Splunk Terms for Splunk Offerings

Published:February 2025

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

Specific Offering 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 out in the Splunk Cloud Security Exhibitlocated at https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html ("**Cloud Security Exhibit**").
   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 Exhibit), 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 out 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 out at https://docs.splunk.com/Documentation/SplunkCloud/latest/Service/SplunkCloudservice#Data_policies.

Splunk On-Call

1. **Service Description**
   https://help.victorops.com/
2. **Additional Users**
   If Customer wants to add additional permitted users, Customer can do so through the Offering administrative portal, and either (i) Splunk will immediately charge Customer's credit card for the prorated amount for the current term, or (ii) if Customer does not have a credit card on file, then Splunk will invoice Customer for the additional permitted users in accordance with the General Terms.
3. **Support**
   Splunk On-Call support is provided via the following portal:
   https://help.victorops.com/knowledge-base/how-to-contact-splunk-on-call-support/.
4. **Security of Customer Content**
   Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content on Splunk On-Call as set out in the Splunk On-Call Security Exhibit located at https://www.splunk.com/en_us/legal/splunk-on-call-security-addendum.html ("Splunk On-Call Security Exhibit").
   Customer acknowledges and agrees that Splunk On-Call has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification.
5. **Service Level Schedule**
   Splunk's Splunk On-Call Service Level Schedule, set out at https://www.splunk.com/en_us/legal/splunk-on-call-service-level-schedule.html, will apply to the availability and uptime of the Splunk On-Call service.

Splunk Observability Cloud

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

1. **Service Descriptions**
   https://docs.splunk.com/Observability/
2. **Usage, Subscription Limits Enforcement, and Entitlements**

   https://www.splunk.com/en_us/legal/usage-subscription-limits-enforcement-and-entitlements.html
3. **Security and Protection of Customer Content.**
   - Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content as set out in the Security Exhibit located at https://www.splunk.com/en_us/legal/splunk-observability-security-addendum.html ("**Observability Security Exhibit**"). 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 Observability Security Exhibit), 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.
   - Customer is responsible for using Splunk Observability Cloud in compliance with applicable laws, including but not limited to providing notice to and obtaining any necessary consent from individuals whose data will be collected by Customer's use of the services.
4. **Service Level Schedule – Splunk Observability Cloud**
   Splunk's Splunk Observability Cloud Service Level Schedule, set out at https://www.splunk.com/en_us/legal/observability-service-level-schedule.html, will apply to the availability and uptime of the Splunk Observability Cloud. Customer will be entitled to service credits for downtime in accordance with the applicable Service Level Schedule.
5. **Integration with PCI-DSS-Certified Environments**
   Customer hereby acknowledges that Splunk Observability Cloud is not PCI-DSS-certified. Integrating PCI-DSS-certified platforms with Splunk Observability Cloud may result in exposure of PCI data to non-PCI-certified environments.
6. **Definitions.** The following definitions are applicable to Orders for Splunk Observability Cloud services
   "Analyzed Trace" means a trace that was sent to and processed by Splunk APM.
   "APM Identities" means the count of all unique spans and initiating operations across all service endpoints for metricization. Additional dimensions on these, specified as select span tags, create further APM Identities based on the count of values of those tags.
   "Container" means a stand-alone, executable package of software that includes application software and sufficient operating system libraries to run in isolation but shares the underlying operating system with other Containers.
   "Custom Metric" means any Metric that is not automatically collected and reported as part of Splunk's standard Host-based integrations.
   "Host" means a virtual machine or physical server being monitored.
   "Metric" means any unique combination of a metric name and dimension value reporting data to Splunk within the last hour.
   "Monitoring MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to alert on changes in application performance. A Monitoring MetricSet includes metrics such as request rate, error rate, and latency percentiles.
   "MTS" means Metric Time Series.
   "**Profiled Container**" means a Container that is instrumented to send Profiling data to Splunk APM.
   "**Profiling**" means automated collection and analysis of code behavior data from runtime environments.
   "**Profiling Volume**" means the amount of Profiling data that customers pay for to be ingested by Splunk APM.
   "Serverless Function" means a stand-alone, executable package of single-purpose software that runs in serverless environments and is triggered by an event or message.
   "Session Volume" means the amount of Session data that customers pay for to be ingested by Splunk RUM.
   "Span" means an area of code instrumented to be captured as part of a recorded transaction (eg. rpc, function). Each service can have many spans. At a minimum, there will be 2 spans - inbound and outbound to the service.
   "TAPM" means Trace Analyzed Per Minute.
   "Trace" means an array of spans represented as a Directed Acyclic Graph.
   "Trace Volume" means amount of trace data per minute that customers pay for to be ingested by Splunk APM.
   "Troubleshooting MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to enable detailed analysis and troubleshooting of an application. A Troubleshooting MetricSet includes metrics such as the request rate, error rate, root-cause error rate and latency percentiles.

