Supplier Information Security Exhibit

This Supplier Information Security Exhibit ("**Exhibit**") describes certain technical and organizational security measures that Supplier must implement and maintain to protect the security of the Cisco Data that it Processes, as well as the Products and Services that it provides, in connection with the Agreement. Supplier shall implement and maintain all such measures for so long as: (i) with regards to Cisco Data, Supplier or any of its Representatives Process Cisco Data, and (ii) with regards to Products and Services, for so long as Supplier provides Products and Services. In the event of a conflict between the terms of the Agreement and this Exhibit, the terms that are most protective of Cisco Data and the Products and Services shall prevail.

1. Definitions

1.1. "**Agreement**" refers any and all written agreements between Cisco and Supplier related to Supplier's provisioning of Products and Services to Cisco.

1.2. "**Cardholder Data**" refers to 'cardholder data' as defined by the PCI Compliance Standards.

1.3. "**Cisco Data**" refers to all information and data (i) provided to Supplier by or on behalf of Cisco in connection with the Products or Services, or (ii) that Supplier collects, generates, or obtains by virtue of (a) Cisco's use of the Products or Services or (b) Supplier's provisioning of the Products and Services to or on behalf of Cisco.

1.4. "**Cisco Offerings**" refers to all products and services that Cisco sells, licenses, or otherwise provides to its distributors, resellers, partners, customers, or end users.

1.5. "**Entrusted Systems**" refers to any of Cisco's or any of Cisco's customers', end users' or suppliers' systems or networks that Supplier or Supplier's Representatives obtain access to in connection with this Agreement.

1.6. "**Security Incident**" refers to any known or suspected event that actually or imminently jeopardizes the confidentiality, integrity, or availability of Cisco Data, Entrusted Systems or the Products. For the avoidance of doubt, "Security Incident" includes any unauthorized access to or use, disclosure, modification, loss, corruption, deletion or destruction of Cisco Data.

1.7. "**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.

1.8. "**Process**" and any other form of the verb "Process" means any operation or set of operations that is performed upon information or 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.

1.9. "**Products**" refers to all products, including any Software and hardware, as well as any technical documentation related thereto, that Supplier provides in connection with the Agreement.

1.10. "**Representatives**" refers to Supplier's and its affiliates' respective officers, directors, employees, agents, contractors, temporary personnel, sub-processors, subcontractors, and consultants.

1.11. "**Services**" refers to all services, including any technical support, managed services, professional services, and cloud services, that Supplier provides in connection with the Agreement.

1.12. "**Software**" includes all software that Supplier provides in connection with the Agreement, including any (i) firmware, (ii) any source, object, and binary code, (iii) any software updates and patches, and (iv) any software (e.g., software clients) that Supplier provides to Cisco in connection with its Services (e.g., mobile applications and other locally installed clients).

1.13. "**Supplier Systems and Networks**" refers to the systems and networks that Supplier uses to Process Cisco Data and the systems and networks that Supplier uses to develop or otherwise provide the Products and Services, including Supplier's build environments and code repositories.

1.14. Terms such as "include", "including", "for example", and "e.g." shall not be interpreted as having a limiting effect, but rather as introducing a non-exhaustive example or list in the same fashion as phrases like "including, without limitation" and "including, but not limited to."

2. General Security Practices.

2.1. General Requirements. Supplier shall, in line with industry best practices, maintain appropriate technical and organizational measures that ensure the security (i.e., confidentiality, integrity, availability, and authenticity) of Cisco Data and the Products, Services, Supplier Systems and Networks, and any Entrusted Systems within Supplier's possession and control, including: (i) appropriate measures that protect Cisco Data against accidental loss, destruction and alteration, unauthorized disclosure and access, and unlawful destruction, (ii) all measures described in this Exhibit, and (iii) all measures required by applicable laws, rules, regulations and industry standards (the "***Security Measures***").

2.2. Security Reviews and Adjustments. Supplier shall regularly monitor, evaluate, and enhance, as appropriate, the Security Measures in light of relevant changes in circumstances, such as changes in technology, applicable industry standards, applicable laws, rules and regulations, internal and external threats (including emerging threats), environmental and operational conditions, contractual requirements, Supplier's business (including Supplier Systems and Networks), and Supplier's business relationships.

