visitors must visibly display and wear, identity badges when in Splunk facilities. Visitors must always be accompanied. Splunk logs visitor access to Splunk facilities.

15.3 Splunk reviews data center physical access, including remote access, on a quarterly basis to confirm that access is restricted to authorized personnel.

15.4 Splunk employs additional measures to protect its employees and assets, including video surveillance systems, onsite security personnel, and such other technologies deemed industry best practice.

16. Disaster Recovery Plan

16.1 Splunk has a written Disaster Recovery Plan to manage significant disruptions to Splunk Cloud Platform 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 Splunk Cloud Platform 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 Confidential Information, including 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.

17.5 Splunk retains Customer Content stored in its cloud computing services for at least thirty (30) days after the expiration or termination of the Agreement.

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 Confidential Information, including Customer Content, in accordance with relevant laws and regulations. The background checks are commensurate to an individual's job duties.

19. CSE Proof of Compliance

19.1 Splunk Cloud Platform Standard: Security Audits. At least once a year, Splunk Cloud Platform (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 Cloud Platform 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 Platform Premium: Security Audits. For Splunk Cloud Platform 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 Platform 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 and data breach notification requirements 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 H
Splunk Cloud Service Level Schedule

SPLUNK CLOUD SERVICE
SERVICE LEVEL SCHEDULE *

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-platform-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 for how 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 I Splunk Support Policy

Splunk Support Policy

Splunk Inc. provides Support Services for Purchased Offerings as set forth in the [Splunk General Terms](#) to Customers or applicable Partner Agreement to Partners (Partner to be defined as a “Customer” herein), with active subscriptions to a [Support Program](#). All defined terms in the [Splunk General Terms](#) or Partner Agreement apply here as well. Purchased Offerings may comprise either or both On-Premise Products (“Products”) and Hosted Services Offerings (“Services”). This Policy details the timelines during which specific Product versions are eligible for Support Services, as well as other policies that determine eligibility of both Products and Services for Support Services.

Product Version Numbering

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

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

Product Supported Version Timelines

Any given Product version is considered a Supported Version (“Supported”) for a finite period following its release. The particular timelines for each Product are detailed below for all recent Product versions. Note that any prior version of any of these Products not listed here is no longer supported.

Support includes support for any version of commercial third-party components shipped with a Supported Version of a given Product, even if a particular version of a commercial third-party component has been deprecated or marked as end of life/support by the source developer or entity. Once a Product version is no longer supported, it is considered End of Support. End of Support Product versions are not eligible for Support Services, and any software, associated product documentation,

and Splunk Extensions that are not compatible with Supported Versions will no longer be available to Customers.

Splunk Core Products

Splunk Enterprise (Version 7.0 Onward)

Splunk Light (Version 7.x Only)

Splunk Analytics for Hadoop

Splunk Data Fabric Search

Splunk Data Stream Processor

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

Splunk Enterprise & Splunk Light (Version 6.x Only)

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

Splunk Universal Forwarder (Version 7.0 Onward)

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

Splunk Universal Forwarder (Version 6.x Only)

Each minor version of Splunk Universal Forwarder version 6.x was Supported from release of that minor version through the October 22, 2019 release of Splunk Universal Forwarder 8.0.

Universal Forwarder versions 6.3 through 6.6 only will be Supported at the P3 level through the June 4, 2021 End of Support of Universal Forwarder 7.3. All minor versions of Splunk Universal Forwarder prior to version 6.3 have reached End of Support.

Security Products

Splunk Enterprise Security

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

Splunk SOAR

Starting with version 4.10, each minor version of Splunk SOAR is supported for twenty-four (24) months from the release of that minor version.

Splunk User Behavioral Analytics

Starting with version 5.1, each minor version of Splunk User Behavior Analytics is supported for twenty-four (24) months from the release of that minor version.

Splunk Intelligence Management (TruSTAR legacy system)

Splunk support for the TruSTAR legacy system (including, the [TruSTAR platform](#), [TruSTAR Unified App](#), and [TruSTAR App for SOAR](#)) will end on June 30, 2025 (unless specified otherwise in customer's terms). Splunk [Threat Intelligence Management](#) functionality is now regionally accessible by eligible customers within [Mission Control](#) as an integrated service of [Enterprise Security](#).

