This Technical and Organizational Security Measures Exhibit (the “TOM”) forms part of the Professional Services Subcontract Agreement between the parties (“Agreement”).

1. **Scope**

This TOM provides details of the information security expectations and requirements between Cisco and Subcontractor and describes the technical and organizational security measures that must be implemented by the Subcontractor to secure Protected Data (as defined below) prior to providing any Services or Deliverables, or engaging with Customers on behalf of Cisco.

2. **Definitions**

All capitalized terms not defined in the TOM have the meanings set forth in the Agreement and any appendices or exhibits thereto.

- **“Cisco Data”** means all information and data provided or made available to Subcontractor, including Customer information and data, any manipulation of that data and any data or information Subcontractor collects, generates, or otherwise obtains in connection with its performance of the Services. For clarity, to the extent Cisco Data contains Personal Data as defined by the Data Usage and Protection provision in the Agreement, the terms related to Personal Data will also apply.

- **“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.

- **“Protected Data”** means Cisco Data, Confidential Information, Customer Confidential Information and all Personal Data.

3. **General Security Practices**

3.1. Subcontractor has implemented and shall maintain appropriate technical and organizational measures to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this TOM for its personnel, equipment, and facilities at the Subcontractor locations providing any Services.

4. **General Compliance**

4.1. **Compliance.** The Subcontractor shall document and implement processes and procedures to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any 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 Subcontractor. The Subcontractor shall ensure that information security is implemented and operated in accordance with the Subcontractor’s organizational policies and procedures.

4.2. **Intellectual property rights.** Subcontractor shall implement appropriate procedures to ensure compliance with legislative, regulatory, and contractual requirements related to Intellectual Property Rights and use of proprietary software products.
4.3. **Protection of records.** Subcontractor shall protect records from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual, and business requirements.

4.4. **Independent review of information security.** Subcontractor’s approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

4.5. **Compliance with security policies and standards.** Subcontractor’s management shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

4.6. **Technical compliance review.** Subcontractor’s information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.

4.7. **Information Risk Management (“IRM”).** Risk assessment is the process of assessing potential business impact, evaluating threats and vulnerabilities, and selecting appropriate controls to meet the business requirements for information security. Subcontractor is required to have a risk management framework and conduct a yearly risk assessment of their environment and systems to understand their risks and apply appropriate controls to manage and mitigate the risks. Threat and vulnerability assessment must be periodically reviewed and remediation actions taken where material weaknesses are found. Subcontractor will provide Cisco with the reports and analysis as required, provided the disclosure of which would not violate Subcontractor’s own information security policies, or Applicable Laws.

5. **Technical and Organizational Measures for Security**

5.1. **Organization of Information Security**

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

   b. **Security Roles and Responsibilities.** Subcontractor shall ensure that all information security responsibilities are defined and allocated in accordance with Subcontractor’s approved policies for information security. Such policies shall be published and communicated to employees and relevant external parties.

   c. **Project Management.** Subcontractor shall ensure that information security be addressed in project management, regardless of the type of project to ensure that information security risks are identified and addressed as part of the project.

   d. **Risk Management.** Subcontractor shall have a risk management framework and conduct a yearly risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before processing Protected Data or offering its services.

5.2. **Human Resources Security**

   a. **General.** Subcontractor shall inform its personnel about relevant security procedures and their roles and ensure that personnel with access to Protected Data are subject to written confidentiality obligations. Subcontractor shall further inform its personnel of possible
consequences of breaching Subcontractor’s security policies and procedures, which must include disciplinary action, up to and including termination of employment for Subcontractor’s employees and termination of contract or assignment for Contractors and temporary personnel.

b. Training. Subcontractor personnel with access to Protected Data shall receive annual 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.

i. Training shall be provided before Subcontractor personnel have access to Protected Data or begin providing services.

ii. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards and other training materials.

c. Background Checks. In addition to any other terms in the Agreement related to this subject matter, Subcontractor shall perform criminal and other relevant background checks on its personnel in compliance with local laws.

5.3. Asset Management

a. Asset Inventory. Access to Protected Data shall be restricted to Subcontractor personnel authorized in writing to have such access.

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

c. Trusted Device Standards.

