SUPPLIER DATA PROTECTION AGREEMENT

This Supplier Data Protection Agreement ("SDPA") is entered into by and between Cisco Systems, Inc. and its Affiliates ("Cisco"), and the Supplier and its Affiliates identified in the Agreement and/or on the face of the purchase order ("Supplier"). This SDPA is effective as of the effective date of the Agreement (the "Effective Date"). Cisco and Supplier may be referred to individually as a "Party" or collectively as the "Parties."

This SDPA is incorporated into and governed by the terms of the applicable Agreement entered into by and between the Parties for the supply of Products and/or Services by Supplier to Cisco ("the Agreement"). Unless stated otherwise, in the event of a conflict between this SDPA, including any attachments thereto, and the Agreement, the provisions of this SDPA will control but only to the extent that Supplier Processes or has access to Protected Data in the Performance of its obligations to Cisco.

Parties shall comply with all Applicable Laws, rules, policies, procedures, and all licenses, registrations, permits, and approvals required by any government or authority and any ambiguity in this SDPA shall be resolved to permit Cisco to comply with all Applicable Laws. In the event and to the extent that Applicable Laws impose stricter obligations on the Supplier than under this SDPA, the Applicable Laws shall prevail. Capitalized terms used herein and not otherwise defined shall have the meanings ascribed to them in the Agreement or as defined under Applicable Laws.

1. Definitions

1.1. "**Administrative Data**" means data related to employees or representatives of Cisco that is collected and used by Supplier in order to administer or manage Supplier's Performance, or Cisco's account. Administrative Data may include Personal Data and information about the contractual commitments between Cisco and Supplier, whether collected at the time of the initial registration or thereafter in connection with the delivery, management, or Performance. Administrative Data is Protected Data.

1.2. "**Affiliates**" means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity, for so long as such control exists. In the case of companies and corporations, "control" and "controlled" mean beneficial ownership of more than fifty percent (50%) of the voting stock, shares, interest or equity in an entity. In the case of any other legal entity, "control" and "controlled" mean the ability to directly or indirectly control the management and/or business of the legal entity.

1.3. "**APEC**" means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information.

1.4. "**APEC Member Economy**" means the members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.

1.5. "**Applicable Laws**" means any applicable supranational, national, federal, state, provincial, or local law, ordinance, statute, by-law, regulation, order, regulatory policy (including any requirement or notice of any regulatory body), compulsory guidance of a regulatory body with authority over the applicable Party, rule of court or directives, binding court decision or precedent, or delegated or subordinate legislation, each of the above as may be amended from time to time. For avoidance of doubt, Applicable Laws includes data protection and privacy laws of each jurisdiction where a Cisco entity is legally responsible for such Personal Data and those of each jurisdiction where Personal Data is collected or otherwise Processed. If any of the Applicable Laws are superseded by new or modified Applicable Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Applicable Laws shall be deemed to be incorporated into this SDPA, and Supplier will promptly begin complying with such Applicable Laws.

1.6. "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found

here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

1.7. "**Business Associate Agreement**" means the specific terms and conditions that apply when the Supplier Processes Protected Health Information, located on the Cisco Software and Services Supplier Portal (https://www.cisco.com/c/en/us/about/legal/supplier-portal.html).

1.8. "**Cardholder Data**" refers to "cardholder data" as defined by the PCI Compliance Standards and includes a cardholder's name, full account number, expiration date, and the three-digit or four-digit security number printed on the front or back of a payment card. For the purposes of this SDPA Cardholder Data constitutes Protected Data and Sensitive Personal Data.

1.9. "**CCPA"** means the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CPRA"), and any related regulations or guidance provided by the California Attorney General.

1.10. "**Confidential Information**" means any Customer Data, confidential information, and/or materials relating to the business, products, customers or employees of Cisco and includes, without limitation, trade secrets, know-how, inventions, techniques, processes, programs, schematics, software source documents, data, customer lists, financial information, pricing, product development, sales and marketing plans, or information that the Supplier knows or has reason to know is confidential, highly confidential, restricted, proprietary, or trade secret information obtained by Supplier from Cisco or at the request or direction of Cisco in the course of Performing: (i) that has been marked as Confidential, Highly Confidential, or Restricted; (ii) whose confidential nature has been made known by Cisco to the Supplier; or (iii) that due to their character and nature, a reasonable person under like circumstances would treat as confidential.