Splunk® Security for SAP® solutions

"Splunk Security for SAP solutions" includes Splunk components "Splunk Security App for SAP solutions" and "Splunk Security Add-on SAP solutions". "Splunk Security Add-on SAP solutions" includes the following SAP components ("SAP Components"):

- SAP Enterprise Threat Detection (ETD) - OEM, and
- SAP HANA, Runtime edition for Applications & SAP BW - New/Subsequent partial

Support for Splunk Security for SAP solutions is supported for twenty-four (24) months (from the release of that minor version). The support for SAP components will end after twenty-four (24) months OR on Mar 31, 2026 whichever date comes earlier.

IT Products

Splunk IT Service Intelligence

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

Supported Splunk Extensions

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

Purchased Offering Support Services Policies

Unsupported Customers and Offerings

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

Unsupported Splunk and Third Party Extensions

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

Support for Multiple Offerings

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

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

Operating System Support Status

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

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

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

is required to receive those product defects and/or security fixes, Customers must have that active support subscription to be eligible for the above described P4 level Support Services.

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

- a. The End of Support of that Universal Forwarder minor version, per the standard timelines for that version, or
- b. The end of Customer’s active subscription to the applicable vendor support offering, or
- c. (12) twelve months from the vendor-declared end of life of that operating system version, even if the vendor continues to offer support programs for that operating system version beyond that date.

Japanese language technical support for Splunk Cloud Platform

Customers can purchase Japanese language support as an add on to their Splunk Cloud Platform Standard support contract. Once purchased, technical support in Japanese will cover P2, P3 and P4 issues and will be available during normal business hours of 9AM to 5PM Japan Standard Time on business days. For P2, P3 and P4 technical support issues outside of normal business hours, support will default to the English language.

All P1 issues, at all times, will default to the English language to ensure quick response and round the clock incident management.

Service levels for Japanese language support will follow the underlying support plan and can be found [here](#). Japanese language support is available only for Splunk Cloud Platform and only for technical support issues. Issues not related to technical support (*Example: Change requests, Entitlement queries etc.*) will be answered in English only.

Core

Splunk Enterprise / Splunk Analytics for Hadoop / Splunk Light*

Version	Release Date	End of Support Date	End of Support Criteria
6.0	Oct 1 2013	Oct 22 2019	Splunk Enterprise 8.0 Release

Version	Release Date	End of Support Date	End of Support Criteria
6.1	May 6 2014	Oct 22 2019	Splunk Enterprise 8.0 Release
6.2	Oct 7 2014	Oct 22 2019	Splunk Enterprise 8.0 Release
6.3	Sept 22 2015	Oct 22 2019	Splunk Enterprise 8.0 Release
6.4	Apr 5 2016	Oct 22 2019	Splunk Enterprise 8.0 Release
6.5	Sept 27 2016	Oct 22 2019	Splunk Enterprise 8.0 Release
6.6**	May 2 2017	Jan 31 2020	Splunk Enterprise 8.0 Release
7.0**	Sept 26 2017	Jan 31 2020	24 Months
7.1**	Apr 24 2018	Oct 31 2020	24 Months
7.2***	Oct 2 2018	April 30 2021	24 Months
7.3****	June 4 2019	Oct 22 2021	24 Months
8.0	Oct 22 2019	Oct 22 2021	24 Months
8.1*****	Oct 19 2020	Apr 19 2023	24 Months

Version	Release Date	End of Support Date	End of Support Criteria
8.2*****	May 12 2021	Sep 30 2023	24 Months
9.0	Jun 14 2022	Jun 14 2024	24 Months
9.1	Jun 28 2023	Jun 28 2025	24 Months
9.2	Jan 31 2024	Jan 31 2026	24 Months

*Splunk Light EOL applies only for 6.0 - 7.3 The last minor version released and corresponding End of Support Date for Splunk Light is Version 7.3

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

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

****A Limited Support phase is being provided for Splunk Enterprise 7.3 from the End of Support date through Oct 22, 2021

*****The End of Support Date for Splunk Enterprise 8.1 has been extended to April 19 2023.

*****The End of Support Date for Splunk Enterprise 8.2 has been extended to September 30, 2023.

Splunk Universal Forwarder

Version	Release Date	End of Support Date	End of P3 Support Date
6.0	Oct 1 2013	Oct 22 2019	Oct 22, 2019
6.1	May 6 2014	Oct 22 2019	Oct 22, 2019

