Supplier Information Security Exhibit

This Supplier Information Security Exhibit ("SISE") applies to the extent that Supplier Processes or has access to Protected Data in the Performance of its obligations to Cisco. This SISE outlines the information security requirements between Cisco and Supplier and describes the technical and organizational security measures that shall be implemented by the Supplier to secure Protected Data prior to the Performance of any Processing under 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 otherwise stated, in the event of a conflict between the Agreement and this SISE, the terms of this SISE will control as it relates to the Processing of Protected Data.

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, for Supplier's own business purposes. 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. "**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.

1.4. "**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.

1.5. "**Confidential Information**" means any confidential information 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, 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; (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.

1.6. "**Customer Data**" means all data (including text, audio, video, or image files) that are either provided by a customer in connection with the customer's use of products or services, or data developed at the specific request of a customer pursuant to a statement of work or contract. Customer Data does not include Administrative Data, Financing Data, Support Data, or Telemetry Data.

1.7. "**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.

1.8. "**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).

1.9. "**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.

1.10. "**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.

1.11. "**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.

1.12. "**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.

1.13. "**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.

1.14. "**Protected Data**" means Administrative Data, Confidential Information, Customer Data, Financing Data, Cardholder Data, Support Data, Telemetry Data, and all Personal Data.

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

1.16. "**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.

1.17. "**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.

1.18. "**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. General Security Practices

Supplier has implemented and shall maintain appropriate technical and organizational measures designed to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this SISE for its personnel, equipment, and facilities at the Supplier's locations involved in Performing any part of the Agreement.

3. General Compliance

3.1. **Compliance**. Supplier shall document and implement processes and procedures to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes and procedures shall be designed to provide appropriate security to protect Protected Data given the risk posed by the nature of the data Processed by Supplier. The Supplier shall implement and operate information security in accordance with the Supplier's own policies and procedures, which shall be no less strict than the information security requirements set forth in this SISE.

3.2. **Protection of records**. Supplier shall implement appropriate procedures designed to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

3.3. **Review of information security.** Supplier's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures) shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

3.4. **Compliance with security policies and standards.** Supplier's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

3.5. **Technical compliance review.** Supplier shall regularly review information systems for compliance with Supplier's information security policies and standards.

3.6. **Information Risk Management ("IRM").** Supplier shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. Supplier is required to have a risk management framework and conduct periodic risk assessments of its environment and systems to understand the risks and apply appropriate controls to manage and mitigate such risks. Threat and vulnerability assessment must be periodically reviewed and prompt remediation actions taken where material weaknesses are found. Supplier will provide Cisco with relevant summary reports and analysis upon written request, provided the disclosure of which would not violate Supplier's own information security policies, or Applicable Laws.

3.7. **Processing of Sensitive Personal Data**. To the extent that Supplier Processes Sensitive Personal Data and the security measures referred to in this SISE are deemed to provide insufficient protection, Cisco may request that Supplier implements additional security measures.

4. Technical and Organizational Measures for Security

4.1. **Organization of Information Security**

a. **Security Ownership**. Supplier shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.

b. **Security Roles and Responsibilities**. Supplier shall define and allocate information security responsibilities in accordance with Supplier's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to Representatives required to comply with such policies.

c. **Project Management**. Supplier shall address information security in project management to identify and appropriately address information security risks.

d. **Risk Management**. Supplier shall have a risk management framework and conduct periodic risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before Processing Protected Data.

4.2. **Human Resources Security**

a. **General**. Supplier shall ensure that its personnel are under a confidentiality agreement that includes the protection of Protected Data and shall provide adequate training about relevant privacy and security policies and procedures. Supplier shall further inform its personnel of possible consequences of breaching Supplier's security policies and procedures, which must include disciplinary action, including possible termination of employment for Supplier's employees and termination of contract or assignment for Representatives and temporary personnel.

b. **Training**. Supplier personnel with access to Protected Data shall receive appropriate, periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents. Training shall be provided before Supplier personnel are granted access to Protected Data or begin providing services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

c. **Background Checks**. In addition to any other terms in the Agreement related to this subject matter, Supplier shall conduct criminal and other relevant background checks for its personnel in compliance with Applicable Laws and the Supplier's policies.

4.3. **Trusted Device Standards.**

a. Supplier personnel shall:

i. Only use trusted Devices that are configured with security software (i.e., anti-virus, anti-malware, encryption, etc.);

ii. Follow trusted device standards when accessing Protected Data or when having Protected Data in their possession, custody, or control. The trusted device standard specifies the requirements that user devices ("**Devices**") must satisfy to be trusted when Processing Protected Data whether or not connected to a Cisco's network through wired, wireless, or remote access (the "**Network**"). Devices that fail to comply with this standard will not be entitled to access Network unless Cisco determines limited access is acceptable.