1.11. "**Controller**" shall have the same meaning ascribed to "controller" under the GDPR and other equivalent terms under other Applicable Laws (e.g., "**Business**" as defined under the CCPA), as applicable.

1.12. "**Customer Data**" means all data (including text, audio, video, or image files) that are either provided by Cisco in connection with Cisco's use of Products or Services, or data developed at the specific request of Cisco pursuant to the Agreement, a statement of work, or contract. Customer Data is Confidential Information.

1.13. "**Data Subject**" means the individual to whom Personal Data relates (e.g., "**Consumer**" as defined under the CCPA).

1.14. "**EEA**" or "**European Economic Area**" means those countries that are members of European Free Trade Association, and the then-current, post-accession member states of the European Union.

1.15. "**Financing Data**" means information related to Cisco's financial health that Cisco provides to Supplier in connection with the Agreement. Financing Data is Protected Data.

1.16. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

1.17. "**Information Security Incident**" means a successful or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.

1.18. "**PCI Compliance Standards**" means the Payment Card Industry Data Security Standard, as published and updated by the Payment Card Industry Security Standard Council from time to time.

1.19. "**Performance**" means any acts by either Party in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Personal Data, or providing Software as a Service ("SaaS"), cloud platforms, or hosted services. "**Perform**," "**Performs**," and "**Performing**" shall be construed accordingly.

1.20. "**Personal Data**" means any information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person. Personal Data shall be considered Confidential Information regardless of the source (e.g. "**Personal Information**" as defined under the CCPA). Personal Data is Protected Data.

1.21. "**Process**" and any other form of the verb "Process" means any operation or set of operations that is performed upon Protected Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.22. "**Processor**" shall have the same meaning ascribed to "processor" under the GDPR and other equivalent terms under other Applicable Laws (e.g., "**Service Provider**" as defined under the CCPA), as applicable.

1.23. "**Product**" means Supplier hardware and software products.

1.24. "**Protected Data**" means Administrative Data, Confidential Information, Customer Data, Financing Data, Support Data, Telemetry Data, Personal Data, and Sensitive Personal Data.

1.25. **"Protected Health Information"** shall have the meaning given to such term under the Privacy and Security Rules at 45 CFR Section 164.103, limited to the information created or received by Supplier from or on behalf of Cisco.

1.26. "**Representatives**" means either Party and its Affiliates' officers, directors, employees, agents, contractors, temporary personnel, subprocessors, subcontractors, and consultants.

1.27. "**Sensitive Personal Data**" refers to sensitive personal information (as defined under the CCPA), special categories of personal data (as described in Article 9 of the GDPR), and other similar categories of Personal Data that are afforded a higher level of protection under Applicable Laws.

1.28. "**Service**" means a service offering from Supplier described in an applicable service or offer description, statement of work, or purchase order listed selected by Cisco.

1.29. "**Standard Contractual Clauses**" means, (i) in those instances in which Cisco acts as a Controller and the Supplier acts as a Processor, the Controller to Processor Standard Contractual Clauses located on the Cisco Software and Services Supplier Portal (https://www.cisco.com/c/en/us/about/legal/supplier-portal.html), and (ii) in those instances in which Cisco acts as a Processor and the Supplier acts as a Processor, the Processor to Processor Standard Contractual Clauses located on the Cisco Software and Services Supplier Portal (https://www.cisco.com/c/en/us/about/legal/supplier-portal.html). The Standard Contractual Clauses are agreed to by and between the Parties and are incorporated into the SDPA as if set forth fully herein. Transfers of Personal Data subject to the Standard Contractual Clauses are specified in and subject to Annex I and Annex II (the "Annexes") below.

1.30. "**Standard Contractual Clauses – UK Addendum**" means the UK Addendum to the EU Commission Standard Contractual Clauses available and located at: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/uk-addendum.pdf (the official version issued by the UK Information Commissioner's Office is available and located at: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.) The Standard Contractual Clauses UK Addendum is entered into by and between the Parties and is incorporated into the SDPA as if set forth fully herein.

1.31. **"Supplier Information Security Exhibit"** means the Supplier Information Security Exhibit, as amended from time to time, located on the Cisco Software and Services Supplier Portal (https://www.cisco.com/c/en/us/about/legal/supplier-portal.html).