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

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

Version	Release Date	End of Support Date	End of P3 Support Date
8.0	Oct 22 2019	Oct 22 2021	24 Months Oct 22 2024 36 Months
8.1***	Oct 19 2020	Apr 19 2023	24 Months Oct 22 2025 36 Months
8.2****	May 12 2021	Sep 30 2023	24 Months May 12 2026 36 Months
9.0	Jun 14 2022	Jun 14 2024	24 Months Jun 14 2027 36 Months
9.1	Jun 28 2023	Jun 28 2025	24 Months Jun 28 2028 36 Months
9.2	Jan 31 2024	Jan 31 2026	24 Months Jan 31 2029 36 Months

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

**The End of Support Date for Splunk Universal Forwarder 7.3 has been extended to Oct 22 2021

***The End of Support Date for Splunk Universal Forwarder 8.1 has been extended to Apr 19, 2023.

****The End of Support Date for Splunk Universal Forwarder 8.2 has been extended to September 30, 2023.

Splunk Data Fabric Search

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

Splunk Data Stream Processor

Version	Release Date	End of Support Date	End of Support Criteria
1.0	Oct 30 2019	Oct 30 2021	24 Months
1.1	May 08 2020	May 08 2022	24 Months
1.2	Oct 30 2020	Oct 30 2022	24 Months
1.3	Mar 30 2022	Jul 01 2023*	See note (*) below
1.4	Feb 28 2023	Feb 28 2025	24 Months

* The End of Support date for Splunk Data Stream Processor (DSP) 1.3 was March 30, 2024. However, all DSP releases prior to DSP 1.4 use Gravity, a Kubernetes orchestrator, which has been announced end-of-life. We have replaced Gravity with an alternative component in DSP 1.4. Therefore, we will no longer provide support for versions of DSP prior to DSP 1.4 after July 1, 2023. We advise all of our customers to upgrade to DSP 1.4 before July 1, 2023 in order to continue to receive full product support from Splunk.

Security

Splunk Enterprise Security

Version	Release Date	End of Support Date	End of Support Criteria
5.0	Feb 20 2018	Feb 20 2020	24 Months
5.1**	May 14 2018	Oct 31 2020	24 Months
5.2	Oct 16 2018	Oct 16 2020	24 Months
5.3	Apr 4 2019	Apr 4 2021	24 Months
6.0	Oct 28 2019	Oct 28 2021	24 Months
6.1	Jan 23 2020	Jan 23 2022	24 Months
6.2	June 4 2020	June 4 2022	24 Months
6.3	Aug 29 2020	Aug 29 2022	24 Months
6.4	Dec 9 2020	Dec 9 2022	24 Months
6.5	Mar 1 2021	Mar 1 2023	24 Months
6.6	June 30 2021	June 30 2023	24 Months
7.0	Dec 16 2021	Dec 16 2023	24 Months

Version	Release Date	End of Support Date	End of Support Criteria
7.1	Jan 11 2023	Jan 11 2025	24 Months
7.2	Sept 7 2023	Sept 7 2025	24 Months
7.3	Dec 14 2023	Dec 14 2025	24 Months

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

Splunk User Behavioral Analytics

Version	Release Date	End of Support Date	End of Support Criteria
4.1	May 24 2018	Oct 16 2019	Release of 5.0
4.2	Oct 16 2018	Jul 28 2022	Release of 5.1
4.3	Mar 26 2019	Feb 15 2023	2nd version after 5.0
5.0	Oct 16 2019	Aug 16 2023	3rd version after 5.0
5.1	Jul 28 2022	Jul 28 2024	24 Months
5.2	Feb 15 2023	Feb 15 2025	24 Months
5.3	Aug 16 2023	Aug 16 2025	24 Months

Version	Release Date	End of Support Date	End of Support Criteria
5.4	May 8 2024	May 8 2026	24 Months

Splunk SOAR

Version	Release Date	End of Support Date	End of Support Criteria
3.5	Feb 22 2018	Sep 21 2021	Release of 5.0
4.0	Sep 3 2018	Sep 21 2021	Release of 5.0
4.1	Oct 1 2018	Sep 21 2021	Release of 5.0
4.2	Jan 30 2019	Sep 21 2021	Release of 5.0
4.5	May 31 2019	Sep 21 2021	Release of 5.0
4.6	Sept 30 2019	Sep 21 2021	Release of 5.0
4.8	Jan 30 2020	Feb 22, 2023	Release of 6.0
4.9	Jun 29 2020	Feb 22, 2023	Release of 6.0
4.10	Dec 9 2020	Dec 9 2022	24 Months
5.0	Sep 21 2021	Sep 21 2023	24 Months
5.1	Nov 11 2021	Nov 11 2023	24 Months
5.2	Jan 26 2022	Jan 26 2024	24 Months