Splunk Synthetic Monitoring (Legacy Rigor Platform)

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

3. **Usage, Subscription Limits Enforcement, and Entitlements**
   https://www.splunk.com/en_us/legal/usage-subscription-limits-enforcement-and-entitlements.html

Splunk Secure Gateway
Secure Gateway app facilitates communication between mobile devices and Splunk instances with an end-to-end encrypted free cloud service called Spacebridge. Spacebridge cloud service environment, and the service itself, is separate from the Splunk Enterprise and Splunk Cloud offering. Spacebridge is a free Hosted Service and use is subject to Splunk General Terms available at: https://www.splunk.com/en_us/legal/splunk-general-terms.html. See here to learn more about the Spacebridge offering. Learn more
You may not transmit regulated data, including PHI data or PCI data, to Spacebridge unless you are using Spacebridge with a managed Splunk Cloud deployment and have specifically purchased the applicable regulated environment for that managed Splunk Cloud deployment. Spacebridge does not leverage the FIPS 140-2 validated Splunk Cryptographic Module and may not be used in environments that require this standard.
You must agree to use Spacebridge to use Splunk Secure Gateway. If you want to permanently disable the use of Spacebridge, you must disable Splunk Secure Gateway. Disable Splunk Secure Gateway in Apps > Manage Apps. If you're using a managed Splunk Cloud deployment, file a support ticket to disable Splunk Secure Gateway.

SPLUNK SECURITY OFFERINGS

Splunk Asset and Risk Intelligence
1. Security Industry Certifications
   Customer acknowledges and agrees that Splunk Asset and Risk Intelligence has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification.

Splunk Attack Analyzer (TwinWave legacy service)
1. Service Level Schedule
   The Service Level Schedule for the Splunk Attack Analyzer, set out at https://www.splunk.com/en_us/legal/attack-analyzer-service-level-schedule.html , will apply to service availability of the Splunk Attack Analyzer Hosted Service. Customer will be entitled to service credits for downtime in accordance with the Service Level Schedule.
2. Security of Customer Content
   Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content on Splunk Attack Analyzer as set out in the Splunk Attack Analyzer Security Exhibit located at https://www.splunk.com/en_us/legal/splunk-attack-analyzer-security-exhibit.html ("SAA Security Exhibit").

   Customer acknowledges and agrees that Splunk Attack Analyzer has not yet undergone a security audit by an independent third party and therefore does not have SOC2 certification.
3. Use of Customer Content
   The operation and functionality of Splunk Attack Analyzer depends on the continuous improvement of detection capabilities through the application of threat intelligence information that is derived from the data our customers submit to the Splunk Attack Analyzer service. Accordingly, Customer agrees that Splunk may use Customer Content submitted to Splunk Attack Analyzer for purposes of analyzing threat trends, enhancing detection capabilities, and otherwise testing, improving and operating Splunk's products and services, provided that Customer Content will not be disclosed to any third party except in aggregated format and in a manner that does not identify Customer as the source of the Customer Content and could not otherwise be attributable to Customer or any individual. Cisco's Talos Threat Hunting Service may be deployed as part of the Splunk Attack Analyzer service in which case the Cisco Talos team may access Customer Content if such data triggers or is related to a security event. Talos Threat Hunting will process data as set forth in the Threat Hunting Privacy Data Sheet.