2.3. Compliance with Cybersecurity Laws. Supplier shall comply with, and ensure the Products and Services comply with all applicable privacy, data protection, and cybersecurity laws, rules, and regulations, including the E.U. Cyber Resilience Act (Regulation (EU) 2024/2847) and the EU NIS2 Directive (Directive (EU) 2022/2555) ("***Cybersecurity Laws***"). In the event that Supplier or any of its Products or Services (i) fail to comply with any Cybersecurity Law, (ii) cause Cisco's Offerings to fail to comply with Cybersecurity Laws, or (iii) results in a government authority requesting or requiring Cisco to address (e.g., mitigate or eliminate) risks associated with the Products or Services pursuant to a Cybersecurity Law, Supplier shall provide such cooperation and assistance as reasonably requested by Cisco to address any such non-compliance or risks. Upon request, Supplier shall promptly provide Cisco with all such information and documentation regarding the Products and Services (including user instructions, technical documentation, and declarations of conformity) that Cisco may reasonably require to comply with its obligations under Cybersecurity Laws. Supplier shall use commercially reasonable efforts to provide all such information and documentation shall be provided in English unless otherwise required by law.

3. Technical and Organizational Measures

3.1. Information Security Governance.

a. **Information Security Program**. Supplier will implement and maintain a written information security program, consisting of a set of policies, standards, procedures, and other controls aimed at protecting the security of Cisco Data and the Products and Services ("***Information Security Program***"). Supplier's Information Security Program will be based on and conform with one or more widely accepted international information security standards for information security management systems (e.g., AICPA SOC 2, ISO 27001).

b. **Information Risk Management ("IRM")**. Supplier's Information Security Program shall include an appropriate information risk management framework to frame, assess, respond to and monitor risk. Without limiting the generality of the foregoing, Supplier shall perform regular, documented risk assessments and threat modelling to identify risks applicable to the Products, Services, and Supplier Systems and Networks, and (ii) take appropriate steps to promptly manage such risks,

including assigning a risk-score and a risk owner that is responsible for determining and implementing appropriate mitigation and remediation measures. Supplier shall perform such assessments and modelling at least annually. Additionally, Supplier shall update its risks assessment to assess the risks associated with and account for changes made to the Products, Services, and Supplier Systems and Networks, as appropriate, taking into consideration the nature and scope of such changes.

c. **Security Ownership**. Supplier shall appoint one or more security officers responsible for coordinating and monitoring Information Security Program. 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.

d. **Security Roles and Responsibilities**. Supplier shall maintain formal documentation detailing Supplier's security measures and that define the security responsibilities of, and allocates such responsibilities to, the appropriate Supplier Representatives, including Representatives that (i) administers Supplier Systems and Networks, (ii) have access to Cisco Data or Supplier Systems and Networks, or (iii) develop or otherwise participate in the provisioning of the Products and Services. Supplier shall require its Representatives to comply with Supplier's policies, procedures and other security-related requirements, the terms of the Agreement, as well as any and all applicable laws, rules, and regulations.

e. **Independent Audits**. Supplier will undertake regular (but no less frequent than annually) independent audits of its Information Security Program to ensure Supplier's compliance with the requirements of this Exhibit. Such audits shall be (i) based on one or more widely accepted international information security management standards (e.g., ISO 27001, SOC 2) and (ii) performed by one or more qualified and reputable third-party auditors.

f. **Compliance**. Supplier shall comply with its statutory, regulatory, contractual and other legal obligations related to information security and other relevant security requirements, including Supplier's policies and procedures. Supplier's management shall regularly review its compliance with such obligations and requirements, including performing regular reviews of its Supplier Systems and Networks.

g. **Maintenance of Evidence.** Supplier shall maintain evidence to sufficiently demonstrate compliance with Supplier's obligations under the Agreement in accordance with applicable audit standards and industry best practices.

h. **Protection of Records**. Supplier shall implement appropriate technical and organizational measures to protect the security of records (e.g., security event logs), including protecting records from loss, tampering, falsification, and unauthorized access, use and disclosure.

3.2. Human Resources Security

a. **General**. Supplier shall ensure that its Representatives are bound by a contractual or professional duty of confidentiality that requires them to protect the security of Cisco Data.

b. **Training**. Supplier shall ensure its personnel (e.g., employees and contingent workers) periodically receive appropriate privacy and security education and role-based awareness training, including Supplier's privacy- and security-related policies and procedures. Supplier personnel shall be required to successfully complete such awareness training before being granted access to any Cisco Data, Entrusted Systems or Supplier Systems and Networks and at least annually thereafter. Supplier shall regularly reinforce its education and awareness training through other means, such as email campaigns, posters, notice boards, training exercises, and other resources and activities.