Version	Release Date	End of Support Date	End of Support Criteria
5.3	April 4 2022	April 4 2024	24 Months
5.4	Oct 26 2022	Oct 26 2024	24 Months
5.5	Jan 3 2023	Jan 3 2025	24 Months
6.0	Feb 22 2023	Feb 22 2025	24 Months
6.1	July 12 2023	July 12 2025	24 Months
6.2	Nov 30 2023	Nov 30 2025	24 Months

IT Operations

Splunk IT Service Intelligence

Version	Release Date	End of Support Date	End of Support Criteria
3.0	Oct 20 2017	Oct 20 2019	EOS of Enterprise 7.0
3.1	Apr 24 2018	Apr 24 2020	24 Months
4.0**	Oct 1 2018	Jan 19 2021	24 Months
4.1	Jan 19 2019	Jan 19 2021	24 Months

Version	Release Date	End of Support Date	End of Support Criteria
4.2	April 30 2019	April 30 2021	24 Months
4.3	July 17 2019	July 17 2021	24 Months
4.4	Oct 22 2019	Oct 22 2021	24 Months
4.5	Apr 29 2020	Apr 29 2022	24 Months
4.6	Aug 14 2020	Aug 14 2022	24 Months
4.7	Oct 28 2020	Oct 28 2022	24 Months
4.8	Jan 28 2021	Jan 28 2023	24 Months
4.9	Apr 29 2021	Apr 29 2023	24 Months
4.10	Aug 13 2021	Aug 13 2023	24 Months
4.11	Dec 8 2021	Dec 8 2023	24 Months
4.12	Jan 25 2022	Jan 25 2024	24 Months
4.13	May 16 2022	May 16 2024	24 Months

Version	Release Date	End of Support Date	End of Support Criteria
4.14	Aug 8, 2022	Aug 8, 2024	24 Months
4.15	Nov 15, 2022	Nov 15, 2024	24 Months
4.16	Feb 2, 2023	Feb 2, 2025	24 Months
4.17	Jun 13, 2023	Jun 13, 2025	24 Months
4.18	Jan 23 2024	Jan 23 2026	24 Months
4.19	May 28, 2024	May 28, 2026	24 Months

**The End of Support Date for Splunk IT Service Intelligence 4.0 has been extended to January 19 2021 due to the global impact of COVID-19.

Last Updated: December 2023

EXHIBIT J Splunk Data Processing Addendum

Splunk Data Processing Addendum – US Laws

This Data Processing Addendum ("DPA") is incorporated into and forms part of the Splunk General Terms or such other written or electronic agreement between Splunk and Customer for the purchase of Offerings and any applicable Orders ("Agreement") and is made as of the date of last signature to the Agreement ("DPA Effective Date").

Capitalized terms used but not defined in the body of this DPA or the Agreement are defined in the Definitions section below.

In case of any conflict between the Agreement and the DPA, the DPA will prevail.

This DPA is not available for and does not apply to trial, evaluation, beta, free, donated, test, or development licences of Splunk's products or services. A DPA executed in connection with any such licence will be void.

How and to Whom this DPA Applies

This DPA applies to Splunk as a Service Provider for the Customer, as follows:

1. If the Customer is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. The Customer enters into this DPA on behalf of itself and, to the extent required under applicable law, in the name and on behalf of its Affiliates authorized to use the Offerings under the Agreement (whether or not such Affiliates have executed an Order).
2. If the Customer is an Affiliate authorized to use the Offerings under the Agreement, is not subject to a separate agreement with Splunk, and has executed an Order with a Splunk entity, this DPA is an addendum to that Order and applicable renewal Order.
3. If the Customer is neither a party to the Agreement nor a party to an Order, this DPA is not valid and is not legally binding.

For data not Processed by Splunk as a Controller, see [Splunk's Privacy Policy](#).

Part I – Applicable Terms for Protecting Personal Information

Subject to the Agreement, the below terms apply to all Personal Information regardless of its source of origin.

