

**PRODUCT-SPECIFIC ATTACHMENT
MASERGY UNIFIED THREAT MANAGEMENT (UTM)**

ATTACHMENT IDENTIFIER: Masergy UTM, Ver. 2.0

The following additional terms and conditions are applicable to Service Order Forms for the Masergy Unified Threat Management Services ("UTM") ordered under a Master Service Agreement:

DEFINITIONS

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Master Service Agreement.

"Architectural Confirmation Document" or **"ACD"** means the document containing the initial configuration for the Services, as agreed to by Customer and Masergy.

"Base Service" means the SD-WAN Service provided by Masergy.

"Masergy Data" means any and all data provided to Customer by Masergy, Masergy's Affiliates, or Masergy's vendors or that is collected by Customer or its subcontractors on Masergy's behalf.

"Masergy Systems" means applications, websites, computing assets, systems, databases, devices, products, or services owned or operated by or for Masergy.

"Customer Premises Equipment" or "CPE" means the hardware appliance or other endpoint device installed at the Service Location as part of the Base Service. CPE constitutes Masergy Equipment.

"Customer Devices" means computing, storage, or networking devices operated by or on behalf of Customer that Process Masergy Data or that are used to access Masergy Systems.

"Customer System" means any Customer or its subcontractors' applications, websites, computing assets, systems, databases, devices, products, or services that Process Masergy Data.

"Estimated Availability Date" means the target date for delivery of Service.

"Information Security Standards" means prescribed for use by the National Institute of Standards and Technology, aligned with the International Organization for Standardization/International Electrotechnical Commission 27000 series of standards.

"Masergy" means Masergy Communications, Inc. or one of its applicable operating affiliates or subsidiaries by which the Service is provided.

"Process" and its cognates means any operation or set of operations that is performed on information, including collection,

storage, transmission, disclosure, erasure, and destruction.

"Service(s)" means UTM enabled managed firewall services as described in Schedule A-1 hereto.

"UTM Fortinet" means UTM Service with Fortinet as the UTM vendor.

"UTM Meraki" means UTM Service with Meraki as the UTM vendor.

"Underlay Service" means the internet connectivity over which the Service operates.

ARTICLE 1. SERVICES

This attachment shall apply to the Services. A further description of the Services is set forth in Schedule A-1 hereto which is incorporated herein by reference.

ARTICLE 2. PROVIDER

The Service is provided by Masergy and Customer may be invoiced for the Services by Masergy.

ARTICLE 3. PROVISIONING INTERVAL

Following Masergy's acceptance of a Service Order Form, Masergy shall notify Customer of the Estimated Availability Date applicable to that Service Order Form. Masergy shall use commercially reasonable efforts to provision the Service on or about the Estimated Availability Date; provided, however, that Masergy's failure to provision Services by the Estimated Availability Date shall not constitute a breach of the Agreement.

ARTICLE 4. SERVICE COMMENCEMENT DATE

Charges for the Services shall begin to accrue on the Service Commencement Date. The Service Commencement Date shall be the date Masergy informs Customer that the Service is available. A single Service Order Form containing multiple Service Locations or Services may have multiple Service Commencement Dates.

ARTICLE 5. TERMINATION CHARGES; PORTABILITY

5.1 The charges set forth or referenced in each Service Order Form have been extended to Customer in reliance on the Service Term.

5.2 Termination Charges.

A. Subject to Sections 5.2(C) and 5.2(D), in the event that a Service is terminated following Masergy's acceptance of the applicable Service Order Form, but prior to the Service Commencement Date, Customer shall pay Termination Charges equal to one hundred and twenty percent (120%) of the costs and expenses incurred by Masergy in installing or preparing to install the Service.