c. **Background Checks and ID Verification**. Supplier shall conduct criminal and other relevant and appropriate background checks on its personnel. Such background checks shall (i) include reasonable and appropriate steps to validate the identity of Supplier personnel and the authenticity

of any government-issued identification used to validate the identity, (ii) be conducted in accordance with applicable laws and industry best practices, and (iii) be completed prior to providing the relevant personnel with access to Cisco Data or the Products or Services (including any component thereof). Additionally, Supplier shall take steps to verify, throughout the hiring and onboarding process, that Supplier personnel hired or contracted by Supplier are the same individuals as the individuals that were interviewed for the role, including monitoring for and investigating suspicious circumstances (e.g., monitoring and comparing voice and visual appearance throughout the interview and onboarding process, investigating requests to ship equipment to addresses other than the residential address listed on government-issued identification or bank account records, etc.).

d. **Accountability**. Supplier shall implement appropriate disciplinary measures and corrective actions to address failures by its Representatives to abide by its security policies, procedures, or other security-related requirements, the terms of this Agreement, or applicable laws, rules, and regulations. Supplier shall inform its Representatives of possible consequences of such failures, including possible disciplinary actions (e.g., termination of employment and termination of contingent worker assignments).

3.3. Trusted Devices Requirements, Entrusted Systems.

a. **Trusted Device Requirements.** Supplier shall implement and maintain appropriate trusted device measures, including documented requirements that devices (e.g., cell phones, tablets, laptops, workstations, servers, etc.) must satisfy before such devices are permitted to access or otherwise Process Cisco Data, access any Supplier Systems or Networks, or otherwise be used to provide Products or Services, regardless of whether the device is connected to a network through wired or wireless means. Such requirements shall include requirements for devices to be hardened with appropriate security software, features, functionality, and configurations, including (i) anti-malware software with on-access scanning, automatic updates enabled, and definitions that are updated daily or more frequently if recommended by the developer of the software, (iii) strong device encryption, (iii) data loss prevention and monitoring solutions, (iv) remote lock and remote wipe capabilities; (v) enabling automatic installation of patches and updates, where appropriate, and other measures to ensure security patches are installed in a timely manner and in accordance with industry best practices; (v) configure devices to automatically enable screen lock and account log out after an appropriately defined period of inactivity; (vi) ensure devices are not rooted or jailbroken. Additionally, Supplier shall periodically perform scans for restricted/prohibited software at appropriate intervals, and where appropriate, uniquely associate each device with a specific individual user.

b. **Automatic Enforcement of Trusted Device Standards.** Supplier shall implement appropriate measures, including automatic device health and compliance checks, to ensure only devices that comply with Supplier's trusted device requirements may be used to access or otherwise Process Cisco Data or access any other Supplier Systems or Networks.

c. **Entrusted Systems.** In the event the Services involve access to any Entrusted Systems, Cisco may, in its sole discretion, require (i) any device that Supplier uses to access Entrusted Systems to comply with Cisco's trusted device policies, and/or (ii) Supplier to use Entrusted Systems selected by Cisco when performing all or a portion of the relevant Services.

d. **Removable Media.** Supplier shall not store or otherwise Process Cisco Data on removable or portable media storage devices (e.g., USB drives, DVD/CDs, external hard drives, etc.) without Cisco's prior written consent. Supplier shall implement and maintain reasonable and appropriate measures to protect the security of Cisco Data while processed via any such device, including ensuring all Cisco Data is encrypted while stored on the device.

3.4. Access Management

a. **General.** Supplier shall maintain appropriate policies and procedures for managing access to Cisco Data, Supplier Systems and Networks, and where appropriate, Entrusted Systems.

b. **Access to and Use of Cisco Data and Entrusted Systems**. Supplier shall not and shall not permit its Representatives to (i) access or use Cisco Data or Entrusted Systems for any purpose other than as necessary to Perform its obligations to Cisco; or (ii) use any such access to engage in any unauthorized activities, including, without limitation, engage in activities that exceed the scope of any authorized access, circumvent any security measures, or engage in any activities that violate any applicable laws, rules, and regulations. To the extent that Supplier's Services involves access to Entrusted Systems, Supplier shall comply with Cisco's information security policies.

c. **Provisioning, Reviewing, and Revoking Access.** Supplier shall maintain appropriate policies and procedures for the creation and deletion of accounts and for approving, provisioning, reviewing, suspending and revoking access and other privileges. Without limiting the generality of the foregoing, Supplier shall: (i) restrict access to systems, networks, and Cisco Data based on the principle of "least privilege" and on a "need-to-know" basis; (ii) promptly review, and where appropriate, deactivate, user access when users change reporting structure; (iii) deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months; and (iv) immediately terminate a Representative's access in the event the Representative ceases to be employed by or provide services to Supplier. Supplier shall periodically review and revalidate the need for ongoing user access at least every: (i) 90 days in the case of privileged users, and (ii) 180 days in the case of non-privileged users.

d. **Suspension and Termination**. At Cisco's reasonable request, Supplier shall promptly and without undue delay suspend or terminate a Representative's access rights to Cisco Data and/or Entrusted Systems in the event Cisco reasonably suspects the Representative has breached any of the security-related requirements under the Agreement, including this Exhibit, or otherwise poses a risk to the security of Cisco Data or Entrusted Systems. Supplier shall immediately deactivate credentials whenever Supplier discovers or reasonably suspects the credentials have been corrupted, exposed or have otherwise been compromised.

e. **Privilege Escalation**. Supplier shall maintain appropriate organizational and technical measures that prohibit its Representatives from assuming access rights beyond what they have been assigned.