1. Processing Personal Information

- 1.1 **Roles and Responsibilities.** Splunk is a "service provider" for purposes of the Offerings it provides to Customer pursuant to the Agreement, according to the meaning given to that term under Data Protection Law. Customer is a Business or a Service Provider. Customer grants a general authorization to engage Sub-processors and specifically authorizes: (i) Splunk to appoint any other Splunk Affiliate as a Sub-processor; and (ii) Splunk and any Splunk Affiliate to appoint third-party Sub-processors to support the performance of the Offerings as provided below.
- 1.2 **Splunk Processing Activities.** Splunk agrees that it (and its Sub-processors) will: (i) Process Personal Information only on the specific purpose of performing the Offerings specified in the Agreement with the Customer, unless otherwise agreed or permitted under Data Protection Law, including for a Business Purpose; (ii) ensure that only authorized personnel who are under written obligations of confidentiality have access to such Personal Information; and (iii) take appropriate technical and organizational measures to secure the Personal Information as set out in Section 7 (Technical and Organizational Measures).

Splunk certifies that it will not Sell or Share a Consumer's Personal Information or combine it with Personal Information Splunk receives from, or on behalf of, another person or entity, unless otherwise agreed.

Splunk certifies that it understands the restrictions set out for service providers under Data Protection Law and will comply with them. In the event of Splunk's uncored material breach of Section 1.2 above, Customer retains the right, upon reasonable notice to Splunk, to take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Personal Information by Splunk.
- 1.3 **Customer Processing Activities.** Customer agrees that if it uses the Offerings to submit Personal Information to Splunk, it will: (i) do so in accordance with the requirements of Data Protection Law, including, if applicable, providing notice to Consumers of the use of Splunk; and (ii) provide documented instructions for the Processing of Personal Information that comply with Data Protection Law. Customer will have sole responsibility for the accuracy, quality and legality of Personal Information and the means by which Customer or any relevant third-party acquired Personal Information. Unless specifically identified in an Order, Customer agrees to not transmit or store within the Offerings any data that it is not otherwise entitled to transmit or store under the Agreement.
- 1.4 **Details of Processing Activities.** The nature and extent of Processing Personal Information by Splunk to deliver the Offerings is determined and controlled solely by Customer. Annex I of the Appendix to this DPA sets out the duration,

nature and purpose of the Processing of Personal Information. The categories of Personal Information and Consumers whose Personal Information may be Processed by Splunk are also set out in Annex I.

2. Sub-processing

- 2.1 **Current Sub-processors.** A list of Splunk's current Sub-processors by Offering is at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html.
- 2.2 **New Sub-processors.** To receive advance notification of new Sub-processors added to Offerings, subscribe to Splunk's Data Protection Notification Portal at: https://www.splunk.com/en_us/form/splunk-subprocessor-signup.html ("Advance Notification").
- 2.3 **Obligations of and Liability for Sub-processors.** Splunk requires that any Sub-processor it engages to provide Offerings 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 no less protective of Personal Information than those imposed on Splunk in this DPA. Splunk agrees to be fully liable for the acts or omissions of its third-party Sub-processors to the same extent as Splunk would be liable if performing the Offerings of the Sub-processors under the terms of the Agreement.

3. Consumer Requests

If Splunk receives a Consumer Request from Customer's Consumer, it will promptly notify Customer. Splunk will refrain from responding to the Consumer except to acknowledge receipt of the Consumer Request, to which Customer hereby agrees. Customer can address Consumer Requests within the Offering in accordance with the applicable Documentation. Upon Customer's request, Splunk will provide reasonable assistance to help Customer fulfil a Consumer Request. Splunk reserves the right to charge a mutually agreed fee for assistance rendered upon Customer request. Requests for assistance from Splunk should be made to DPO@splunk.com.

4. Assistance

Splunk will provide 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 or similar privacy assessments required under Data Protection Law; (b) Customer's compliance with its obligations under Data Protection Law with respect to the security of Processing; and (c) any prior consultations required with a regulatory authority.

Requests for assistance from Splunk as provided herein should be made to DPO@splunk.com or such other location as Splunk may make available on its website from time to time.

