Fusion Managed Security Services Addendum

The additional terms and conditions set forth in this Fusion Managed Security Services Addendum (the "**Managed Security Services Addendum**") apply to Fusion's provision of Anti-Virus, Whitelist/Blacklist, Web Filtering, Managed Firewall, and Intrusion Detection/Prevention Services (the "**Services**" or "**Managed Security 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 Managed Security Services 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 Managed Security Services 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 Managed Security Services 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 provides Managed Security Services via geo-diverse, redundant secure gateways located at its datacenters in North America as well as via CPE located at Customer's sites (each a "Security Platform"). A description of each Security Platform and a list of Service options are set forth below:

(a) **Cloud Managed Security Services**. Fusion provides Managed Security Services via the routing of traffic through secure gateways to enable security policies and signatures to be applied to protect Customer traffic against threats, with the option for routing all traffic or only public (Internet) traffic via a split-tunnel design or routing all traffic through its gateways. Managed Security Services enforce global policies across all locations without any variability at the Customer site level. As a standard, Managed Security Services require Customer to purchase one or more of the following Fusion Services: Managed IPSec VPN, SD-WAN and/or MPLS.

(b) **CPE-Based Managed Security Services**. Fusion provides Managed Security Services via CPE located at Customer's remote locations. The CPE-based Managed Security Services scans all traffic using security software contained within the CPE device. CPE-based Managed Security Services provide granular security policies specific to individual locations. CPE-based Managed Security Services is a stand-alone offering and does not require Customer to purchase any other services from Fusion.

(c) **Managed Security Services Options**:

i. Anti-Virus/Malware Service: Fusion's Anti-Virus/Malware Service provides Customer locations with virus, malware, greyware and spyware protection to and from the Internet. The Anti-Virus Service operates bi-directionally and will detect and quarantine viruses, malware, greyware and spyware traversing the CPE at the Customer location. Anti-Virus Service protocols include POP3, SMTP, IMAP, HTTP, HTTPS, FTP and IM. Anti-virus compressed file filtering supports the following protocols: ZIP, MIME/UU, and CAB. The Anti-Virus Service utilizes signature and rule based blocking.

ii. Whitelist/Blacklist Service: Fusion's Whitelist/Blacklist Service provides Customer with the ability to control Internet site access from its locations. The "explicitly allow" (Whitelist) or "explicitly deny" (Blacklist) functions can be configured in a granular fashion at the site level. The Whitelist/Blacklist Service supports HTTP and HTTPS protocols. Whitelist/Blacklist Service URL's can be specified at both server and domain level.

The Whitelist/Blacklist Service is configured at the site level and provides customizable policies for each Customer location.

iii. Web Filtering Service: Fusion's Web Filtering Service provides Customer with the ability to control Internet site access from its locations by category of web content. Web Filtering supports HTTP and HTTPS protocols. Web Filtering provides reports detailing the use of Internet browsing by IP address, allowing for productivity monitoring as well as acceptable use enforcement. Web Filtering is configured at the site level with customizable policies for each Customer location.

iv. Advanced Firewall Service: Fusion's Advanced Firewall Service provides the ability to define specific "allow" and "deny" rules to control traffic between Fusion's private network and the Internet. The Advanced Firewall Service provides stateful multi-layered inspection access control and enforcement that tracks the operating state and characteristics of network connections traversing it. Advanced Firewall Services operate in a NAT/Route mode, providing additional anti-spoofing capabilities.

v. Intrusion Detection/Prevention Service: Fusion's Intrusion Detection/Prevention Service ("IPS") provides Customer with signature and anomaly attack prevention to and from the Internet. This Service includes features that prevent DoS/DDoS attacks. IPS supports a minimum of 80 protocols for common application attacks and a continuously growing database of attack anomalies and attack signatures.

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

3. Ancillary Services. All Managed Security Services are fully managed by Fusion and include the following support services: (1) on-going reactive support; (2) 24x7x365 customer support; (3) firmware and subscription updates (so long as Customer's devices have active licenses to enable updates); and (4) reporting.

4. Configuration Updates. Each Service includes a set number of standard configuration changes per month which vary by security feature. Examples of these changes include adding or removing Firewall rules, turning on/off Anti-Virus/Malware, IPS policy changes, Web Filtering Category changes and Whitelist/Blacklist entries. Changes that involve redesign of the Service or the addition/removal of Service features are not considered as standard configuration changes. Any changes that involve design work or that exceed the allotted change limit will be billed at the rates set forth in Fusion Fees and Surcharges Guide. All changes must be submitted through the change request process by documented authorized personnel of Customer. A list of standard configuration changes per Service is as follows:

i. Whitelist/Blacklist Service includes one (1) monthly policy change (up to 20 URLs) per site per month. Additional packages of 20 URL changes can be purchased by Customer as needed. Unlimited self-administered policy changes via the Fusion Connect Customer Portal are included in the Service.
ii. Web Filtering Service includes one (1) monthly policy change (up to 20 Web Filtering categories via single change) per site per month. Additional packages of 20 Web Filtering Category changes can be purchased by Customer as needed. Unlimited self-administered policy changes via the Fusion Connect Customer Portal are included in the Service.
iii. Advanced Firewall Service includes two (2) Customer initiated policy changes per month per site (subject to technical limitation of the Firewall).
iv. IPS includes two (2) Customer initiated policy changes per month per location.

