Fusion Managed Remote Access VPN and Multi-Factor Authentication Service Addendum

The additional terms and conditions set forth in this Fusion Remote Access VPN and Multi-Factor Authentication Service Addendum (the "**Remote Access VPN and Multi-Factor Authentication Service Addendum**") apply to Fusion's Managed SD-WAN and Managed Security Services (the "**Services**") and supplement the terms and conditions set forth in the Master Services Agreement (the "**MSA**") executed by Customer with Fusion or the Basic Terms and Conditions (the "**Basic Terms and Conditions**") incorporated by reference into the Service Order signed by Customer with Fusion for the purchase of the Services. This Remote Access VPN and Multi-Factor Authentication Service Addendum, together with the MSA or Basic Terms and Conditions, as applicable, and the Service Order are herein collectively referred to as the "Agreement". For purposes of this Remote Access VPN and Multi-Factor Authentication Service Addendum, "Fusion" means the subsidiary of Fusion Connect, Inc., a Delaware corporation, that provides the Services in the applicable state to Customer. Capitalized terms used in this Remote Access VPN and Multi-Factor Authentication Service Addendum and not otherwise defined herein have the meaning given each such term in the MSA or Basic Terms and Conditions, as applicable.

1. Service Description. Fusion's Remote Access VPN ("**RAVPN**") Service utilizes industry leading technologies to allow remote workers to securely access the managed private network currently under management by Fusion. Fusion utilizes existing managed security infrastructure (either via the cloud or a premise-based solution) to terminate VPN tunnels originating from remote workers' VPN clients to secure communication between remote users and Customer's private networks. By default, the VPN Service utilizes split tunneling, routing only traffic destined for the Customer's network inside the tunnel, with all public traffic being routed outside of the VPN. The Services is billed based on the total number of named users in a given billing cycle. Fusion provides Multi-Factor Authentication ("**MFA**") to validate the identity of users attempting to connect to the VPN Service. The MFA application prompts users to verify they are attempting to access the Service via a mobile application. Upon verifying the identity of the user via the MFA application, users are able to securely connect to their VPN.

Fusion utilizes two underlying vendor solutions for the VPN Service as follows:

(a) Meraki-based solutions (used with Fusion's SD-WAN Pro Service) requiring use of the Customer's Native VPN Client (Windows OS Native VPN client and MacOS Native VPN client). Customer is solely responsible for native VPN client software. For Meraki-based solutions, Customer must identify a Guest Administrator to self-administer creation and deletion of VPN user accounts.

(b) Fortinet-based solutions (used with Fusion's SD-WAN Enterprise and/or Fusion's Unified Threat Management and Firewall Service) require the use of FortiClient VPN software. Customer is solely responsible for downloading the FortiClient VPN software. A free download of the FortiClient VPN is available at www.forticlient.com/downloads. For Fortinet-based solutions, Customer must contact Fusion Support for creation and deletion of VPN user accounts.

Fusion has two distinct pricing models for RAVPN Services as follows:

i) Named User Pricing Model enables only users specifically identified by the Customer to access the RAVPN Service. For named user pricing, RAVPN end-users are built out directly on the VPN aggregation device(s) with pricing associated with each individual named user. For Customers with Services deployed after July 1, 2022 the MFA feature is included in the fees associated with the

Named User pricing. Customers with Services deployed prior to July 1, 2022 are required to purchase of MFA feature in addition to the Named User Service. Fusion strongly recommends upgrading existing instances of VPN Services to use MFA in order to promote a strong security posture and mitigate risk.

ii) Maximum Authenticated User Pricing Model leverages either Customer-hosted or Fusion-hosted authentication (e.g., LDAP) to enable users to be authenticated for connecting to the RAVPN Service. The Maximum Authenticated User pricing model measures the maximum number of unique RAVPN users connecting at any point in time within a calendar month. Once the calendar month is completed, a calculation of total unique authenticated users is compiled to calculate any overage beyond the initial five (5) users included in the base offering. Rates for Maximum Authenticated User Pricing will be as set forth in the Fusion Fees and Surcharges Guide. MFA is a fee-based add-on to the Maximum Authenticated User model. All individual users are required to have MFA in order to connect to the VPN Service.

2. Customer Requirements. Customer is responsible for installing the VPN client to enable use of the Services and must provide Fusion with the usernames and passwords for its users for configuration of the VPN locally to the VPN aggregation device. Alternatively, eligible Customers may utilize existing authentication fabric (i.e. LDAP, Radius, etc.) for the Services. The Services do not include local scanning of computing devices for presence of malicious content. It is the responsibility of the Customer to ensure all user workstations are protected via locally installed security software (e.g., AntiVirus and/or Anti-Malware clients.)

