GLOSSARY OF TERMS

All capitalized terms not defined in this Glossary have the meanings set forth in the Agreement. In the event of a conflict between the definitions in the Agreement and any definitions in this Glossary, this Glossary will control as it relates to the subject matter set forth herein.

a. "**Agreement**" means all applicable agreements between the Cisco and the Supplier, including: Vendor Services Agreement, Master Service Agreement, Professional Services Subcontract Agreement, Supplier Base Agreement, and applicable licensing and other agreements under which the Supplier Performs.

b. **"Applicable Laws"** means any applicable country, federal, state, and local law, ordinances, statute, by-law, regulation, order, regulatory policy (including any requirement or notice of any regulatory body), compulsory guidance or industry code of practice, 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. Supplier will comply with all laws, all licenses, permits and approvals required by any government or authority, and shall comply with all applicable laws, rules, policies and procedures.

c. "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: **http://ec.europa.eu/justice/data-protection/international transfers/adequacy/index_en.htm.**

d. "**Business Associate Agreement**" means the specific terms and conditions that apply when the Supplier Processes Protected Health Information.

e. "**Cardholder Data**" is a category of Sensitive Personal Data 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.

f. "**Cisco**" is defined as it is in the Agreement.

g. "**Cisco Data**" means all information and data provided or made available to Supplier, including customer information and data, any manipulation of that data and any data or information Supplier collects, generates, or otherwise obtains in connection with its Performance under the Agreement. For clarity, to the extent Cisco Data contains Personal Data as defined herein, the terms related to Personal Data will also apply.

h. "**Confidential Information"** means any confidential information or materials relating to the business, products, customers or employees of the disclosing party 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 receiving party knows or has reason to know is confidential, proprietary or trade secret information obtained by receiving party from the disclosing party or at the request or direction of the disclosing party in the course of Performing: (i) that has been marked as confidential; (ii) whose confidential nature has been made

known by the disclosing party to the receiving party; or (iii) that due to their character and nature, a reasonable person under like circumstances would treat as confidential.

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

j. "**Electronic Protected Health Information**" or "**Electronic PHI**" shall have the meaning given to such term as set forth in the Business Associate Agreement.

k. "**EU Directives**" means the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), any amendments or replacements to them (such as the EU General Data Protection Regulation). For clarity, the EU Directives are a subset of Applicable Laws.

l. **"Generally Accepted Practices**" means those practices used by shall refer to the levels of accuracy, quality, care, prudence, completeness, timeliness, responsiveness, resource efficiency, productivity, and proactive monitoring of service performance that are at least equal to the then-current accepted industry standards of first-tier providers of the tasks contemplated in Performance of the Agreement.

m. "**Information Security Incident"** means a suspected, 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.

n. "**Performance**" means any acts by the Supplier 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.

o. "**Personal Data**" or "**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.

p. "**Process**" or "**process**" means any operation or set of operations that is performed upon Personal 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. "**Processes**" or "**processes**" and "**Processing**" or "**processing**" shall be construed accordingly.

q. "**Protected Data**" means Cisco Data, Confidential Information, Cisco customer Confidential Information and all Personal Data.

r. "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term as set forth in the Business Associate Agreement and is a category of Personal Data. "Protected Health Information" includes "Electronic Protected Health Information" or "ePHI".

s. "**Representatives**" means Supplier and its affiliate's officers, directors, employees, agents, contractors, subcontractors and consultants.

t. "**Sensitive Personal Data**" or "**Special Categories of Data**" means personal information that requires an extra level of protection and a higher duty of care. These categories are defined by Applicable Law and include: information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, precise geolocation over time, or information related to offenses or criminal convictions. Sensitive Personal Data and Special Categories of Data are each a category of Personal Data that are particularly sensitive and pose greater risk. Cisco may require additional privacy responsibilities when dealing with such Personal Data, which will be appended to the Agreement or a statement of work, as applicable.

u. "**Supplier**" means the person or legal entity, regardless of the form of organization that has entered into an Agreement with Cisco. Supplier may be defined as Subcontractor, Vendor, Contractor, Licensor, or other such defined term in the Agreement.