B. Subject to Sections 5.2(C) and 5.2(D), in the event that a Service is terminated on or following the Service Commencement Date, but prior to the end of the applicable Service Term, Customer shall pay: (a) all unpaid non-recurring Charges, excluding any waived charges, specified in any Service Order Form; (b) all unpaid recurring charges for Services specified in any Service Order Form through the date of termination; (c) one hundred percent (100%) of all recurring charges for canceled or terminated Services specified in the related Service Order Form for the balance of the Initial Service Term or the current Extension Service Term of such Service; and (d) all fees related to the canceled or terminated Services that Masergy is charged by any and all third parties that Masergy is unable to avoid after using commercially reasonable efforts, including without limitation, all termination charges due to any and all third-party service providers; provided, however, that such third-party fees will not be separately charged if they are included in fees paid pursuant to subsection (c) of this Section.

Termination Charges shall be immediately due and payable upon cancellation or termination, and shall be in addition to any and all accrued and unpaid charges for the Service rendered by Masergy through the date of such cancellation or termination.

C. Termination Charges shall not apply to Service(s) terminated by Customer as a result of Masergy's material and uncured breach in accordance with the Master Service Agreement.

D. Customer acknowledges and agrees that termination of either the Masergy-provided Underlay Service or the Base Service shall constitute a termination of the Services and Customer shall pay Termination Charges with respect to the Services as provided herein; provided, that, if Customer terminated such Underlay Service or the Base Service as a result of Masergy's material and uncured breach in accordance with the Master Service Agreement applicable hereto, then Customer will not be obliged to pay Termination Charges with respect to the Service.

ARTICLE 6. ADDITIONAL INFORMATION

If Customer's Underlay Service is provided by a third-party, Customer's Base Service must be interconnected with such third-party provided Underlay Service in accordance with the applicable PSA.

ARTICLE 7. CUSTOMER PORTAL

Masergy provides the Customer with a password-protected web portal ("**Portal**") to access information regarding the Customer's Service. UTM Meraki Customers may have the option to use the Portal to enter changes to Customer's UTM configuration, subject to the availability of the configuration service, as determined by Masergy.

ARTICLE 8. INFORMATION SECURITY REQUIREMENTS

8.1 Access to Masergy Systems. Customer must meet the following requirements with respect to its access to any Masergy Systems:

A. Customer must use reasonable identity and access management processes that meet or exceed Information Security Standards;

B. Customer must use unique user/system identities and must prohibit the use of shared, default, or temporary credentials;

C. Customer must terminate the access of any end user or, if unable to terminate directly, must notify Masergy within twenty-four (24) hours, if an end user no longer needs access to a Masergy System;

D. Customer devices must lock after a reasonable period of inactivity and must disable upon repeated, failed access attempts;

E. Customer must periodically conduct user access reviews no less frequently than every six (6) months and must cooperate with any access reviews conducted by Masergy;

F. Customer may only access Masergy Systems to the extent necessary to Process Masergy Data;

G. Customer must comply with all security requirements when accessing Masergy Systems, which may include Masergy virtual private networks, transport encryption, and multi-factor authentication;

H. Only approved connections to a Masergy System using the Masergy approved protocols and services may be used;

I. Upon request, Customer must document the ports, rules, and protocols acceptable to Masergy; and

J. Masergy may suspend or terminate access to a Masergy System without notice and without penalty.

8.2 Maintenance. If the Services require the reconfiguration of Customer Systems or Masergy Systems for maintenance or support, when such configurations are no longer necessary or upon Masergy request, Customer must revert such reconfigurations. To the extent that only Masergy can make such reconfigurations, Customer must inform Masergy and assist Masergy in making such reconfigurations.

8.3 Customer Devices. Customer must implement and maintain reasonable security standards for all Customer devices that meet or exceed Information Security Standards, including but not limited to timely patch management, and (A) usage of next generation threat detection or (B) real time anti-virus monitoring and updates and full scans (including system and boot files) as frequently as recommended by Information Security Standards. All Customer devices must be owned or leased and managed by Customer or its subcontractors. Customer must only Process Masergy Data or access Masergy Systems from Customer Devices or devices provided by Masergy. Customer must maintain device management controls for all mobile Customer Devices with access to a Masergy System. Such controls must include the ability to wipe the device remotely.