Splunk Enterprise Security
1. Threat Data Usage.
   In order to continuously improve and update threat intelligence, threat detection and security event management in our security Offerings, we depend on analysis and use of threat and event data from customers in Splunk's Hosted Service Enterprise Security Offering ("Threat Data"). Accordingly, Customer instructs and grants Splunk the right to extract a copy of Threat Data and use Threat Data for purposes of enhancing detection capabilities, updating threat intelligence, analyzing threat trends, and otherwise testing, improving and operating Splunk's security Offerings, provided that in all cases Splunk's use of Threat Data is subject to Splunk's obligations under this Agreement with respect to Customer Content and Confidential Information, including without limitation Section 6 (Security), Section 15 (Confidentiality), and the DPA. More information about this use is set out in our Documentation at https://docs.splunk.com/Documentation/ES/latest/User/ShareThreatData.
2. Use of Customer Content by Cisco Talos.
   Cisco's Talos Threat Hunting may be deployed as part of the Splunk Enterprise Security service. The Cisco Talos team may access Customer Content if such data triggers or is related to a security event. Talos Threat Hunting will process data as set forth in the Threat Hunting Privacy Data Sheet.

Splunk Intelligence Management (TruSTAR legacy service)
1. **Service Description**
   https://docs.splunk.com/Documentation/SIM/current/User/Intelligenceoverview
2. **Security**
   Customer hereby acknowledges and agrees that Splunk Intelligence Management no longer has SOC2 attestation as audited by an independent third party.

Splunk Security for SAP® solutions

1. **Service Description**
   https://docs.splunk.com/Documentation/SAPSecurity
2. **General Availability**
   License to use Splunk Security for SAP solutions is subject to general availability. In the event this Offering is no longer generally available, Splunk may terminate the Offering and refund to you any prepaid fees covering the unexpired Term.
3. **Monitored Users**
   A "Monitored User" cannot be assigned to more than one (1) individual. However, a Monitored User assignment may be transferred from one (1) individual to another, but only if the individual to which the Monitored User was assigned is:
   - is on vacation;
   - is absent due to sickness;
   - has their employment terminated;
   - is moved into a new job function which no longer requires them to use Splunk Security for SAP solutions; or
   - is subject to a condition that is otherwise agreed by Splunk.
4. **Additional License Restrictions**
   SAP software bundled in the Splunk Security for SAP solution ("SAP Software") can only be used with the Splunk Security for SAP solution for the duration of the subscription term of the license to Splunk Security for SAP solutions. The SAP Software may only be used with Splunk Security for SAP solutions to enable its performance, with data access limited to data created or processed by Splunk Security for SAP solutions. The Splunk Security for SAP solution may only be used with Splunk Enterprise and/or Splunk Cloud Platform.
5. **Restricted Activity**
   You may not distribute or publish keycodes or otherwise endanger the security or operation of Splunk Security for SAP solutions, including the SAP Software, or other materials provided in connection therewith.

   Despite anything to the contrary in the General Terms, You do not have the right to make additional copies of Splunk Security for SAP solutions for archival and back-up purposes.

   SAP Software and related material is Confidential Information. With respect to your use of Splunk Security for SAP solutions, you agree not disclose or reveal any such Confidential Information to any person other than your Affiliates, employees, contractors, legal representatives, accountants, or other professional advisors whose access is necessary to enable you to exercise your rights or perform your obligations under the General Terms and who are under obligations of confidentiality substantially similar to those in the General Terms, including these Specific Terms for Splunk Offerings.
6. **Your responsibilities**
   You are responsible for (i) setting up, installing, configuring and managing the Splunk for SAP solution on any SAP software, and (ii) obtaining internet connectivity. Splunk will not be responsible for loss due to your failure to comply with your responsibilities in this section or for activities that take place in your SAP environment (which shall be governed by your applicable agreement with SAP).
7. **Not for Resale and Evaluation Licenses**
   If Splunk makes available the Splunk Security for SAP solution pursuant to Section 1.4 of the General Terms, the Splunk Security for SAP solution must not be used in production and must be destroyed or deleted when the license terminates. Licenses to Splunk Security for SAP solutions made available under Section 1.4 of the General Terms may be terminated at any time upon written notice from Splunk.
8. **SAP Open Source**
   Applicable specific conditions related to certain open source products made available in SAP Software are part of the applicable product documentation and apply to your use of any such open source products. The SAP Software open source components and their related licenses are documented at https://docs.splunk.com/Documentation/SAPSecAddOn/1.0.0/User/Credits.
9. **SAP Software License Specific Terms**
   Splunk Security for SAP solutions includes SAP Enterprise Threat Detection - OEM and SAP HANA, RTed Appl&BW-new/subsq partial ("SAP Products"). Subject to the license restrictions under the General Terms, including these Specific Terms for Splunk Offerings, SAP products come with additional software usage rights. Such rights can be found in the SAP Software Usage Rights available at https://assets.cdn.sap.com/agreements/oem-agreements/sur/sap-partneredge-build-formerly-oem-software-use-rights-english-v7-2022.pdf. Exercise of any of such additional rights shall be subject to the SAP Software Usage Rights.