b. Trusted device standards include, at a minimum, the following:

i. Each Device must be uniquely associated with a specific, individual user;

ii. Devices must be configured for automatic patching. All operating system and application security patches must be installed within the timeframe recommended or required by the issuer of the patch;

iii. Devices must be encrypted (i.e., full disk, endpoint encryption) and secured with a protected (e.g., password, PIN, finger print, facial recognition, biometrics, etc.) screen lock with the automatic activation feature. Users must lock the screen or log off when the device is unattended;

iv. Devices must not be rooted or jailbroken;

v. Devices must be periodically scanned for restricted/prohibited software (e.g., certain peer-to-peer sharing apps that have been found to exploit/exfiltrate data); and

vi. Devices must run an acceptable industry standard anti-malware solution. On-access scan and automatic update functionality must be enabled.

c. Supplier shall implement policies designed to prevent the storage of Protected Data on unencrypted smartphones, tablets, USB drives, DVD/CDs, or other portable media without prior written authorization from Cisco; and take measures to prevent accidental exposure of Protected Data (e.g., using privacy filters on laptops).

4.4. **Personnel Access Controls**

a. **Access.**

i. **Limited Use.** Supplier understands and acknowledges that Cisco may be granting Supplier access to sensitive and proprietary information and computer systems. Supplier will not (i) access the Protected Data or computer systems for any purpose other than as necessary to Perform its obligations to Cisco; or (ii) use any system access information or log-in credentials to gain unauthorized access to Protected Data or Cisco's systems, or to exceed the scope of any authorized access.

ii. **Authorization.** Supplier shall restrict access to Protected Data and systems at all times solely to those Representatives whose access is necessary to Performing Supplier's obligations to Cisco.

iii. **Suspension or Termination of Access Rights.** At Cisco's reasonable request, Supplier shall promptly and without undue delay suspend or terminate the access rights to Protected Data and systems for any Supplier's personnel or its Representatives reasonably suspected of breaching any of the provisions of this SISE; and Supplier shall remove access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

iv. Information Classification. Supplier shall classify, categorize, and/or tag Protected Data to help identify it and to allow for access and use to be appropriately restricted.

b. **Access Policy**. Supplier shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Supplier shall maintain a record of security privileges of its personnel that have access to Protected Data, networks, and network services.

4.5. **Access Authorization**.

a. Supplier shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Cisco's systems and networks. Supplier shall use an enterprise access control system that requires revalidation of its personnel by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role/Performance obligations.

b. For systems that Process Protected Data, Supplier shall revalidate (or where appropriate, deactivate) access of users who change reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.

c. Supplier shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

4.6. **Network Design**. For systems that Process Protected Data, Supplier shall have controls to avoid personnel assuming access rights beyond those that they have been assigned to gain unauthorized access to Protected Data.

4.7. **Authentication**

a. Supplier shall use industry standard practices including ISO/IEC 27002:2013 and NIST SP 800-63-3B (Digital Identity Guidelines) to identify and authenticate users who attempt to access information systems.

b. Where authentication mechanisms are based on passwords, Supplier shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability) with at least 8 characters and containing the following four classes: upper case, lower case, numeral, special character.

c. Supplier shall ensure that de-activated or expired identifiers and log-in credentials are not granted to other individuals.

d. Supplier shall monitor repeated failed attempts to gain access to the information system.

e. Supplier shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

f. Supplier shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

g. Supplier shall use a multi-factor authentication solution to authenticate personnel accessing its information systems.

4.8. **Cryptography and Key management**

a. Supplier shall have a policy on the use of cryptographic controls based on assessed risks.

b. Supplier shall assess and manage the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecate and disallow usage of weak cypher suites and insufficient bit and block lengths.

c. Supplier shall have procedures for distributing, storing, archiving, and changing/updating keys; recovering, revoking/destroying, and dealing with compromised keys; and logging all transactions associated with such keys.

4.9. **Physical and Environmental Security**

a. **Physical Access to Facilities**

i. Supplier shall limit access to facilities where systems that Process Protected Data are located to authorized individuals.

ii. Security perimeters shall be defined and used to protect areas that contain Protected Data and Processing facilities.

iii. Facilities shall be monitored and access-controlled at all times (24x7).

iv. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems Processing Protected Data. Supplier must register personnel and require them to carry appropriate identification badges.

b. **Physical Access to Equipment**. Supplier equipment used to Process or store Protected Data shall be protected using industry standard processes to limit access to authorized individuals.

c. **Protection from Disruptions**. Supplier shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

d. **Clear Desk**. Supplier shall have policies requiring a “clean desk/clear screen” to prevent inadvertent disclosure of Protected Data.

4.10. **Operations Security**

a. **Operational Policy**. Supplier shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. Supplier shall communicate its policies and requirements to all persons involved in the Processing of Protected Data. Supplier shall implement the appropriate

management structure and control designed to ensure compliance with such policies and with Applicable Laws concerning the protection and Processing of Protected Data.

b. **Security and Processing Controls**.

i. Areas. Supplier shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks and services that store or Process Protected Data.

ii. **Standards and Procedures.** Such standards and procedures shall include: security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

c. **Logging and Monitoring**. Supplier shall maintain logs of administrator and operator activity and data recovery events related to Protected Data.