3. Use of the Services. Customer agrees not to use the Services for malicious purposes, including uses that might involve viruses, worms or Trojans. Only Customer and its end users are authorized to access the Services. Customer is responsible for any unauthorized use of the Services.

4. Incompatibility with Other Services. In the event that Customer uses the Services (i) in combination with any equipment or service not provided by Fusion, (ii) with any other software and/or service provide by Customer or any source other than Fusion, which may be installed to integrate with the Services, including but not limited to Internet access, voice services (local, long distance, toll) or any IP solutions (VoIP telephone system, etc.), (iii) with any other service platform that is not connected to a Fusion provided access facility, or (iv) any Fusion provided equipment used in combination with any broadband Internet connection not provided by Fusion, Customer agrees as follows:

(a) Fusion will not be liable or responsible for any integration, installation, testing, troubleshooting, repair, support or maintenance regarding any Customer provided equipment used in connection with the Services; and

(c) Fusion will not be liable or responsible for quality of Service issues or Service degradation resulting from Customer's use of third-party applications.

In addition, the Services may not be compatible with existing network security configurations and may require changes by Customer to enable the Services to function properly.

5. Activation and Installation. The Services will be deemed installed when the Services successfully communicate with the Customer's existing VPN or upon verification of activation of the Services by Fusion's technician. No on-site installation is required for the Services. Fusion provides reactive remote support for service activation as needed.

6. Maintenance, Changes and Firmware Upgrades. Fusion may, in its sole discretion without incurring any liability, change the features or discontinue the sale of VPN Services. Fusion will use commercially reasonable efforts to ensure that any such changes do not have a material adverse effect on the functionality or performance of the Services. Fusion will also use reasonable methods to notify the Customer in advance of any material changes to the Services.

7. Technical and Administrative Support. Support for the Services is provided on a Tier 2 level,

with Customer's support organization providing Tier 1 support directly to its end users. Customer must open all trouble tickets on behalf of its end users; however, if necessary, Fusion will communicate directly with the end user to resolve issues. Fusion support is available 24x7x365 to help Customer resolve Service related issues, and during regular business hours to address administrative issues.

8. Term. Each Service is subject to a minimum Service Term starting from the date that the Service is installed. The Service Term is set forth in the applicable Service Order. The applicable monthly recurring charges ("MRC") shown in the Service Order shall apply to each Service installed for Customer. The Initial Service Term and each Renewal Service Term for the Services shall automatically renew for additional Terms of one (1) year, unless Customer provides written notice to Fusion at least sixty (60) days prior to the end of the then-current Term. If a Service is disconnected or terminated prior to the end of the then current Term, by Fusion due to a breach of the Agreement, or by Customer for any reason, then Customer agrees to pay an Early Termination Fee equal to the monthly recurring charge for the Services multiplied by the number of months remaining in the then-current Term.

9. Export Control. The Services may be subject to certain export laws and regulations. Customer will not and will not permit any end user to access or use the Services in a U.S. embargoed country (including Cuba, Iran, North Korea, Sudan or Syria) or in violation of any U.S. export law or regulation and will ensure that the Services and equipment will not be exported, directly or indirectly, in violation of any export laws or regulations, or used for any purpose prohibited by such export laws or regulations.

10. Additional Terms and Conditions for VPN Services. Customer's use of the VPN Services which are made available for resale by Fusion from Fortinet and Meraki and are subject to the terms and conditions of the then-current End User License Agreements as identified below:

(a) For Fortinet-based solutions, these are located at https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf.

(b) For Meraki-based solutions, these are located at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html and amended by the Supplemental End User License Agreement located at: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/cisco-meraki.pdf.

The terms of both the Fortinet and Meraki End User License Agreements which include, but are not limited to, provisions regarding limitations of liability, disclaimers of warranty, reservation of intellectual property rights, and restrictions on the use and resale of the respective services, are incorporated herein by reference. Fusion is required to ensure that Customer's use of the Services abides by the underlying technology partners' (Fortinet and Meraki) terms at all times and Fusion is required to report unauthorized use of the Services, or, if necessary, suspend Customer's use of the Services for violations of the underlying End User License Agreement.

11. Service Level Agreement. Remote Access VPN and MFA Service is provided on a best-effort basis with no corresponding Service Level Agreements.