SUPPLIER ARTIFICIAL INTELLIGENCE POLICY

1. Use of Protected Data for Artificial Intelligence and Machine Learning.

1.1. Supplier is not permitted to Process Protected Data for training, retraining or improving Artificial Intelligence or Machine Learning technologies without Cisco's express written permission. The same applies to Supplier's Representatives.

1.2. If Supplier seeks permission according to the above section 1.1., Supplier shall provide Cisco with all information and assistance reasonably required by Cisco to (i) comply with Applicable Laws, and (ii) perform all types of assessments and related diligence that Cisco deems necessary.

1.3. A permission granted by Cisco according to section 1.1. is limited to one (1) year, unless otherwise agreed upon between the Parties.

2. Supplier's Use of Artificial Intelligence and Machine Learning.

2.1. If Supplier is using or intends to use Artificial Intelligence and/or Machine Learning technologies in the course of Performing, it is required to have an AI/ML governance program in place, with defined policies and procedures, that meets or exceeds current best industry standards.

2.2. If Supplier seeks permission according to the above section 1.1., Cisco reserves the right to audit Supplier's AI/ML governance program before deciding whether to grant the requested permission and on a regular basis (with a notice period of 14 days) after a permission has been granted.

3. Definitions

3.1. "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 customer 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.

3.2. "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.

3.3. "Artificial Intelligence" or "AI" is a machine's ability to perform some cognitive functions usually associated with human intelligence. AI technology is able to receive inputs from the environment, interpret and learn from such inputs, and output behaviours and actions that help achieve a particular goal or objective.

3.4. "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.

3.5. “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.

3.6. “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.

3.7. “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.

3.8. “Machine Learning” or “ML” is a form of AI that can adapt to a wide range of inputs, including large sets of historical data, synthesized data, or human inputs. ML algorithms can detect patterns and learn how to make predictions and recommendations by Processing data, rather than by receiving explicit programming instruction.

3.9. “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.

3.10. “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. Personal Data is Protected Data.

3.11. “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.

3.12. “Product” means Supplier hardware and software products.

3.13. “Protected Data” means Administrative Data, Confidential Information, Customer Data, Financing Data, Support Data, Telemetry Data, Personal Data, and Sensitive Personal Data.

3.14. “Representatives” means either Party and its Affiliates’ officers, directors, employees, agents, contractors, temporary personnel, subprocessors, subcontractors, and consultants.

3.15. “Sensitive Personal Data” refers to sensitive personal information, special categories of personal data, and other similar categories of Personal Data that are afforded a higher level of protection under Applicable Laws.

3.16. “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.

3.17. “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).

3.18. “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.

3.19. “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.