1.32. "**Support Data**" means information that Supplier collects when Cisco submits a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident, such as authentication information, information about the condition

of the product, system and registry data about software installations and hardware configurations, and error-tracking files. Support Data is Protected Data.

1.33. "**Telemetry Data**" means information generated by instrumentation and logging systems created through the use and operation of the products and/or services. Telemetry Data is Protected Data.

2. Processing of Personal Data

2.1. **Roles of the Parties.** For the Processing of Personal Data, Supplier will act as Processor to Cisco, and Cisco may act as a Controller and/or a Processor with respect to Personal Data.

2.2. **Additional Cisco Obligations.** Cisco shall:

a. ensure all instructions given by Cisco to Supplier with respect to the Processing of Personal Data are at all times in accordance with Applicable Laws, and to the extent that Cisco is acting as a Processor on behalf of a customer who is acting as Controller, that these instructions impose the same or more protective data protection obligations on Supplier as the Controller has imposed on Cisco;

b. ensure all Personal Data provided to Supplier has been collected in accordance with Applicable Laws and that Cisco has all authorizations and/or consents necessary to provide such Personal Data to Supplier; and

c. keep the amount of Personal Data provided to Supplier to the minimum necessary for the Performance of the Products and/or Services.

2.3. **Additional Supplier Obligations.** Supplier shall:

a. only retain, use, disclose, or otherwise Process Personal Data, including Processing of Personal Data on its systems or facilities, to the extent necessary for the Performance of the Services and/or Products and its obligations under the Agreement, Cisco's documented instructions and this SDPA. Supplier shall immediately notify Cisco if Supplier reasonably believes that Cisco's instructions are inconsistent with any Applicable Law or if Supplier makes a determination that it can no longer meet its obligations under Applicable Laws;

b. ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Supplier to keep the Personal Data confidential that are no less protective of Personal Data than the terms of this SDPA, and that these Representatives are aware of these obligations;

c. appoint data protection lead(s) and provide Cisco with the contact details of the appointed person(s) upon request;

d. if required by Applicable Laws, court order, warrant, subpoena, or other legal or judicial process to Process Personal Data other than in accordance with Cisco's instructions, notify Cisco immediately upon receipt of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such notification, in particular on important grounds of public interest);

e. maintain reasonably accurate records of the Processing of any Personal Data received from Cisco under the Agreement, including all records of Processing as may be required by Applicable Law;

f. make reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent Supplier has the ability to do so;

g. not lease, sell, share, (as those terms are defined under the CCPA), disclose Personal Data in exchange for valuable consideration, or otherwise encumber Personal Data;

h. grant the Cisco the right to take reasonable and appropriate steps to ensure that Supplier processes the Personal Data that it received from, or on behalf of, Cisco in a manner consistent with Cisco's obligations under Applicable Laws including

without limitation ongoing manual reviews and automated scans of the Supplier's system and regular assessments, audits, or other technical and operational testing;

i. not combine, or update Personal Data received from, or on behalf of, Cisco with Personal Data that Supplier has collected or received from any other source;

j. not attempt to identify, re-identify, de-aggregate, or de-anonymize any data that has been de-identified, pseudonymized, anonymized, or aggregated pursuant to Cisco's instructions or in compliance with Applicable Laws;

k. provide such information and assistance as Cisco may reasonably require (taking into account the nature of the Processing and the information available to Supplier) to enable compliance by Cisco with its obligations under Applicable Laws with respect to:

   i. security of Processing;

   ii. data protection impact assessments (as such term is defined by Applicable Laws);

   iii. prior consultation with a supervisory authority regarding high-risk Processing;

   iv. responding to requests from supervisory authorities, Data Subjects, customers, controllers, or others to provide information related to Supplier's Processing of Personal Data;

   v. notifications by the applicable supervisory authority and/or communications to Data Subjects by Cisco in response to any Information Security Incident; and

   vi. Cisco's ability to meet any applicable filing, approval or similar requirements in relation to Applicable Laws.