Subcontractor personnel shall:

i. Use trusted devices that are configured with security software (i.e., anti-virus, anti-malware, encryption, etc.) and protected against corruption, loss, or disclosure;

ii. Follow Cisco’s trusted device standards when accessing Protected Data or when having Protected Data in his/her 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 network through wired, wireless or remote access (the “network”). Devices that fail to comply with this standard will not be entitled to access to the network unless Cisco determines limited access is acceptable. Cisco’s network access policies establish requirements for physical and wireless network data ports that provide local network communications and telephony services.

Cisco’s trusted device standards include, at a minimum, the following requirements:

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

b. Devices must be configured for automatic patching. All OS and application security patches must be installed within four (4) weeks of release. Devices may be required to immediately install emergency patches as necessary;

c. Devices must be encrypted (i.e., full disk, endpoint encryption) and secured with a password/PIN screen lock with the automatic activation feature set to
ten (10) minutes or less. Users must lock the screen or log off when the device is unattended;

d. Devices must not be rooted or jailbroken;

e. Devices must be periodically scanned for restricted or prohibited software (e.g., peer-to-peer sharing and social media apps); and

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

iii. Not accept or store Protected Data on smartphones, tablets, USB drives, DVD/CDs, or other portable media without prior written authorization from Cisco; and

iv. Take measures to prevent accidental exposure of Protected Data, including using privacy filters on laptops when in areas where over-the-shoulder viewing of Protected Data is possible.

5.4. Personnel Access Controls

a. Access.

i. Limited Use. Subcontractor understands and acknowledges that Cisco and Cisco’s customers are providing access to sensitive and proprietary information and access to computer systems to Subcontractor in order to perform the Services. Subcontractor represents and warrants that it will not access the Protected Data or computer systems for any purpose other than as necessary to perform the Services; and Subcontractor will not use any system access information (such as usernames or passwords) to gain unauthorized access to Protected Data or Cisco or its customers’ systems, or to exceed the scope of any authorized access.

ii. Authorization. Subcontractor shall restrict access to Protected Data and systems at all times solely to those individual Contractors whose access is essential to performing the Services.

iii. Suspension or Termination of Access Rights. At Cisco’s request, Subcontractor shall immediately suspend or terminate the access rights to Protected Data and systems for any Subcontractor’s personnel or its Contractors suspected of breaching any of the provisions of this TOM; and Subcontractor shall remove access rights of all employees and external party users upon suspension or termination of their employment, contract, or agreement.

b. Access Policy. Subcontractor shall determine appropriate access control rules, rights, and restrictions for each specific user’s roles towards their assets. Subcontractor shall maintain a record of security privileges of its personnel that have access to Protected Data, networks, and network services. Subcontractor shall restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.


i. Subcontractor shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Cisco’s and customers’ systems and networks. Subcontractor shall use an enterprise access control system
that requires its personnel revalidation by managers at regular intervals based on the principle of “least privilege” and need-to-know criteria based on job role.

ii. Subcontractor shall maintain and update a record of personnel authorized to access systems that contain Protected Data and Subcontractor shall review users’ access rights at regular intervals.

iii. For systems that process Protected Data, Subcontractor shall revalidate access of users who change reporting structure and deactivates authentication credentials that have not been used for a period of time not to exceed six (6) months.

iv. Subcontractor shall ensure that access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, will be restricted in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

d. Network Design. For systems that process Protected Data, Subcontractor shall have controls to avoid personnel assuming access rights they have not been assigned to gain unauthorized access to Protected Data.

e. Least Privilege. Subcontractor shall limit access to Protected Data to those personnel performing the Services and, to the extent technical support is needed, its personnel performing such technical support.

f. Authentication

i. Subcontractor shall use industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Subcontractor shall require that the passwords are renewed regularly, no less often than every six (6) months.

ii. Where authentication mechanisms are based on passwords, Subcontractor shall require the password to conform to very strong password control parameters (e.g., biometrics, multi-factor authentication, length, character complexity, and/or non-repeatability).

iii. Subcontractor shall ensure that de-activated or expired identifiers are not granted to other individuals.

iv. Subcontractor shall monitor repeated attempts to gain access to the information system using an invalid password.

v. Subcontractor shall maintain industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

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

5.5. Cryptography

a. Cryptographic controls policy
i. Subcontractor shall have a policy on the use of cryptographic controls based on assessed risks.

ii. Subcontractor shall assess and manage the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecates and disallows usage of weak cypher suites, and mathematically insufficient block lengths and bit lengths.

iii. Subcontractor’s cryptographic controls/policy shall address appropriate algorithm selections, key management and other core features of cryptographic implementations.

b. **Key management.** Subcontractor 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.