3.5. Authentication

a. Supplier shall use industry best practices for identifying and authenticating users and systems and for securing credentials and secrets, which such practices shall be no less stringent than those measures described in NIST SP 800-63- 3B (Digital Identity Guidelines) and any successor thereto. Without limiting the generality of the foregoing, Supplier shall: (i) require and enforce strong password requirements (e.g., length, character complexity, and/or non- repeatability) where authentication mechanisms include the use of passwords; (ii) ensure that de-activated or expired identifiers and log-in credentials are not granted to other individuals; (iii) monitor repeated failed authentication attempts; (iv) ensure credentials and secrets are appropriately encrypted in-transit and at rest; (v) prohibit the use of shared credentials and group credentials; (vi) require default credentials and other initially assigned credentials to be changed at first log-in; (vii) change system-level passwords (privileged administration accounts or user-level accounts with privileged administration access) at least every 90 days; and (viii) when authentication is being performed remotely, use multi-factor authentication mechanisms that, at a minimum, comply with the FIDO2 standard and any successors thereto.

3.6. Cryptography and Key Management. Supplier shall implement and maintain appropriate cryptographic controls, including (a) appropriately managing the lifecycles of (including protecting the security of) cryptographic algorithms, keys, and certificates, including securely distributing, storing, archiving, and changing/updating algorithms, keys and certificates, as well as taking appropriate steps to address risks associated with compromised keys and certificates; (b) ensuring that Cisco Data is, at all times, encrypted in transit and at rest using strong encryption; and (c) ensuring appropriate cryptographic strength, taking into consideration the state-of-the-art technologies (including technologies for breaking encryptions) and not using weak or obsolete cypher suites or insufficient bit or block lengths.

3.7. Physical and Environmental Security.

a. **Physical Access.** Supplier shall use reasonable and appropriate measures, in line with industry best practices, to restrict and manage physical access to and within its facilities and to Supplier Systems and Networks, Entrusted Systems within its possession and control, and Cisco Data. Without limiting the generality of the foregoing, Supplier shall (i) require all personnel and visitors to sign-in and conspicuously carry identification badges, (ii) require all visitors to be escorted; (iii) define and use security perimeters to protect areas that are used to Process Cisco Data or develop or otherwise provide the Products and Services; (iv) monitor facilities at all times using appropriate surveillance systems and logging and monitoring mechanisms and procedures; (v) appropriately control access to and within facilities using electronic locking mechanisms that log access events, security personnel and other physical access controls (e.g., barriers, signs, obstacles and other means of guiding individuals to controlled ingress and egress points and preventing unauthorized access); and (vi) maintain "clear desk" and "clear screen" policies.

b. **Power Supply and Environmental Controls.** Supplier shall ensure its facilities have appropriate power supplies and environmental controls, including (i) backup generators or other secondary power supplies, (ii) temperature and humidity controls for heating, ventilation, and air conditioning (HVAC) equipment, and (iii) fire detection and suppression systems.

3.8. Operations Security

a. **System Administration and Change Management**.

i. **Standards and Procedures**. Supplier shall maintain, document, and implement standards and procedures for the configuration, operation, and management of Supplier Systems and Networks. Such standards and procedures shall include standards and procedures that appropriately address the risks associated with Supplier Systems and Networks, including identification and patching of security vulnerabilities, change management processes and procedures, and incident prevention, detection, remediation, and management.

ii. **Change Management.** Supplier shall maintain appropriate change management policies and procedures, including documented procedures for reviewing, approving, monitoring and implementing changes to production systems, networks, applications, and data file structures and a documented procedure describing relevant roles and responsibilities and maintains appropriate separation of duties (e.g., request, approve, implement).

b. **Logging and Monitoring**. Supplier shall implement and maintain appropriate logging and continuous monitoring for all Supplier Systems and Networks, including logging and monitoring of administrator and operator activity, configuration changes, authentication successes and failures, changes in user privileges, data recovery events, file movement, code commits and other appropriate security events (e.g., events from security systems, such as firewalls, intrusion detection and prevention systems, and antimalware solutions). Logs shall be retained for an appropriate period of time, taking into consideration the nature and risks associated with the relevant Products, Services, and Supplier Systems and Networks, as well as all applicable laws, rules, and regulations and standards. Supplier shall implement and maintain reasonable and appropriate measures to ensure the integrity and availability of all such logs. Supplier shall also incorporate reasonable and appropriate logging and monitoring capabilities into its Products and Services (including logs of changes to data, services, or functions), including the capability for Cisco to access relevant event logs generated by the Products and Services, as appropriate.