5. Deletion or Return of Personal Information

Upon termination of the Hosted Service, Customer may at its sole discretion and expense, delete or retrieve Customer Content, including any Personal Information contained therein, from the Hosted Services as provided in the Agreement. For On-Premises Products, Splunk does not Process or store Customer Content, except to the extent it may be included in diagnostic files submitted in connection with Splunk's Support Program, which are deleted in accordance with Splunk's Data Retention Policy at: https://www.splunk.com/en_us/legal/splunk-retention-policy.html. In the event Splunk is required under applicable law to retain Personal Information Processed under this DPA after termination of the Agreement, Splunk will protect the Personal Information as set out in Section 7 (Technical and Organizational Measures).

6. Inspections and Audit

- 6.1 Splunk will contribute to audits requested by Customer, not more than once annually (except in the event of a Personal Information Breach or request from a regulatory authority) to demonstrate Splunk's compliance with its obligations under this DPA by: (i) in the case of Hosted Services, providing to Customer (or Customer's independent third-party auditor that is not a competitor of Splunk) a copy of the relevant and most recent third-party audit reports or certifications, or such other written documentation generally provided by Splunk if the Hosted Services are not audited by a third-party; (ii) in the case of On-Premises Products, providing such information generally provided to similarly situated customers to demonstrate Splunk's compliance with its obligations as a Service Provider; and (iii) such additional information in Splunk's possession or control requested or required by a regulatory authority to demonstrate its compliance with the Personal Information Processing activities carried out by Splunk under this DPA.
- 6.2 If a Customer who purchased Hosted Services is required under Data Protection Law to request any further information to confirm Splunk's compliance with its obligations under this DPA, such additional information (including any on-site inspections) will be provided and/or conducted in accordance with Splunk's fee-based Customer Audit Program. Splunk's Customer Audit Program terms are available upon request by email to DPO@splunk.com. 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 an on-site audit.
- 6.3 Requests or inquiries regarding audit services provided herein should be made to DPO@splunk.com or such other location as Splunk may make available on its website from time to time.

7. Technical and Organizational Measures

Splunk provides the technical and organizational measures required under Data Protection Law for the security of the Personal Information it Processes as set out in the Agreement and Annex II of the Appendix to this DPA.

8. Personal Information Breach

- 8.1 **Personal Information Breach Notification.** Splunk will notify Customer without undue delay after becoming aware of a Personal Information Breach. Where appropriate in respect of any Personal Information which has been the subject of a Personal Information Breach, Splunk will provide reasonable assistance to Customer to the extent required for Customer to comply with Data Protection Law, which may include assistance in notifying Consumers and the relevant regulatory authority, providing a description of the Personal Information Breach, including where possible: (i) the nature of the Personal Information Breach and the categories and approximate number of Consumers and/or Personal Information records concerned; (ii) the name and contact details of Splunk’s data protection officer or other contact point; (iii) a description of (a) the likely consequences of the Personal Information Breach and (b) measures to mitigate its possible adverse effects. If it is not possible to provide the above information simultaneously, additional information will be provided without undue delay as it becomes available.
- 8.2 **Cooperation in case of Personal Information Breach.** If Customer determines that a Personal Information Breach must be notified to a regulatory authority, Consumer, or the public under Data Protection Law, to the extent such notice makes reference to Splunk, whether or not by name, Customer agrees to consult with Splunk in good faith and in advance to consider any clarifications or corrections Splunk may reasonably request to the notification consistent with Data Protection Law.

9. General

- 9.1 Splunk will inform Customer, immediately upon becoming aware, if in Splunk’s opinion any instructions provided by Customer under this DPA infringe Data Protection Law.
- 9.2 Splunk’s aggregate 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, whether liability arises under the Agreement or this DPA.
- 9.3 This DPA will be governed by and construed in accordance with the governing law provisions set out in the Agreement.
- 9.4 Splunk will notify Customer within five (5) business days if it determines that it can no longer meet its obligations under Data Protection Law.