5.6. **Physical and Environmental Security**

a. **Physical Access to Facilities**

i. Subcontractor shall limit access to facilities where systems that process Protected Data are located to authorize individuals.

ii. Security perimeters shall be defined and used to protect areas that contain both sensitive, or critical information and information 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. Subcontractor must register personnel and require them to carry appropriate identification badges.

b. **Physical Access to Equipment.** Subcontractor equipment that is located off premises shall be protected using industry standard process to limit access to authorized individuals.

c. **Protection from Disruptions.** Subcontractor shall use a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

d. **Clear Desk.** Subcontractor shall have policies requiring a "clean desk/clear screen".

5.7. **Operations Security**

a. **Operational Policy.** Subcontractor 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. Subcontractor shall ensure the policies are communicated to all persons involved in the processing of Protected Data. Compliance with such policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of Protected Data requires appropriate management structure and control.

b. **Security and Processing Controls.**

i. **Areas.** Subcontractor shall maintain, document, and make available standards and procedures to address the configuration, operation, and management of systems and networks, services, and Protected Data.
ii. **Standards and Procedures.** The standards and procedures shall include: security controls; identification and patching of security vulnerabilities; change control process and procedures; problem management; and incident detection and management.

c. **Logging and Monitoring.** Subcontractor shall maintain logs of administrator and operator activity and data recovery events.

5.8. **Communications Security and Data Transfer**

a. **Networks.** Subcontractor shall, at a minimum, use the following controls to secure its networks that access Cisco or customer servers which store Protected Data:

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

ii. Access to network devices for administration must utilize a minimum of 256-bit, industry standard encryption.

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

iv. Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 7 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days.

v. Initial user passwords are required to be changed during the first logon. Subcontractor shall have a policy prohibiting the sharing of user IDs and passwords.

vi. Firewalls must be deployed to protect the perimeter of Cisco and customers’ networks.

b. **Virtual Private Networks ("VPN").** When remote connectivity to the Cisco network is required for processing of Protected Data, Subcontractor shall use VPN servers for the remote access with the following or similar capabilities:

i. Connections must be encrypted using a minimum of 256-bit encryption.

ii. Connections from Cisco or its customers to Subcontractor locations shall only be established using the Cisco VPN servers.

iii. The use of multi-factor authentication is required.

c. **Data Transfer.** Subcontractor 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 TOM. Such policies shall be designed to protect transferred information from interception, copying, modification, corruption, mis-routing and destruction.

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

a. **Security Requirements.** Subcontractor shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.
b. **Development Requirements.** Subcontractor shall have policies for secure development, system engineering, and support. Subcontractor shall conduct appropriate tests for system security as part of acceptance testing processes Subcontractor shall supervise and monitor the activity of outsourced system development.

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

a. **Testing.** Subcontractor will perform annual penetration test on their internet perimeter network. Audits will be conducted by the Subcontractor compliance team using industry recommended network security tools to identify vulnerability information. Upon request from Cisco, Subcontractor can provide a Vulnerability & Penetration testing report at an organization level which will include an executive summary and not the details of actual findings.

b. **Audits.** Subcontractor shall respond promptly to all reasonable security audit, scanning, discovery, and testing reports requested from Cisco, or from regulators (to the extent required by law) and shall cooperate and assist those regulators as required by law.

c. **Remedial Action.** If any audit or penetration testing exercise referred to above reveals any deficiencies, weaknesses or areas of non-compliance, Subcontractor shall promptly take such steps as may be required to remedy those deficiencies, weaknesses and areas of non-compliance as soon as may be practicable in the circumstances and in any case within three (3) months of the findings from the audit and/or test.

d. **Status of Remedial Action.** Subcontractor shall keep Cisco informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Cisco as soon as may be practicable in the circumstances that all remedial actions have been completed.