3.9. Asset Management. Supplier shall maintain appropriate policies and procedures for securely managing assets throughout the asset lifecycle, including the following:

a. **Asset Inventories.** Supplier shall (i) maintain accurate and up-to-date records of the hardware and software assets and other information resources, such as databases and file structures, that are used to Process Cisco Data and that are used to develop or otherwise provide the Products and Services, and (ii) periodically review such records.

b. **Data Classification.** Supplier shall maintain appropriate policies and procedures for classifying and tagging data and use such classifications and tagging to protect the security of the data, including to appropriately restrict access to the data and monitor the movement and use of data for data loss prevention purposes.

c. **Deletion of Cisco Data, Media Sanitization & Destruction.** Except as otherwise required by law, Supplier shall promptly and irreversibly delete or destroy Cisco Data, in a manner consistent with NIST SP 800-88 Guidelines for Media Sanitization (or any successor thereto), upon the earlier of: (i) receiving written request from Cisco, (ii) when Cisco Data is no longer necessary for the performance of its obligations under the Agreement, or (iii) termination of the Agreement. When Supplier Systems and Networks are repurposed, or decommissioned or otherwise disposed of, Supplier shall sanitize or destroy the Supplier Systems and Networks in a manner consistent with NIST SP800-88 Guidelines for Media Sanitization (or any successor thereto) and maintain documented evidence of such sanitization or destruction.

3.10. Communications Security

a. **Networks.** Supplier shall implement reasonable and appropriate measures to protect the security of Supplier's networks, including firewalls, segmentation, distributed denial-of-service mitigation, network flow analyses, and domain name service (DNS) security. Without limiting the generality of the foregoing, Supplier shall: (i) ensure that network traffic passes through firewalls and is logged and continuously monitored and protected, including through the use of intrusion prevent systems; (ii) ensure network devices used for administration utilize industry best practices for cryptographic controls; (iv) enable anti-spoofing filters and controls on routers; (v) when Supplier Representatives remotely accessing Supplier Systems and Networks, secure the connections using VPN or zero trust architecture (vi) encrypt wireless connections with Supplier Systems and Networks using strong encryption; (vii) maintain appropriate isolation and segregation of its production and non-production environments, and (viii) if Cisco Data is transferred to a non-production environment, ensure the security and privacy measures that are applicable to the non-production environment are equivalent to those in the production environment and as otherwise required under this Exhibit.

b. **Data Transfers.** Supplier shall use appropriate measures, aligned with industry best practices, to ensure the secure transfer of information that should be treated as confidential (e.g., Cisco Data, source code, credentials and secrets, etc.), including appropriate organizational and technical measures that are designed to protect information in transit from unauthorized interception, copying, modification, corruption, routing and destruction.

3.11. Secure Acquisition and Development

a. **Secure Acquisition.** Supplier shall implement and maintain reasonable and appropriate measures that adequately address the security risks associated with the purchase, use, and development of third-party technologies (e.g., software, hardware and other information systems), including for the acquisition and use of open source and other third-party software code in the Products and Services as well as application services delivered through public networks (e.g., cloud services). Such measures shall include pre-acquisition assessments and periodic post-acquisition assessments of the risks associated the intended use of such technologies. Post-acquisition assessments must be performed at appropriate intervals, taking into consideration the risks associated with the use of such technologies.

b. **Secure Development.** Supplier must maintain reasonable and appropriate secure development lifecycle (SDL) measures, including for defining, acquiring, developing, enhancing, modifying, testing, and implementing the Products and Services, following industry best practices and in accordance widely accepted international standards (e.g., ISO/IEC 27034, NIST SP 800-218). Without limiting the generality of the foregoing, Supplier shall use industry best practices to address security risks associated with the Products and Services, including preventing vulnerabilities, backdoors and covert channels, malicious and disabling code, and other similar security risks from being introduced in or otherwise affecting the Products and Services, including:

i. adhering to the principles of “secure by default”, “secure by design”, and ‘data minimization’ throughout the lifecycle of the Products and Services;

ii. implementing appropriate measures to protect against cybersecurity risks associated with machine learning and other forms of artificial intelligence, including malicious acts such as prompt injection, data poisoning, and model inversion, in accordance with industry standards (e.g., ISO/IEC 42001);