8.4 Customer End Users. Customer is responsible for the acts and omissions of all end users. Customer must ensure that end users do not retain any Masergy Data, any Masergy device, or access to any Masergy System at the request of Masergy.

**PRODUCT-SPECIFIC ATTACHMENT
MASERGY UNIFIED THREAT MANAGEMENT (UTM)**

**SCHEDULE A-1
SERVICE DESCRIPTIONS**

The Service will be provided in accordance with the service descriptions set forth below:

1. Service Descriptions

The Service, which is a premises-based solution, helps Customer maintain perimeter security of, manage, and continuously monitor its firewalls.

The Service is provided from secure facilities that operate on a 24x7x365 basis.

The Service includes standard design consultation, initial setup and installation and integration of the managed firewall with the CPE (as defined and further described in Section 3 below). System updates, policy and rule changes are also available with the Service, but may be subject to additional fees. For clarity, any additional services beyond standard design consultation, initial setup and installation and integration of the managed firewall with the CPE will be subject to additional fees.

UTM Fortinet includes the following standard features. UTM Fortinet may also be referred to as Unified Threat Protection (UTP).

- A. Next Generation Firewall
 - i. Source, destination, application/protocol enforcement.
- B. Web Filtering
 - i. Based on automatic security intelligence tools and targeted threat analysis, real-time updates designed to enable Customer to apply granular policies that filter web access based on content categories.
- C. Intrusion Prevention Service (IPS)
 - i. Implements a database of thousands of signatures, designed to stop attacks that evade conventional firewall defenses.
- D. Anti-Virus Service
 - i. Employs advanced virus, spyware, and heuristic detection engines designed to protect endpoint security agents, to help prevent both new and evolving threats from gaining access to Customer's network's content and applications.
- E. Malware Service
 - i. Cloud-based threat analysis service that provides analysis and helps prevent for zero-day exploits and malware.
- F. Application Control
 - i. Protection of managed desktops and servers by allowing or denying network applications based on enforced policies.

UTM Meraki includes the following standard features.

- A. Next Generation Firewall
 - i. Source, destination, application/protocol enforcement.
- B. Web Filtering
 - i. Web Category, Specific URL, URL pattern blocking. Safe search and YouTube restriction
 - ii. Based on Talos security intelligence updates and targeted threat analysis; real-time updates designed
- C. Intrusion Prevention Service (IPS)
 - i. Real time integration from SNORT database of thousands of signatures, auto signature download designed to add firewall defenses.
- D. Advanced Malware Protection (AMP) Service
 - i. Scans and blocks HTTP file downloads based on behavior based malware detection.

2. Service Requirements

In order to provide the Service to a Customer's Service Location, the Service Location must have an Underlay Service and Base Service. With respect to the Underlay Service, Masergy supports the Service over Masergy Ethernet Dedicated Internet (EDI) Service, Masergy Business Internet Service, or internet connectivity services provided by a third-party service provider. If the Base Service or Underlay Service is terminated at a Service Location or unavailable for any reason at any time, the Service at such Service Location will be inoperable.