5.11. **Contractor Relationships**

a. **Policies.** Subcontractor shall have information security policies or procedures for its use of Contractors that impose requirements consistent with this TOM. Such policies shall be reviewed at planned intervals or if significant changes occur. Subcontractor shall have agreements with Contractors in which they agree to comply with Cisco’s and/or Subcontractor’s security requirements. Agreements with Contractors shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

b. **Monitoring.** Subcontractor shall monitor and audit service delivery by its Contractors and review security against the agreements with Contractors. Subcontractor shall manage changes in Contractor services that may have an impact on security.

5.12. **Management of Information Security Incidents and Improvements**

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

b. **Reporting Information Security Incident.** Subcontractor shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as possible. All employees and Contractors should be made aware of their responsibility to report Information Security Incidents as quickly as possible.
c. **Reporting Information Security Weaknesses.** Subcontractors, employees, and Contractors using information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.

d. **Assessment of and Decision on Information Security Events.** Subcontractor 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 is based on the impact and extent of an incident.

e. **Response Process.** Subcontractor shall maintain a record of Information Security Incidents with a description of the incident, the consequences 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 correct future security incidents.

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

a. **Planning.** Subcontractor shall maintain emergency and contingency plans for the facilities in which Subcontractor information systems that process Protected Data are located. To ensure that they are valid and effective during adverse situations, Subcontractor shall verify the established and implemented information security continuity controls at regular intervals.

b. **Data Recovery.** Subcontractor’s redundant storage and its procedures for recovering data shall be designed to reconstruct Protected Data in its original state from before the time it was lost or destroyed.

6. **Notification and Communication Obligations**

6.1. **Notification.** Subcontractor shall immediately (i.e., within 24 hours) notify Cisco’s Data Protection Incident Remedy team at:

    [data-incident-command@cisco.com](mailto:data-incident-command@cisco.com)

    if any of the following events occur:

    i. any Information Security Incident or compromise of Protected Data;
    
    ii. any security vulnerability, or weakness in Cisco’s or Customers’ systems, or networks, or Subcontractor’s systems or networks that could allow an attacker to compromise the integrity, availability, or confidentiality of the Protected Data;
    
    iii. an Information Security Incident that compromises or could compromise the security of information and weaken or impair business operations;
    
    iv. an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of information that is processed, stored and transmitted using a computer in connection with Protected Data; or
    
    v. failure or inability to maintain compliance with the requirements of this TOM or Applicable Laws.

6.2. **Cooperation**

    a. Subcontractor shall: (i) respond promptly to any Cisco communication(s); and (ii) provide all information, cooperation, and assistance to a Cisco designated response center.
6.3. **Information Security Communication**

a. Except as required by Applicable Laws, Subcontractor agrees that it will not inform any third party of any of the events described above in this Section without Cisco’s prior written consent. Subcontractor shall fully cooperate with Cisco and any customer and with legal enforcement authorities concerning any actual or potential unauthorized access to Cisco’s or customer’s systems or networks, or Protected Data. Such co-operation shall include the retention of all information and data within Subcontractor’s possession, custody, or control that is related to any Information Security Incident. If disclosure is required by law, Subcontractor will work with Cisco regarding the content of the disclosure to minimize any potential adverse impact upon Cisco and its customers. Subcontractor will bear the cost of reproduction or any other remedial steps necessary or advisable to address the suspected or actual incident or compromise.

6.4. **Post-Incident**

a. Subcontractor shall cooperate with Cisco in any post-incident investigation, remediation, and communication efforts. In addition, Subcontractor shall conduct a forensic and security review and audit in connection with any such Information Security Incident and, if appropriate to the nature and scope of the incident, retain an independent third party auditor to perform an audit or assessment of Subcontractor’s information security procedures, systems, and network, including: testing of the system of controls; appropriate systems implementation and vulnerability analysis and penetration testing. In the event of the identification of any material security-related risk by Subcontractor, or the third party auditor, Subcontractor shall take timely remedial action based on industry best practices and the results of such assessment, audit or risk identification.