iii. taking appropriate steps to minimize (a) the use of code that creates undue risk in its Products and Services (b) the impact that the Products and Services may have on the availability other products and services; (c) the attack surface of the Products and Services, and (d) the impact of security incidents involving the Products and Services may have, including on other systems and networks;

iv. requiring developers to use secure coding guidelines in line with industry standards, which may include the Open Web Application Security Project "(OWASP") Guide and Top 10 lists, the SANS CWE Top 25 Most Dangerous Software Errors, and CERT Secure Coding, as applicable;

v. conducting security testing and code reviews as part of the testing phase of Supplier’s development lifecycle, including (a) functional testing of security controls (e.g., access controls, cryptographic modules, etc.), as applicable; (b) static and dynamic code scanning for vulnerabilities; and (c) code reviews to verify the code is free of (1) any means or functions that may detrimentally interfere with or adversely affect use of any the Products or Services or any Cisco product or otherwise damage or destroy data or other property, including any software traps, viruses, worms, trap doors, or other forms of malicious code or disabling code, (2) software that replicates, transmits, or otherwise distributes itself or data on a network or system, (3) any master key access or backdoors or any means of remote control or remote command access that is either unplanned or not conspicuously disclosed in the technical documentation provided to Cisco, and (4) known exploited vulnerabilities;

vi. maintaining code versioning records, log and monitor provenance data, and take other appropriate measures to protect the security of software code; and

vii. supervise and monitor the activity of outsourced system development to ensure development in compliance with the Agreement, including this Exhibit.

c. **Segregation of Data.** Supplier shall logically segregate Cisco Data from data of its other customers and end users.

d. **Penetration Testing.** Supplier shall perform periodic penetration tests on its Products and Supplier Systems and Networks. Penetration tests will be conducted at least annually, using industry standard methodologies, and using qualified (and in the case of external penetration testers, reputable) penetration testers. Upon written request from Cisco, Supplier shall provide Cisco with an executive summary of the penetration test results, which must include a summary of the scope and methodology of the tests and relevant findings (e.g., number of vulnerabilities identified broken down by CVSS level).

e. **Vulnerability Scanning.** Supplier shall perform vulnerability scans prior to each software release for its Products and Services, including dynamic and static code scans as well as scans for known vulnerabilities in open-source software and other third-party components. Supplier shall also perform regular (but no less than weekly) vulnerability scans in the Products and Services, including Supplier Systems and Networks.

f. **Documentation of Security Requirements.** Supplier shall maintain clear documentation how the Product and Services meet the relevant security requirements, including those requirements identified in Supplier’s risk assessments and threat modelling for the applicable Products or Services, as well as any security specifications and requirements mutually agreed to by the parties.

3.12. Vendor Risk Management

a. **Vendor Agreements.** Prior to permitting a third-party Representative to access Cisco Data, Entrusted Systems, or any Supplier Systems and Networks, Supplier shall enter into written agreements with Representatives containing terms that are no less protective than the terms of this Exhibit.

b. **Assessments, Supervisions, and Accountability.** Prior to permitting a third-party Representative to access Cisco Data, Entrusted Systems, or any Supplier Systems and Networks and periodically thereafter, Supplier shall perform appropriate risk assessments, including an assessment of the Representatives ability to provide services in compliance with the applicable terms of the Agreement, including this Exhibit. Supplier shall also regularly monitor its third-party Representatives' provisioning of products and services and periodically perform appropriate risk assessments at appropriate intervals, taking into consideration the risk associated with the services performed by the Representative as well as applicable laws, rules and regulations and contractual obligations. Supplier shall be liable for the acts and omissions of its Representatives and solely responsible for ensuring its Representatives' compliance with this Exhibit.

4. Security Incidents

4.1. General. Supplier shall maintain appropriate policies and procedures, and use appropriate technical measures, for monitoring and detecting security incidents, and to ensure timely, effective, and orderly management of security incidents, including reporting, triaging, mitigation and remediation of security incidents. Supplier shall inform its Representatives of their responsibility to immediately report security incidents using the designated reporting channels.

4.2. Incident Records. Supplier shall maintain records of all security incidents. Such records shall contain the salient details of each incident, including a detailed description of the incident, the known scope of impact (including information, systems, and individuals and entities impacted by the incident and the nature of impact, and risks posed to the impacted individuals and entitles), the mitigation and remediation measures taken to address the incident, and the actions taken to prevent future security incidents. Supplier shall also use commercially reasonable efforts to preserve all logs that are relevant to the investigation of the security incident, including preserving a copy of such logs in their original state at the time the logs are captured for investigative purposes.