3. Rights of Data Subjects

3.1. **Data Subject Requests.** Supplier shall, to the extent legally permitted, promptly notify Cisco if it receives a request from a Data Subject to exercise their rights under any Applicable Law related to Personal Data, including without limitation requests to exercise a Data Subject's rights for access to, correction, portability, or deletion of such Data Subject's Personal Data. Unless required by Applicable Laws, Supplier shall not respond to any such Data Subject request without Cisco's prior written consent except to confirm that the request relates to Cisco and to redirect the Data Subject to Cisco.

3.2. **Complaints or Notices related to Personal Data.** In the event Supplier receives any complaint, notice, or communication that relates to Supplier's Processing of Personal Data or either Party's compliance with Applicable Laws in connection with Personal Data, Supplier shall promptly notify Cisco and, to the extent applicable, Supplier shall provide Cisco with reasonable cooperation in relation to any such complaint, notice, or communication.

4. Transfers of Personal Data

4.1. Before transferring Personal Data outside of the jurisdiction where the Personal Data was obtained, Supplier shall first provide Cisco advance notice by email to ask_privacy@cisco.com and an opportunity to object. If Cisco reasonably objects to the proposed cross border transfer and the Parties do not mutually agree to an alternative method of Processing, Cisco may terminate the Agreement with respect to the Products and/or Services which Supplier is unable to Perform due to the objection.

4.2. **Transfers of Personal Data from the EEA to third countries.** Where Supplier Processes Personal Data from the EEA on behalf of Cisco in a third country which is not an Approved Jurisdiction and the transfer of Personal Data is not permitted by an alternative means pursuant to the relevant Applicable Laws, Supplier shall perform such Processing in a manner consistent with the applicable Standard Contractual Clauses. If necessary to comply with Applicable Laws, and where requested by Cisco on behalf of its customers, Supplier shall enter into the Standard Contractual Clauses directly with Cisco's customers. Further, Supplier shall perform such Processing in a manner consistent with the EU-U.S. Data

Privacy Framework ("EU-U.S. DPF") principles (see https://www.dataprivacyframework.gov) or its successor framework(s) to the extent the principles are applicable to Supplier's Processing of such data. If Supplier is unable to provide the same level of protection as required by the EU-U.S. DPF principles, Supplier shall promptly notify Cisco and cease Processing. In such event, Cisco may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

4.3. **Transfers of Personal Data from Switzerland to third countries.** Where Supplier Processes Personal Data from Switzerland on behalf of Cisco in a third country which is not an Approved Jurisdiction, Supplier shall perform such Processing in a manner consistent with the applicable Standard Contractual Clauses modified as follows: i) the term "member state" shall not be interpreted in a way to exclude data subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses, ii) references to the GDPR shall be understood as and are replaced with references to the Federal Act on Data Protection ("FADP"), and iii) the Federal Data Protection and Information Commissioner of Switzerland shall be the competent supervisory authority. Further, Supplier shall perform such Processing in a manner consistent with the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") principles (see https://www.dataprivacyframework.gov) or its successor framework(s) to the extent the principles are applicable to Supplier's Processing of such data. If Supplier is unable to provide the same level of protection as required by the Swiss-U.S. DPF principles, Supplier shall promptly notify Cisco and cease Processing. In such event, Cisco may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

4.4. **Transfers of Personal Data from the UK (and Gibraltar) to third countries.** Where Supplier Processes Personal Data from the UK in a third country which is not an Approved Jurisdiction and the transfer of Personal Data is not permitted by an alternative means pursuant to the relevant Applicable Laws, Supplier shall perform such Processing in a manner consistent with the applicable Standard Contractual Clauses - UK Addendum. Any further changes to the Standard Contractual Clauses - UK Addendum approved with an official decision by the Information Commissioner's Office will be incorporated by reference and a copy of the new Standard Contractual Clauses -UK Addendum will be available on the Cisco Software and Services Supplier Portal. Further, Supplier shall perform such Processing in a manner consistent with the U.K. Extension to the EU-US DPF ("U.K Extension") principles (see https://www.dataprivacyframework.gov) or its successor framework(s) to the extent the principles are applicable to Supplier's Processing of such data. If Supplier is unable to provide the same level of protection as required by the U.K. Extension principles, Supplier shall promptly notify Cisco and cease Processing. In such event, Cisco may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