Splunk SOAR

Use of Customer Content by Cisco Talos.
Cisco's Talos Threat Hunting may be deployed as part of the Splunk SOAR service. The Cisco Talos team may access Customer Content if such data triggers or is related to a security event. Talos Threat Hunting will process data as set forth in the Threat Hunting Privacy Data Sheet.

HOSTED SERVICES ENVIRONMENT TERMS

FedRAMP or StateRAMP for Splunk Cloud Platform

If you access or use any Hosted Services in the specially isolated Amazon Web Services ("AWS") GovCloud (US) region that are provisioned in a FedRAMP or StateRAMP authorized environment ("Government Cloud"), you acknowledge the Government Cloud is a more restricted environment.

Customer acknowledges that FedRAMP Moderate or StateRAMP Moderate authorized offerings will only meet the standards of an

authorized FedRAMP Moderate or StateRAMP Moderate Hosted Service, respectively, if Customer performs its obligations as set out in both the "FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet" and the "FedRAMP Low or Moderate Customer Responsibility Matrix (CRM) Worksheet" available from Splunk upon request. Customer acknowledges that FedRAMP High authorized offerings will only meet the standards of an authorized FedRAMP High Hosted Service if Customer performs its obligations as set out in the "SSP Appendix J Control Implementation Summary (CIS) and Customer Responsibility Matrix (CRM) Workbook" available from Splunk upon request. To maintain the security of the FedRAMP or StateRAMP authorized offerings, Customer agrees to cooperate with Splunk to remediate any security vulnerabilities upon Splunk's request.

Business Associate Agreement
Splunk will comply with the requirements and obligations in the Splunk Business Associate Agreement set out at https://www.splunk.com/en_us/legal/splunk-baa.html for (i) Hosted Services provisioned in Splunk Cloud Platform's Premium HIPAA environment, as specified in an Order; and (ii) Splunk Observability Cloud.

SPLUNK AI ASSISTANT OFFERINGS

Splunk AI Assistant

1. **Terms**. Your use of a Splunk® AI Assistant ("Assistant") is governed by the Splunk General Terms ("SGT") and these Specific Terms for Splunk Offerings, including those set forth in this Splunk AI Assistant section ("Specific Terms," and the SGT and Specific Terms, "Terms"). By using an Assistant, you agree to be bound by Terms. Unless otherwise noted, an Assistant is a Splunk Extension under the SGT and it is not a "Hosted Service." If you are entering into these Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to the Terms, or do not have the authority to bind Customer, do not use an Assistant. For clarity, these Specific Terms hereby incorporate the SGT terms by reference. **Use of an Assistant is subject to Splunk research and development as outlined in Section 4 below unless you opt out.**

2. **SERVICE DESCRIPTION.** Details relevant to an Assistant vary by the specific use-case specific Assistant You access (each, a "Specific Assistant"). Service Descriptions of each Specific Assistant are available in Assistant Documentation, as defined below. Additional terms and restrictions applicable to your use of each Specific Assistant, including but not limited to license entitlements, Term, service limitations, and compatibility requirements are set forth below and within the relevant Service Descriptions. Assistants are cloud-powered applications that use generative artificial intelligence ("genAI").

3. **PURPOSE AND USE**. When you interact with an Assistant, Splunk will use Inputs, including context data collected as part of the service as further outlined in Assistant Documentation, Outputs and in-product feedback (together, "**AI Service Data**") to provide and maintain the Assistant, comply with applicable law, and enforce our policies. By using an Assistant, you agree to the collection and use of AI Service Data for the purposes stated herein. You hereby grant Splunk a perpetual, irrevocable, worldwide, royalty free, non-exclusive, transferrable, sublicensable (through multiple tiers), fully paid-up license to access and use the AI Service Data for purposes of providing you the Assistant service and as otherwise permitted by these Terms.