4.3. Notification. Supplier shall notify Cisco of any known or suspected Security Incidents without undue delay, and no later than, within 24 hours of discovering the event or suspecting the event has or will occur. Supplier shall send such notices by email to data-incident-command@cisco.com.

4.4. Cooperation and Assistance. Supplier shall promptly provide, at its own expense, all such cooperation and assistance that Cisco may reasonably request in connection with (i) Cisco's incident response efforts, including Cisco's investigation, mitigation, remediation, and communication efforts, and (ii) Cisco's efforts to comply with its contractual, regulatory, and other legal obligations relating to Security Incidents. For the avoidance of doubt, such cooperation shall include, when reasonably requested by Cisco, make any and all relevant logs available to Cisco; however, Supplier may redact or withhold portions of the logs to the extent that the logs include information that is unrelated to Security Incidents (as the security incidents pertain to Cisco) or as otherwise required by applicable law.

4.5. Communications Relating to Information Security Incidents. Except to the extent required by applicable laws, Supplier agrees that it will not disclose to, or otherwise communicate with, any third party about any Security Incident in a manner that references or identifies Cisco without Cisco's prior written consent. If any such disclosure or communication is required by law, Supplier will provide Cisco with reasonable prior notice of the disclosure or communications and work with Cisco regarding the timing, content, and recipients of such disclosure or communication.

5. Vulnerability Management.

5.1. **General** Supplier shall promptly, diligently, and effectively manage (including investigate, mitigate and remediate, as appropriate) all vulnerabilities in the Products, Services, and Supplier Systems and Networks that are reported to Supplier or that Supplier otherwise suspects or becomes aware of. Additionally, Supplier shall implement reasonable and appropriate vulnerability management measures, including documented policies and procedures, a responsible disclosure program with clearly and publicly posted details on how external parties (including Supplier's customers and security researchers) can report vulnerabilities to Supplier, clearly instructing and regularly reminding Supplier Representatives on how to report vulnerabilities to Supplier's vulnerability management team(s), and automated tools and up-to-date asset inventories (including software bills of materials for the Products and Services, as applicable) that enables Supplier effectively monitor and detect vulnerabilities. Supplier shall score vulnerabilities in accordance with the then-current version of the Common Vulnerability Scoring System (CVSS).

5.2. **Vulnerabilities in Products.** Supplier shall use commercially reasonable efforts to promptly provide Cisco with (a) notice of vulnerabilities in Supplier Products, (b) effective mitigations and workarounds for each vulnerability (as appropriate), and (c) effective fixes for each vulnerability (i.e., security patch or update, as appropriate). Such notices shall: (i) be sent via email to psirt@cisco.com, and (ii) include sufficient information to allow Cisco to assess the risk associated with the vulnerability, including details regarding the nature and root cause of the vulnerability, the affected Products (including Product version, as applicable), potential effect of the vulnerability, and information as to whether Supplier knows or reasonably suspects that the vulnerability has been exploited. Without limiting the foregoing, Supplier shall use commercially reasonable efforts to notify Cisco of and provide Cisco with fixes: (1) for "High" vulnerabilities without undue delay, but no later than 30 days from when Supplier becoming aware of the vulnerability, and (2) for any and all "Critical" vulnerabilities, "High" vulnerabilities that are known to have been exploited or that gained significant public attention (e.g., reported by multiple media outlets, publications by security researchers are being broadly circulated on social media, etc.), without undue delay, but no later than 7 days from becoming aware of the vulnerability.

5.3. **Notice of Vulnerabilities in Entrusted Systems.** Supplier shall immediately notify Cisco of any vulnerabilities that it knows or reasonably suspects to exist in any Entrusted Systems. Supplier shall send such notice by email to psirt@cisco.com.

5.4. **Cooperation and Assistance.** Supplier shall promptly provide Cisco with all information, cooperation and assistance reasonably requested by Cisco to address vulnerabilities in the Products and Services, including (i) assisting Cisco in investigating known or suspected vulnerabilities, (ii) coordination of public disclosures of vulnerabilities that impact Cisco Offerings, and using commercially reasonable efforts to respond to Cisco's requests expeditiously, but no later than 48 hours.

5.5. **Third Party Coordination Center.** If a third-party coordination center (i.e., the Computer Emergency Response Team/Coordination Center or National Infrastructure Security Co-ordination Center) coordinates the response and disclosure for multiple vendors of a vulnerability, Supplier will cooperate and work in good faith with Cisco (as applicable) and the third-party coordination center.

5.6. **Right to Disclose Vulnerabilities.** Notwithstanding any other term of the Agreement, in the event any vulnerability related to a Product or Service impacts any Cisco Offerings, Cisco may publicly disclose such vulnerabilities and publish or otherwise distribute any corresponding fixes, workarounds, or mitigations provided or recommended by Supplier.