Definitions

Term	Meaning
Agreement	As defined in the preamble.
Business	As defined under Data Protection Law.
Business Purpose	As defined under Data Protection Law.
Consumer	As defined under Data Protection Law.
Consumer Request	As defined under Data Protection Law.
Customer	The party which has entered into the Agreement with Splunk.
Data Protection Law	The California Consumer Privacy Act of 2018, including as amended by the California Privacy Rights Acts, and all legislation revising, pre-empting, or supplementing the foregoing as updated, amended, or replaced from time to time.
Personal Information	All data which is defined as ‘personal information’ or ‘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 Service Provider as part of its provision of the Offerings to a Customer.
Personal Information Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information while being transmitted, stored or otherwise Processed by Splunk.
Process or Processing	As defined under Data Protection Law, as applicable.
Processor	As defined under Data Protection Law.
Revised FADP	The revised version of the Swiss Federal Act on Data Protection of 25 September 2020, which is scheduled to come into force on 1 January 2023.
Sale or Sell	As defined under Data Protection Law.
Service Provider	As defined under Data Protection Law.
Share or Sharing	As defined under Data Protection Law.
Sub-processor	Another Service Provider engaged by Splunk in Processing of Personal Information for a Business Purpose, or in other words, a sub-Service Provider.
US	The United States of America.

[Signature page follows]

The Parties' authorized signatories have duly executed this DPA:

Parties: **SPLUNK**
Name: **Splunk Inc.** (a Delaware corporation)
Address: 250 Brannan Street
San Francisco, CA 94107
United States

CUSTOMER
Account Name
Street
City
State/Province
Country Billing Zip/Postal Code

Signature:

Declassified by:
Amy Solus
F0199082F050472

Signatory Name: Amy Solus
Job Title: VP, Deal Strategy and Execution

APPENDIX

ANNEX I

A. LIST OF PARTIES

1. **Name:** Customer's name, as noted in the introductory paragraph of the DPA

Address: Customer's address, as noted in the introductory paragraph of the DPA

Contact person's name, position and contact details: As determined by the "Notices" section of the Agreement

Activities relevant to the data transferred: Customer determines the subject-matter of the processing and Splunk processes data as required to deliver the Offerings

Role (controller/processor): Business or Service Provider

1. **Name:** Splunk Inc.

Address: 250 Brannan St., San Francisco, CA 94107 U.S.A.

Contact person's name, position and contact details: Splunk Data Protection Officer, DPO@splunk.com

Activities relevant to the data transferred: Processing operations as required to deliver the Offerings to the Customer.

Role (controller/processor): Service Provider

B. DESCRIPTION OF PROCESSING

Categories of Consumers whose Personal Information is Processed

Customer may submit Personal Information to the Offerings, 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 Information relating to the following categories of Consumers:

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

Categories of Personal Information Processed

Customer may submit Personal Information to the Offerings, 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 Information:

- 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
- File and message content

Sensitive Information Processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The Customer and Splunk do not envisage that sensitive categories of Personal Information will be Processed under this Agreement.

The frequency of the Processing.

Continuous.

Nature of the processing

Customer determines the subject-matter, nature and duration of the Processing and Splunk and its Sub-processors Process Personal Information as required to deliver the Offerings.

Purpose(s) of Processing

Customer is requesting, and Splunk will provide, the Offerings to the Customer pursuant to the Agreement.

The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period

Customer determines the retention periods applicable to Customer Content (including any Personal Information therein).

For transfers to Sub-processors, also specify subject matter, nature and duration of the Processing

A current list of data importer's Sub-processors is at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html. Customer determines the subject-matter, nature and duration of the Processing and Splunk's Sub-processors Process Personal Information as required to deliver the Offerings.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the Splunk (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Splunk provides the technical and organizational measures required under Data Protection Law, as defined in the DPA, for the security of the Personal Information it processes as set out in the Agreement. The specific technical and organizational measures are listed in the applicable Security Addenda identified below and may contain, as applicable, measures reasonably designed for:

- Pseudonymisation and encryption of personal information;
- Ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident;
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- User identification and authorization;
- Protection of data during transmission;
- Protection of data during storage;
- Physical security of locations at which personal information are processed;
- Event logging;
- System configuration, including default configuration;
- Internal IT and IT security governance and management;
- Certification / assurance of processes and products;
- Allowing data portability and ensuring erasure.

Splunk's Security Exhibits for specific offerings: https://www.splunk.com/en_us/legal/splunk-security-exhibits.html

Configuration and Implementation Services Information Security Addendum at: <https://www.splunk.com/prof-serv-isa>

Splunk requires that any Sub-processor it engages to provide the Offerings on its behalf in connection with the DPA does so only on the basis of a written contract which imposes on such Sub-processor terms no less protective of Personal Information than those imposed on Splunk in the DPA, including the transfer of Personal Information to a third country or international organization in accordance with Data Protection Law.

A current list of data importer's Sub-processors is at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html.