4. **CONSENT TO SPLUNK'S RESEARCH AND DEVELOPMENT.** In addition to the uses described in Section 3 above, Splunk may use your AI Service Data to develop and improve an Assistant or for other research and development which may include training our models and creating Updates, as described in this Section 4 ("Research and Development Purposes"). Unless expressly stated otherwise for Specific Assistants, if you do not want your AI Service Data used for Research and Development Purposes, you may opt out of this use of your AI Service Data in the user interface settings. By using an Assistant and not toggling off the collection of AI Service Data for Research and Development Purposes, you agree that, in addition to the rights granted to Splunk in Section 3 above, you also hereby grant Splunk a perpetual, irrevocable, worldwide, royalty free, non-exclusive, transferrable, sublicensable (through multiple tiers), fully paid-up license to use, offer for sale, sell, copy, distribute, perform, display (whether publicly or otherwise), modify, adapt, publish, transmit, commercialize, use as or to develop Updates, create derivative works of, and use the AI Service Data as training data for genAI tools and AI models in any form, medium or technology now known or later developed, and to grant to others rights to do any of the foregoing. You acknowledge and agree that some AI Service Data may be replicated in outputs for third parties who use the AI Offering that has been trained with your AI Service Data and may therefore be disclosed and you consent to the disclosure and use thereof.

   Except for AI Service Data collected for Research and Development Purposes, Inputs and Outputs used to power an Assistant may be removed from the Assistant in accordance with Assistant Documentation. Section 4 of the SGT, subsection titled "Your Responsibility for Data Protection" and Section 13 of the SGT, subsection titled "Third Party Content" shall apply to AI Service Data as if AI Service Data was "Customer Content" for the purpose of these Specific Terms.

   Notwithstanding any election to opt-out of the use of your AI Service Data for Research and Development Purposes as described above, any Feedback you provide relating to an Assistant, as that term is defined in the SGT, may be used by Splunk for Research and Development Purposes.

5. **OWNERSHIP OF INPUTS AND OUTPUTS.**
   As pertinent to your use of an Assistant, as between you and Splunk, Inputs are owned by you. For each Input, you represent and warrant that you have all rights necessary for you to grant the licenses granted in these Terms, and that such Input, and your provision thereof to and through an Assistant, comply with all applicable laws, rules and regulations, and these Terms. Except to the extent noted in Section 4 above, Inputs do not constitute Customer Content for purposes of the SGT.

Outputs, excluding any Pre-existing Splunk Content, are owned by you. You will have the right to access and use the Pre-existing Splunk Content in connection with your applicable Offerings, and those rights will be of the same scope and duration as your rights to the underlying Offering. You also acknowledge and agree that any Outputs may not be protectable under copyright or other intellectual property, proprietary rights, or other law. Splunk makes no warranties or representations, express or implied, that AI Service Data is protectable under any law. As a genAI system, the Assistant 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). You should evaluate the accuracy of any Output as appropriate for your use case, including by using human review of the Output. Except to the extent noted in Section 4 above, Outputs do not constitute Customer Content for purposes of the SGT.

6. **Support**
   For information about the support provided for Assistants, please see https://www.splunk.com/en_us/customer-success/support-programs.html.

7. **RESTRICTIONS AND ACCEPTABLE USE**. You must comply with the Hosted Services acceptable use policy per Section 14 of the SGT as if an Assistant was a Hosted Service. You will comply with all applicable laws in your use of an Assistant, and be responsible for the accuracy, lawful use of, and the means by which you acquired your AI Service Data. You may not, and not allow any user or third party to: (i) use an Assistant in a way that infringes, misappropriates or violates any person's rights; (ii) reverse assemble, reverse compile, decompile, translate or otherwise attempt to discover the source code or underlying components of models, algorithms, and systems of an Assistant; (iii) use an Assistant or any Output from an Assistant to develop or improve models (or other product or service) that are similar to or compete with Splunk or LLM service providers, or to benchmark or to train any other model; (iv) use web scraping, web harvesting, or any other automated or programmatic method to extract data or outputs, including any Personal Data, from an Assistant; (v) represent that Output from an Assistant was human-generated when it is not; (vi) send, upload or transmit to an Assistant any regulated data, including financial data, health data, or Personal Data; (vii) work around any technical limitations in an Assistant or restrictions in Documentation; (ix) install or use any third-party software or technology in a way that would subject an Assistant or any portion thereof to any other license; (x) separate and run parts of any component of an Assistant on more than one device; (xi) upgrade or downgrade part of a component of an Assistant at different times; (xii) transfer part of any component of an Assistant separately, (xiii) use an Assistant or Outputs for legal, financial, or other professional advice use cases, (xiv) 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, or (xv) provide access to third parties not authorized under these Terms or use the Assistant for any purpose not intended by Splunk (as described in these Terms). Excessive use of an Assistant may result in temporary throttling of your access to the Assistant.