6. **Software Bill of Materials.** Upon Cisco's request, Supplier shall provide Cisco with Software Bills of Materials ("***SBOMs***") for all Software (including firmware, operating systems and applications) that it provides to Cisco pursuant to this Agreement. Each SBOM must (i) be cryptographically signed by Supplier, (ii) be in a machine-readable format, (iii) contain all elements specified in the National Telecommunications and Information Administration's "The Minimum Elements for a Software Bill of Materials (SBOM)" available at https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf (or any successor thereto), and (iv) be created using the version of the Software Package Data Exchange Standard formatting standard or CycloneDX formatting standard in effect at the time the SBOM is produced.

7. **Business Continuity/Disaster Recovery.** Supplier shall implement and maintain business continuity and disaster recovery policies and procedures for ensuring the continued provisioning of Products and Services without disruption in the event of a disaster or other disruptive events. Supplier shall test the sufficiency and efficacy of such plans at regular intervals, but no less than annually. In the event a test reveals any material deficiencies, Supplier shall promptly remediate such deficiencies. At Cisco's request, Supplier shall reasonably cooperate with Cisco's business continuity and disaster recovery testing exercises. Cisco and Supplier will discuss, in good faith, the timing and method of such exercises to help minimize the impact of such exercises on Supplier's operations while also helping to ensure compliance with Cisco's contractual and regulatory obligations. Supplier shall maintain appropriate data recovery procedures, including procedures for creating immutable backups of data (including Cisco Data) at appropriate intervals, in geographically diverse locations, and in a manner sufficient to reconstruct the data in its original state as found on the last recorded backup.

8. **PCI Requirements.** To the extent Supplier Services involve the Processing of Cardholder Data, Supplier represents and warrants that it will: (i) comply with the PCI Compliance Standards for so long as Supplier Processes Cardholder Data; and (ii) provide evidence of such compliance to Cisco upon request, including a current attestation of compliance signed by a reputable PCI Qualified Security Assessor.

9. **FedRAMP Requirements.** For those Services for which Supplier has been granted a FedRAMP authorization to operate, Supplier shall, throughout the duration of the relevant subscription term, maintain such authorization, not reduce the designated impact level (e.g., Low, Li-SaaS, Moderate, or High) for the Services, and fully comply with the FedRAMP baseline requirements that correspond to the designated impact level.

10. **Assessments and Audits.** Supplier shall promptly make available to Cisco such information, records, and documentation that Cisco determines to be reasonably necessary to assess Supplier's security practices and compliance with the Agreement, including this Exhibit. Additionally, Cisco may perform audits of Supplier's documents and records, and inspections of the facilities used by Supplier to develop or provide the Products and Services, to the extent Cisco reasonably determines such audits and inspections are necessary for Cisco to comply with its contractual, regulatory, and other legal obligations. Such audits and inspections will be conducted during Supplier's normal business hours and in a manner that helps to limit the disruption that such audits and inspections may have on Supplier's business operations. Cisco will not conduct audits or on-site inspections under this Section 10 (Audits and Assessments) more than once per year, unless Cisco determines that additional audits and inspections are reasonably necessary for it to comply with its contractual, regulatory, or other legal obligations.

11. **Investigating and Addressing Deficiencies, Weaknesses and Non-Compliance.** In the event Supplier learns of or suspects that any deficiencies or weaknesses, or areas of non-compliance (whether as a result of penetration testing, vulnerability scans, reports from Supplier Representatives, reports from Cisco or third-party security researchers or otherwise), Supplier shall immediately take steps to promptly and diligently investigate those deficiencies, weaknesses, and areas of non-compliance and sufficiently address them (including mitigating and remediating them, as appropriate). Upon request, Supplier shall (i) keep Cisco informed of the details and status of the mitigation and remedial measures to be implemented by Supplier and (ii) once the mitigation and remedial measures have been fully implemented, certify in writing that such measures have been fully implemented.

12. **Amendments.** Cisco may amend this Exhibit from time to time if, in its reasonable discretion, to address Cisco's regulatory, contractual and other legal requirements. Cisco will provide Supplier with notice of such amendments by publishing the amended version of this Exhibit to Cisco's Supplier Web Portal (https://www.cisco.com/c/en/us/about/supplier-information/access-manufacturing-supplier-connection/portal.html).

13. **Non-limiting Effect.** Supplier's obligations and Cisco's rights under this Exhibit shall be without prejudice to any other obligations that Supplier may have and rights and remedies that Cisco may have and shall not be deemed to limit or waive any rights or remedies that Cisco may have, whether in equity, under contract or at law.