4.5. **Transfers of Personal Data from APEC Member Economies to third countries.** Where Supplier Processes Personal Data from an APEC Member Economy on behalf of Cisco, Supplier shall perform such Processing in a manner consistent with the APEC Cross Border Privacy Rules system ("CBPRs") and Privacy Recognition for Processors ("PRP") (see www.cbprs.org) to the extent the requirements are applicable to Supplier's Processing of such data. If Supplier is unable to provide the same level of protection as required by the CBPRs and PRP, Supplier shall promptly notify Cisco and cease Processing. In such event, Cisco may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

5. Subprocessing

5.1. Supplier shall not subcontract its obligations under this SDPA to new subprocessors, in whole or in part, without providing Cisco with at least thirty (30) days advance written notice via email to ask privacy@cisco.com with an opportunity for Cisco to object before providing any new subprocessor with

access to Personal Data. If Cisco objects to the proposed subcontracting on reasonable grounds and the Parties cannot resolve the objection, Cisco may terminate by written notice the applicable part of the Agreement with respect only to those Products and/or Services which cannot be provided by Supplier without the use of the subprocessors to whom Cisco objects.

5.2. Supplier shall execute a written agreement with such approved subprocessors containing terms at least as protective as this SDPA and its attachments. Further, if privity of contract is required by Applicable Laws, Supplier shall undertake to ensure that any such subprocessors are contractually bound to cooperate and to enter into any necessary additional agreements as directed by Cisco.

5.3. Supplier shall be liable and accountable for the acts or omissions of its Representatives to the same extent it is liable and accountable for its own actions or omissions under this SDPA.

6. Security

6.1. **Security Measures.** Supplier shall implement and maintain commercially reasonable and appropriate physical, technical, and organizational security measures described in this SDPA designed to protect the confidentiality, integrity, and availability of Protected Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access; all other unlawful forms of Processing; and any Information Security Incident (the "**Security Measures**"). Without limiting the generality of the foregoing, the Security Measures shall include, at a minimum, those measures (a) described in the Supplier Information Security Exhibit, the terms of which are incorporated by reference, and (b) all measures as may be required under any Applicable Law (including Article 32 of the GDPR) and all applicable industry standards.

6.2. **Adjustments to Security Measures.** Supplier shall regularly monitor, evaluate, and adjust, as appropriate, Supplier's Security Measures in light of any relevant changes in circumstances, such as changes in technology or any applicable industry standards, Applicable Laws, internal and external threats to Supplier's information technology assets or Protected Data (including any threats identified on the OWASP Top Ten list, as published from time to time), requirements of applicable statements of work, and Supplier's business and business relationships. Notwithstanding any other term hereof, in no event shall Supplier materially decrease the efficacy or level of protection provided by Supplier's Security Measures.

6.3. **Additional Measures for Sensitive Personal Data.** In addition to the foregoing, to the extent that Supplier Processes Sensitive Personal Data, the Security Measures referred to in this SDPA shall also include encryption of Sensitive Personal Data during transmission and storage. If encryption is not feasible, Supplier shall not store such data on any unencrypted devices unless compensating controls are implemented.

6.4. **Additional Measures for Protected Health Information.** In addition to the foregoing, to the extent Supplier Processes Protected Health Information, the data protection and Security Measures shall include, at a minimum, those measures (a) described in the Business Associate Agreement, the terms of which are incorporated by reference, and (b) all measures as may be required under any Applicable Law and all applicable industry standards.

6.5. **Additional Measures for Cardholder Data**. In addition to the foregoing, to the extent Supplier receives, transmits, stores, or otherwise Processes any Cardholder Data for or on behalf of Cisco, Supplier represents and warrants that it will:

a. comply with the PCI Compliance Standards for so long as Supplier Processes Cardholder Data; and

b. provide evidence of compliance with the PCI Compliance Standards to Cisco upon request. Such evidence of compliance shall include, without limitation, a current attestation of compliance signed by a PCI Qualified Security Assessor.

7. Audit. Supplier shall make available to Cisco such information as is reasonably necessary to demonstrate Supplier's compliance with the obligations of this SDPA in accordance with the terms of the Security Measures.