8. **NO HAZARDOUS OR MEDICAL USE.** You acknowledge and agree that an Assistant is not designed or intended: (i) to support any use in which a service interruption, defect, error, or other failure of an Assistant could result in the death or serious bodily injury of any person or in physical or environmental damage (collectively, "**Hazardous Use**"); or (ii) for use as a medical device(s), to be a substitute for professional medical advice, diagnosis, treatment, or judgment ("**Medical Use**"). You shall not, and not permit anyone to, make Hazardous Use or Medical Use of an Assistant or Output. You will defend, indemnify and hold Splunk and its affiliates harmless from and against all damages, costs and attorneys' fees in connection with any claims arising from a Hazardous Use or Medical Use in connection with an Assistant, including any claims based in strict liability or that Splunk (or any of Splunk's suppliers) was negligent in designing or providing the Assistant (or any part thereof) to you.

9. **IMPROVEMENTS**. Any changes, modifications, improvements and updates made to an Assistant ("Updates"), whether or not supplied by or developed by Splunk, are the sole and exclusive property of Splunk and its licensors. You acquire no rights in any Updates and you hereby assign all worldwide right, title and interest you may have in any Updates to Splunk, subject to the extent such Updates are expressly licensed to you as part of your use of an Assistant according to these terms.

10. **AI SERVICE DATA**. You are responsible for your AI Service Data, including for ensuring that it does not violate any applicable law or these terms. Due to the nature of machine learning, Outputs may not be unique across users and an Assistant may generate the same or similar Output for Splunk or a third party. Responses that are requested by and generated for other users are not considered your AI Service Data or owned by you. The Assistant may integrate with a third-party generative AI service as outlined herein or in the applicable Assistant Documentation. As such, you acknowledge and consent to Splunk sending your AI Service Data to such third-party generative AI service to provide the Assistant services and for the purposes agreed herein.

11. **TERM**. The terms applicable to a Specific Assistant as set forth herein take effect when you gain access to each respective Specific Assistant and remain in effect for the duration of your subscription term of the applicable Assistant or, if no specific subscription term for the applicable Assistant, for the subscription term of the underlying Offering in which the Specific Assistant runs unless terminated earlier. You may terminate the terms applicable to any Specific Assistant at any time for any reason by discontinuing the use of the respective Specific Assistant and providing written notice of termination to Splunk; termination of your subscription to the underlying Offering in which the Specific Assistant runs will automatically terminate the terms specific to your use of the Specific Assistant. Splunk may terminate your access to any Assistant at its convenience upon 30 days' written notice to you. If Splunk, in its sole discretion, believes your use of an Assistant may be in breach of the applicable terms or could result in a potential harm, Splunk may immediately suspend your use of the Assistant.

12. **RETENTION OF TRAINING DATA**. Splunk will retain Training Data in connection with these terms for up to one (1) year following Splunk's receipt of such data, unless otherwise required by applicable law.

13. **LIMITATION OF LIABILITY**. An Assistant constitutes an "Offering" under Section 20 of the SGT ("Limitation of Liability")

14. **DISCLAIMER OF WARRANTIES**. 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 these Terms and that you have adequate rights to use such Outputs, before relying on them. You shall ensure that your Inputs and use of any Output does not violate the intellectual property or proprietary rights of Splunk or any third party. You also acknowledge and agree that any Outputs may not be protectable under copyright or other intellectual property, proprietary rights, or other law. Splunk makes no warranties or representations, express or implied, that the Output is protectable under any law. 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 an Assistant, and that your sole remedy will be to remove the Assistant from the applicable Hosted Service.