3. Service Delivery and Service Management

- 3.1 **Kick-off Call**: Masergy will sponsor a kick-off call with Customer to explain the Service delivery process.
- 3.2 **Technical Interview**: Masergy will engage Customer in one or several interviews related to Customer's network design initiatives. Masergy will document the technical information discovered through the interview process into an Architectural Confirmation Document and the Customer will review and confirm that the ACD is accurate. The ACD will be available via the Portal.
- 3.3 **Configuration**: Customer's Service will be provided with a standard set of pre-configured policies.
- 3.4 **On-Going Solution Support**: If Masergy or a Masergy vendor develops software updates and/or security patches for Masergy's or such vendor's equipment which Masergy uses to provide the Services, Masergy will upload such software updates and/or security patches to the applicable equipment to the extent Masergy determines, in its sole discretion, that such software updates and/or security patches are necessary. Updates or patches that are viewed as critical may require immediate action with a maintenance window. For the avoidance of doubt, Masergy shall have no obligation to develop software updates or security patches and its only obligation under this paragraph is to install updates and security patches developed by its applicable vendors to the extent Masergy determines, in its sole discretion, that such software updates and/or security patches are necessary.
- 3.5 **Security Monitoring and Mitigation**: The Service is designed to provide Customer notice of potential security threats detected by the Service; provided, however, that (A) the Service's failure to provide any such notice(s) shall not constitute a breach of the Agreement and (B) Masergy and its affiliates and their respective officers, directors, employees, agents, suppliers, licensors, successors, and assigns shall have no liability to Customer for any damages that are alleged to or arise from or are caused by or alleged to have been caused by the failure to provide any such notice(s). Furthermore, Customer acknowledges and agrees that (i) Masergy will not make changes to Customer's configurations or security settings for the Services (including in response to any potential security threats of which Masergy has notified Customer) and (ii) Customer maintains overall responsibility and liability for maintaining the security, confidentiality, and reliability of Customer's network, computer systems, and data, including implementing configuration changes to the Services in response to potential security threats. Customer further acknowledges that the Services are not a guaranty by Masergy to protect Customer's network, computer systems, or data against unauthorized access, malicious code, deleterious routines, threats, cyberattacks, ransomware and/or other techniques, attack vectors and/or tools employed by computer "hackers" and other third parties (including nation states) to create, exploit, or expose security vulnerabilities. Masergy makes no warranty, express or implied, that any specific or all security threats and vulnerabilities will be detected or mitigated or that the Services will render Customer's network and computer systems safe from intrusions and other security breaches. Masergy makes no guarantees with respect to the detection or blocking of viruses/worms/malware or any other types of attacks and is not responsible for any such malicious data that may be transmitted over the provided network. Masergy makes no warranty that the Services will be uninterrupted or error-free. The Service constitutes only one component of Customer's overall security program and is not a comprehensive security solution.

4. Additional Terms for Cisco Products

The Service is subject to the then-current, additional terms and consents for Cisco Products located at <https://business.comcast.com/enterprise/terms-conditions> ("Additional Terms for Cisco Products").

5. Customer Responsibilities

Customer shall have the following responsibilities related to the installation, support, and maintenance of the Service.

- 5.1 Provide an operating environment with temperatures not below fifty-five (55) or above eighty-five (85) degrees Fahrenheit. Humidity shall not exceed ninety (90) percent at eighty-five (85) degrees Fahrenheit.
- 5.2 Provide secure space sufficient for access to one (1) standard, freestanding, equipment cabinet at each of the Customer facilities, no further than fifty (50) feet from the Customer router or switch interface.
- 5.3 Provide power including UPS AC power equipment, circuit sizing to be determined, if applicable.
- 5.4 Provide emergency local generator backup service, if applicable.
- 5.5 Provide access to the buildings and point of demarcation at each Service Location to allow Masergy and its approved contractors to install Masergy Equipment. Provide access to each location for regular (8am - 5pm) and emergency (24 hour) service and

maintenance of Masergy's equipment and facilities.

- 5.6 If interfacing with a third-party IP service, provide, install and maintain a device that is capable of routing network traffic between the Service and the Customer's Wide Area Network.
- 5.7 Customer must provide a point of contact (POC) for installation, service activation, notices for service interruptions, and any maintenance activities.

6. **Technical Support and Maintenance**

- 6.1 **Technical Support.** Masergy provides Customers a toll-free trouble reporting telephone number that operates on a 24x7x365 basis. Masergy provides technical support for service-related inquiries. Technical support will not offer consulting or advice on issues relating to non-Masergy Equipment.
- 6.2 **Maintenance.** Masergy's standard maintenance window is Sunday to Saturday from 12:00am to 6:00am local time. Scheduled maintenance is performed during the maintenance window and will be coordinated between Masergy and the Customer. Masergy provides a minimum of forty-eight (48) hour notice for non-service impacting scheduled maintenance. Masergy provides a minimum of seven (7) days' notice for service impacting planned maintenance. Emergency maintenance is performed as needed.