8. **Additional notification requirements.** In the event that (a) Supplier receives any complaint, notice, or communication that relates to Supplier's Processing of Personal Data or either Party's compliance with Applicable Laws in connection with Protected Data, or (b) any investigation or any litigation or dispute arises in relation to Supplier's Processing of Protected Data, Supplier shall promptly notify Cisco and, to the extent applicable, Supplier shall provide Cisco with all reasonable cooperation that Cisco may request in connection therewith. In the event either Party notifies the other Party of an Information Security Incident, Supplier shall (i) respond to any Cisco communication(s) within forty-eight (48) hours or less, (ii) provide all information, cooperation and assistance to at data-incident-command@cisco.com regarding any such Information Security Incident, and (iii) address such Information Security Incident per the severity rating that Cisco assigns to it, including, preparing and making available to Cisco for public distribution any patches, fixes or workarounds that would mitigate against vulnerabilities.

9. **Return and Deletion of Personal Data.** Upon completion, fulfilment, or conclusion of the initial purposes for processing for whatever reason; upon termination or expiration of the Agreement or any transaction document; , and upon written request at any time, Supplier shall cease to Process any Customer Data received from Cisco, and without undue delay, shall: (a) return, or make available for return, all Customer Data in its possession or control, (b) securely and completely destroy or permanently render unreadable or inaccessible (e.g. using a standard such as NIST SP 800-88 Rev. 1 Purge or equivalent) all existing copies of the Customer Data, and (c) provide Cisco with certification within thirty (30) days after: i) the termination or expiration of the Agreement or any transaction document, ii) the conclusion, fulfillment or completion of Cisco's initial purposes for processing, or iii) the date of the deletion request, that Supplier has fully complied with this clause. If continued retention and Processing is required by Applicable Laws, Supplier shall provide a justification as to why such compliance is not feasible.

10. **Additional Processing Restrictions.** Each of Cisco and Supplier acknowledge and agree that Personal Data, or the ability access to Personal Data, is not provided to Supplier in exchange for monetary value or other valuable consideration and that such Processing does not constitute a "sale" of Personal Data to Supplier, or "sharing" of Personal Data with Supplier (as those terms are defined by Applicable Laws).

11. **General terms**

    11.1. **Attorneys' Fees.** In any lawsuit or proceeding, relating to this SDPA, the prevailing Party will have the right to recover from the other its costs and reasonable fees and expenses of attorneys, accountants, and other professionals incurred in connection with the lawsuit or proceeding, including costs, fees, and expenses upon appeal, separately from and in addition to any other amount included in such judgment. This provision is intended to be severable from the other provisions of this SDPA and shall survive expiration or termination and shall not be merged into any such judgment.

    11.2. **Assignment.** Unless otherwise expressly provided under this SDPA, neither Party may assign this SDPA or assign its rights or delegate its obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other Party. Any attempt at such an assignment or delegation without the other Party's written consent will be void. The rights and liabilities of the Parties under this SDPA will bind and inure to the benefit of the Parties' respective successors and permitted assigns. For purposes of this Section 11.2 (Assignment), a twenty percent (20%) change in control of a Party shall constitute an assignment.

    11.3. **Breach**. In the event of a breach of this SDPA, Cisco may be entitled to seek injunctive or equitable relief to immediately cease or prevent the use, Processing, or disclosure of Personal Data and to enforce the terms of this SDPA or enforce compliance with all Applicable Laws.

    11.4. **Complete Agreement, Amendments.** This SDPA is the complete agreement between the Parties concerning the subject matter of this SDPA and replaces any prior oral or written communications between the Parties. This SDPA is subject to the terms and conditions of the Agreement, including, but not limited to any limitations or exclusions of liability set forth in the Agreement unless prohibited by Applicable Laws. There are no conditions, understandings, agreements, representations, or warranties ex-

pressed or implied, that are not specified herein. This SDPA may only be modified by a written document executed by the Parties hereto. Notwithstanding the foregoing, Cisco may amend this SDPA from time to time in the event that Cisco determines, in its sole discretion, that any such amendment is necessary for Cisco to comply with any law, rule, regulation, or contractual obligation ("**Compliance Amendments**"). Cisco will provide Supplier with at least thirty (30) days prior notice of any Compliance Amendments.