    YOUR USE OF A SPLUNK ASSISTANT IS AT YOUR OWN RISK. IT IS 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 A SPLUNK ASSISTANT OR ANY OUTPUTS, 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) A SPLUNK ASSISTANT OR ITS OUTPUTS WILL MEET YOUR REQUIREMENTS, (II) YOUR ACCESS TO SPLUNK ASSISTANT OR ITS OUTPUTS WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE, (III) THE QUALITY OF ANY CONTENT, PRODUCTS, SERVICES, INFORMATION OR OTHER MATERIAL OBTAINED THROUGH A SPLUNK ASSISTANT WILL MEET YOUR EXPECTATIONS, AND (IV) ANY ERRORS IN THE SOFTWARE WILL BE CORRECTED. A SPLUNK ASSISTANT AND OUTPUTS 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.

15. **INDEMNIFICATION**. The “Our Indemnification to You” subpart of Section 21 (Indemnity) of the SGT will not apply with regard to an Assistant. By using an Assistant, and without limiting the “Your Indemnification to Us” subpart of Section 21 (Indemnity) of the SGT (which applies to your use of an Assistant), you agree to defend, indemnify and hold harmless Splunk, our affiliates and our personnel 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 an Assistant, including arising from or in connection with AI Service Data. You may not settle or compromise any claim that requires any action or forbearance on Splunk’s part without first obtaining Splunk’s written consent.

16. **SPECIFIC ASSISTANT TERMS**. The provisions in this Section 16 are applicable to the Specific Assistants indicated. To the extent of any conflict between the provisions set forth in this Section 16 and the generally applicable terms set forth in this AI Assistant section of the SOT, the specific terms of this Section 16 prevail.

    AI Assistant for SPL.
    The Assistant for Splunk Cloud is not available for use with GovCloud environments.

    AI Assistant for Observability.

    The Assistant for Observability is provided to you at no cost for a temporary term, ending on the earlier of the termination of your subscription to Splunk Observability; or July 31, 2025 (the “Promotional Period”). The Assistant for Observability is not available for use with GovCloud environments.

    The Assistant for Observability includes certain components from Microsoft Corporation (“MSFT”). In addition to the Policy, the MSFT acceptable use policy (“MSFT AUP”) applies to your use of the Assistant for Observability and you agree to abide by the MSFT AUP.

    Further, the MSFT code of conduct for Azure OpenAI - content requirements (“Content Requirements”) apply to your use of Assistant for Observability and your AI Service Data, and you agree to abide by the Content Requirements. Your use of any MSFT components in the Assistant for Observability must be limited solely in connection with the use of Assistant for Observability.

17. **Order of Precedence**
    Despite Section 22 of the SGT (Updates to Offerings), in the event of any conflict between these Specific Terms and the SGT, these Specific Terms will control.

18. **DEFINITIONS**

"**AI Model**" means the machine learning algorithm(s) used in an Assistant, including associated parameters and associated weights, if present.

"**Assistant Documentation**" means the descriptive, instructional, and other supporting documentation published by Splunk pertinent to a Specific Assistant. Assistant Documentation for each Specific Assistant is located below.

- Assistant Documentation for the Assistant in SPL
- Assistant Doumentation for the Assistant in Observability

"Input" means the raw data or content that you upload or submit to an Assistant or that is used as input context from your Offering environment to power an Assistant, including in-product feedback, as further described in applicable documentation.

"Output" means the data or content generated by you using or interacting with an Assistant based on any Input.

"Personal Data" means any information relating to an identified or identifiable natural person and any other information that constitutes personal data or personal information under any applicable law. An identifiable natural person is one who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Pre-existing Splunk Content" means any materials in which Splunk has pre-existing intellectual property ownership or rights.

"Training Data" means your AI Service Data, but not derivatives of AI Service Data, from interactions with an Assistant.

Prior Versions of SPLUNK TERMS FOR OFFERINGS AND HOSTED SERVICES

- **Published January 2025**
- **Published October 2024**
- **Published September 2024**
- **Published March 2024**
- **Published February 2024**
- **Published January 2024**