Offer Description: Cisco Secure Managed Remote Access

This Offer Description (the **"Offer Description"**) describes Cisco Secure Managed Remote Access Service (the **"Cloud Service"**). Your subscription is governed by this Offer Description and the Cisco End User License Agreement located at www.cisco.com/go/eula (the "EULA") (or similar terms existing between you and Cisco) (the **"Agreement"**). Capitalized terms used in this Offer Description and not otherwise defined herein have the meaning given to them in the Agreement.

1. Description

1.1. Summary

Cisco Secure Managed Remote Access Service consists of the following:

- VPN access through Cisco hosted infrastructure
  - Uses Cisco AnyConnect VPN client software ("AnyConnect"), purchased and licensed separately
- Use of a virtual firewall
- Use of a cloud-based service portals for virtual private network monitoring and for problem and incident management (collectively, the "Portal")
- 24x7 continuous Cloud Service monitoring performance metrics, and alerting
- Cloud-based, scalable, infrastructure, configured for high resiliency and connected to a scalable, redundant, cloud-based infrastructure, designed to provide scalable remote access
- Establish and monitor site-to site-connectivity, providing secure access to Your systems and applications to locations defined as "sites"
- One or more sites can be configured for diversity, redundancy, and bandwidth requirements through optional sites configured
- **Optional Additional Configurations**: the following additional configurations can be enabled by remotely modifying the AnyConnect client on Your end devices:
  - Cisco Umbrella
  - Cisco Secure Network Analytics (Network Visibility Module)

1.2. Portal

The Portal allows You to view and manage Your end users, review reports, create review support tickets, and other Cloud Service-related information Here is a summary of its capabilities:

- The Portal provides Your the following information from each Remote Access VPN session:
  - The total number of active remote access VPN sessions and the number of currently connected users in Your tenant.
  - Basic information about devices connected via the VPN (mobile, laptop, etc.).
  - The username, login time, duration, and the amount of time the session has been active.
  - The assigned IP address within the enterprise network and the public IP address with which the session was initiated.
  - The connection profile and group policy information associated with a session.
  - The AnyConnect version and operating system type used in a user session.
  - The idle time remaining before the session timeout.
  - The volume of data received and transferred over a specified period.

- This system utilizes single sign-on access to authorized users.
- In addition, the Portal links to the following additional capabilities:
    - The ability to submit an Incident
    - Incidents or Requests by Category
    - Incidents by Priority
    - Trending on both of the Above
    - Incidents Aging status (i.e., how long tickets are still open)

Note: You are responsible for managing end user access to the Portal and requests submitted by Your requestors are deemed to be authorized by You.

1.3. Service Components

- **Service Transition and Activation.** Cisco will provide instruction and guidance to activate the initial configuration of the Cloud Service, which includes configuring the AnyConnect software.
    - Cisco will guide You through a checklist of required steps to configure the Cloud Service and confirm it is functioning and ready for use.
    - After configuring the Cloud Service, You and Cisco will conduct tests to verify the Cloud Service is available and the Portal are accessible and functioning. This will "Activate" the Cloud Service.
    - The parties will perform their responsibilities in the quick start guide so that the Cloud Service can be Activated.

- **Change Management.** Cisco will manage the lifecycle (i.e. planning, testing, backout, and post-change checks) of the deployment of approved technical changes (e.g., ex. Routing, Dynamic Access Policy (DAP), backhaul VPN configuration) to the Cloud Service or changes required to restore the Cloud Service.
    - Cisco will manage AnyConnect profile adjustments (may require service outage or reactivation).
    - Cisco will make changes required to resolve an Incident or changes requested by You and listed in the service catalog. Services not listed in the services catalog may be subject to additional terms and charges.
    - If Cisco is unable to perform all elements of the Change remotely, You will assist Cisco in performing the Changes (with Cisco guidance).
    - You are responsible for reviewing and mitigating any impacts to out-of-scope devices or services as a result of any changes to the Cloud Service.

1.4. Optional Additional Configurations

The following Cloud Services and software components are optional and may be purchased for an additional fee:

- **Cisco Umbrella**: Before users connect to any online destination, Cisco Umbrella acts as a secure onramp to the internet and delivers deep inspection and control to support compliance and block threats. Depending on the package and deployment, Cisco Umbrella integrates secure web gateway, cloud-delivered firewall, DNS-layer security, cloud malware protection, application discovery, in-line data loss prevention (DLP), remote browser isolation (RBI) and more, for effective protection anywhere users go.
    - Additional details on the optional Cisco Umbrella service and its terms can be found at: https://umbrella.cisco.com.

- **Cisco Secure Network Analytics (formerly, StealthWatch Enterprise)**: performs behavior anomaly detection on network connected devices and users on the customer premises and in public clouds to

automatically detect early indicators of compromise such as insider threat activity, malware and multistaged attacks.

- Additional details on the optional Cisco StealthWatch service and its terms can be found at: https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html.

2. Supplemental Terms and Conditions

2.1. AnyConnect Licensing

You must have the appropriate AnyConnect licenses to Activate and use the Cloud Service. AnyConnect licenses are not included with the Cloud Service and must be purchased and licensed separately.

2.2. General Customer Responsibilities

Cisco's provision of the Cloud Service is dependent on Your compliance with Section 1.3 above and Cisco will not be liable for your failure to comply..

2.3. Disclaimers

CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICE WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICE WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD-PARTY MALICIOUS ATTACKS. CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD PARTY SYSTEM OR SERVICE TO WHICH A CLOUD SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS

3. Data Protection

The Cisco Cisco SecureManaged Remote Access Privacy Data Sheet (available here) describes the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services. For further information on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center.

4. Support & Maintenance

The Cloud Services include online support and phone support. Cisco will respond as set forth in the table below and may require information from you to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Online Support allows access for support and troubleshooting via online tools, email and web case submission only. No telephone access is provided. Case severity or escalation guidelines are not applicable. Cisco will respond to a submitted case no later than the next business day during standard business hours.

Phone Support provides Cisco Technical Assistance Center (TAC) access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues. Cisco will respond within one (1) hour for Severity 1 and 2 calls received. For Severity 3 and 4 calls, Cisco will respond no later than the next business day.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

If you have access to Software with the Cloud Services, Cisco will provide (i) work-around solutions or patches to reported problems and (ii) major, minor and maintenance releases of the licensed Software version, which can be accessed on Cisco Software Central. You may be required to update to the latest Software release to correct a reported Software problem.

The below table outlines Cisco's response objectives based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Basic with Phone Support	24x7 via Phone & Web	Response within 1 hour	Response within next Business Day
Basic with Online Support	Web	Response to all cases within next Business Day during Standard Business Hours	

The following definitions apply to this Section.

Response time means the time between case submission in the case management system to support engineer contact.

Severity 1 means the Cloud Service is unavailable or down or there is a critical impact to a significant impact to Case Submitter's business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

Severity 2 means the Cloud Service is degraded or significant aspects of Case Submitter's business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

Severity 3 means the Cloud Service is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

Severity 4 means minor intermittent functionality or performance issue, or information is required on the Cloud Service. There is little or no impact to Case Submitter's business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

Business Day means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco.

Local Time means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

Standard Business Hours means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.

Your access to and use of the Cloud Services may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service or other security breach, or operational incidents.