11.5. **Notices.** All notices required or permitted under this SDPA shall be in writing, written in English, and sent to (a) in the case of Supplier being the recipient of the notice, to the email address designated by Supplier; and (b) in the case of Cisco being the recipient of the notice, by certified or registered mail or by a nationally recognized overnight courier to 170 West Tasman Drive, San Jose, CA 95134, or such other address that Cisco may designate from time to time with a copy sent to ask_privacy@cisco.com. Either Party may change its contact information for receipt of notice by providing with other Party with at least fourteen (14) days' prior written notice of such change. Notices will be deemed to have been given (i) upon delivery of electronic mail, (ii) one day after deposit with a commercial express courier specifying next day delivery; or (iii) two days for international courier packages specifying two-day delivery, with written verification of receipt.

11.6. **Termination, Survival.** Supplier's obligations under this SDPA shall survive the expiration or earlier termination of the Agreement until such time that the Supplier no longer holds, Processes, or otherwise has access to Protected Data, and this Section 11 (General terms) shall survive the expiration or earlier termination of the SDPA indefinitely.

IN WITNESS WHEREOF, the parties hereto have caused this SDPA to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this SDPA hereto.

ANNEX I

The Annexes form part of the Standard Contractual Clauses.

A. LIST OF PARTIES

Data exporter(s):

Name: Cisco Systems, Inc.
Address: 170 West Tasman Ave, San Jose CA, USA 95134

Contact person's name, position and contact details: Jelena Kljujic, EMEAR Data Protection Officer, emear_rpo@cisco.com
Activities relevant to the data transferred under these Clauses: Data is transferred pursuant to Cisco's purchase of services and products.
Role (controller/processor): Cisco's role shall be as described in Section 2.1 (Roles of the Parties) of the main body of the SDPA.

Data importer(s):

Name: Supplier
Address: Supplier's address identified in the Agreement and/or on the face of the purchase order.
Activities relevant to the data transferred under these Clauses: The provisioning of the Products and Services to Cisco pursuant to the Agreement and subject to the SDPA.
Role (controller/processor): Supplier's role shall be as described in Section 2.1 (Roles of the Parties) of the main body of the SDPA.

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred

The personal data transferred may concern the following categories of data subjects: Cisco personnel, Cisco's customers' personnel.

2. Categories of personal data transferred

The personal data transferred may concern the following categories of data:

3. Sensitive data transferred (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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data importer shall implement and maintain those measures described in Section 6 of the main body of the SDPA, including those measures described in Section 6.3 (Additional Measures for Sensitive Personal Data) and those measures described in the Information Security Exhibit, to protect the Sensitive Personal Data described above.

4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuously throughout the term of the Agreement.

5. Nature of the processing

Personal data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analyzing, collecting, transferring, and making available personal data.

6. Purpose(s) of the data transfer and further processing

Perform the Services in accordance with the Agreement and the SDPA.

7. **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

   Supplier shall retain and delete data in compliance with the SDPA and Applicable Laws but in no event shall Supplier retain personal data longer than thirty (30) days after: the initial purposes of processing have been fulfilled, or termination of the Services, the Agreement, or any SOW or other transaction document.

8. **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**

   Where applicable, the same information provided under sections B4-8 of the Annexes shall apply to all subprocessors.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Autoriteit Persoonsgegevens, the Data Protection Authority of the Netherlands.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organizational measures to be implemented and maintained by Supplier are as described in the main body of the SDPA including, without limitation, Section 2.3, Section 5.2, and Section 6, and the Supplier Information Security Exhibit. Without limiting Supplier's obligations under Section 5.2, Supplier shall ensure that each subprocessor implements and maintains, at a minimum, the technical and organizational measures that Supplier is required to implement pursuant to the SDPA, including those measures described in the Supplier Information Security Exhibit and the following:

Measures of pseudonymization and encryption of personal data;

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;

Measures for ensuring the ability to restore the availability and access to personal data 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 organizational measures in order to ensure the security of the processing;

Measures for user identification and authorization;

Measures for the protection of data during transmission;

Measures for the protection of data during storage;

Measures for ensuring physical security of locations at which personal data are processed;

Measures for ensuring events logging;

Measures for ensuring system configuration, including default configuration;

Measures for internal IT and IT security governance and management;

Measures for certification/assurance of processes and products;

Measures for ensuring data minimization;

Measures for ensuring data quality;

Measures for ensuring limited data retention;

Measures for ensuring accountability; and

Measures for allowing data portability and ensuring erasure.