4.11. **Communications Security and Data Transfer**

a. **Networks**. Supplier shall, at a minimum, use the following controls to secure its networks that access or Process Protected Data:

i. Network traffic shall pass through firewalls, which are monitored at all times. Supplier must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.

ii. Network devices used for administration must utilize industry standard cryptographic controls when Processing Protected Data.

iii. Anti-spoofing filters and controls must be enabled on routers.

iv. Network, application, and server authentication passwords are required to meet the same industry standard practices used for the authentication of users set forth in Section 4.7 (Authentication) above. System-level passwords (privileged administration accounts or user-level accounts with privileged administration access) must be changed at minimum every 90 days.

v. Initial user passwords are required to be changed at first log-on. Supplier shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

vi. Firewalls must be deployed to protect the perimeter of Supplier's networks.

b. **Data Transfer**. Supplier shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of this SISE. Such policies shall be designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

4.12. **System Acquisition, Development, and Maintenance**

a. **Security Requirements**. Supplier shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

b. **Development Requirements**. Supplier shall have policies for secure development, system engineering, and support. Supplier shall conduct appropriate tests for system security as part of acceptance testing processes. Supplier shall supervise and monitor the activity of outsourced system development.

4.13. **Penetration Testing and Vulnerability Scanning & Audit Reports**

a. **Testing.** Supplier will perform periodic penetration tests on their internet perimeter network. Audits will be conducted with industry recommended network security tools to identify vulnerability of information. Upon written request from Cisco, Supplier shall provide a

Vulnerability & Penetration testing report at the organization level which may include an executive summary of the results and not the details of actual findings.

b. **Audits.** Supplier shall respond promptly to and cooperate with reasonable requests by Cisco for security audits, scanning, discovery, and testing reports.

c. **Remedial Action.** If any audit or penetration testing exercise referred to in Section 4.13.a (Testing), above reveals any deficiencies, weaknesses, or areas of non-compliance, Supplier shall promptly take such steps as may be required, in Supplier's reasonable discretion, to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances. Upon request, Supplier shall keep Cisco informed of the status of any remedial action that is required to be carried out, and shall certify to Cisco as soon as may be practicable that all necessary remedial actions have been completed.

4.14. **Contractor Relationships**

a. **Policies**. Supplier shall have information security policies or procedures for its use of Representatives that impose requirements consistent with this SISE.

b. **Monitoring**. Supplier shall monitor and audit service delivery by its Representatives and review its Representatives' security practices against the security requirements set forth in Supplier's agreements with such Representatives. Supplier shall manage changes in Representative services that may have an impact on security.

5. Management of Information Security Incidents and Improvements

5.1. **Responsibilities and Procedures**. Supplier shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.

5.2. **Reporting Information Security Incident.** Supplier shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as reasonably possible. All Representatives should be made aware of their responsibility to report Information Security Incidents as quickly as reasonably possible.

5.3. **Reporting Information Security Weaknesses.** Supplier and Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.

5.4. **Assessment of and Decision on Information Security Events.** Supplier shall have an incident classification scale in place in order to decide whether a security event should be classified as an Information Security Incident. The classification scale should be based on the impact and extent of an incident.

5.5. **Response Process.** Supplier shall maintain a record of Information Security Incidents with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

5.6. **Information Security Aspects of Business Continuity Management**

a. **Planning**. Supplier shall maintain emergency and contingency plans for the facilities where Supplier information systems that Process Protected Data are located. Supplier shall verify the established and implemented information security continuity controls at regular intervals.

b. **Data Recovery**. Supplier shall design redundant storage and procedures for recovering data in a manner sufficient to reconstruct Protected Data in its original state as found on the last recorded backup provided by Cisco.

6. Notification and Communication Obligations

6.1. **Notification**. Supplier shall without undue delay (i.e., within 48 hours from confirmation) notify Cisco at: data-incident-command@cisco.com and privacy@cisco.com if any of the following events occur:

a. any unmitigated, material security vulnerability, or weakness of which Supplier has actual knowledge in (i) Cisco's systems, or networks, or (ii) Supplier's systems or networks, that has compromised Protected Data;

b. an Information Security Incident that compromises or is likely to compromise the security of Protected Data and weaken or impair business operations of Cisco;

c. an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of Protected Data; or

d. known and willful failure or inability to maintain material compliance with requirements of this SISE and Applicable Laws.

6.2. **Cooperation.** Supplier shall: (i) respond promptly to any Cisco reasonable requests for information, cooperation, and assistance in any post-incident investigation, remediation, and communication efforts.

6.3. **Information Security Communication.** Except as required by Applicable Laws or by existing applicable contractual obligations, Supplier agrees that it will not inform any third party of any of the events described above in this Section referencing, or identifying Cisco, without Cisco's prior written consent. Supplier shall fully cooperate with Cisco and law enforcement authorities concerning any unauthorized access to Cisco's systems or networks, or Protected Data. Such cooperation shall include the retention of all information and data within Supplier's possession, custody, or control that is directly related to any Information Security Incident. If disclosure is required by law, Supplier will work with Cisco regarding the timing, content, and recipients of such disclosure. To the extent Supplier was at fault, Supplier will bear the cost of reproduction or any other remedial steps necessary to address the incident or compromise.