5. Incompatibility with Other Services. In the event that Customer uses the Services (i) in

combination with any service not provided by Fusion, (ii) with any other software and/or service provided 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, or 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 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

(b) Fusion will not be liable or responsible for quality of Service issues or Service degradation resulting from Customer's equipment and the Service Level Agreement set forth herein shall not apply.

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

6. Activation and Installation. Managed Security Services require on-site installation by a Fusion technician. Customer personnel must be at each Customer location to facilitate that installation. Fusion's on-site installation includes the installation of a Fusion managed router and confirmation that the Managed Security Service(s) is/are functioning according to applicable specifications. Any inside wiring or additional services required at a Customer location are not covered by Fusion's standard installation fee and will be billed at the rates set forth in Fusion's Fees and Surcharges Guide. Once the Fusion technician determines that the Managed Security Service meets the predefined requirements, the Service will be considered installed and billing will commence. Customer shall pay the setup fee and professional on-site installation fees set forth in the applicable Service Order.

7. Virtual Infrastructure. Fusion provides options to support the SD-WAN Services utilizing customer-provided virtual infrastructure ("**Virtual Infrastructure**"). In such instances, Customer is responsible for providing the appropriately sized virtual environment based on requirements provided by Fusion. Customer is also responsible for all aspects of the Virtual Infrastructure, including but not limited to vCPU; memory; bandwidth; and storage. Fusion will provide Customer with a software image for installation on the Customer's virtual instance. Fusion provides ongoing management and support of the Service provided via the Virtual Infrastructure. However, installation and maintenance of the Virtual Infrastructure are solely Customer's responsibility. Upon successful software installation, Fusion will configure the Service to meet the technical requirements outlined in the mutual agreed upon Technical Architecture Document associated with the applicable Service Order. If Fusion identifies issues related to the Customer-provided Virtual Infrastructure, Customer is solely responsible for troubleshooting the virtual environment.

8. 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 (currently 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.

9. Purchased CPE Warranty. CPE purchased from Fusion includes a warranty which is the lesser of (i) one-year or (ii) the manufacturer's warranty against defects in parts or workmanship. This warranty does not cover failure due to abuse, fire, flood, lightning, acts of God, or war. During the warranty period, Fusion, at its sole discretion, will reasonably determine whether the purchased CPE is defective and requires replacement. If Fusion determines that replacement CPE is required, Fusion will ship the replacement CPE as soon as commercially reasonable at Customer's expense.

At Fusion's sole discretion, replacement CPE may include new or refurbished CPE. Fusion will provide Customer with a Return Merchandise Authorization ("RMA") number and return address (included with the replacement CPE), and Customer shall return the defective CPE, with the RMA number clearly visible on the outside of the packaging, to the address specified by Fusion. If the defective CPE is not received within fifteen (15) business days, Customer will be charged the then current list price for the replacement CPE.

10. Service Level Agreement. Except as otherwise provided herein, the Service Level Agreement appearing in **Appendix A** hereto shall apply to the Services.

Appendix A

Fusion Managed Security Services – Service Level Agreements

1. **Overview.** This Service Level Agreement, or SLA, sets forth the service level commitments for the Services as provided via the Fusion Cloud Managed Security platform or the Fusion CPE-Based Security platform. Subject to the terms of this SLA, in the event that a Service fails to meet the Minimum Service Metric, Customer will be eligible to receive Service Credits as set forth herein.

2. **Category Definition.** The following information defines the SLA categories and their respective measurements for the Services:

   (a) **Availability** – the Availability measurement for the Services is defined as the percentage of time over a calendar month that the Services are operational.

   (b) **Mean Time to Respond** – the Mean Time to Respond measurement for the Services is defined as the amount of time between when an issue is reported by Customer and/or detected by Fusion and a trouble ticket is opened, until the time a Fusion technician first begins troubleshooting the issue.

   (c) **Mean Time to Repair** – The Mean Time to Repair measurement is defined as the amount of time between when a Service issue is reported by the Customer and a trouble ticket is opened, to the date and time the trouble issue is resolved and the trouble ticket is closed.

   (d) **CPE Mean Time to Replace** – The CPE Mean Time to Replace measurement for the Services is defined as the amount of time between when an issue is reported by the Customer and a trouble ticket is opened, until the time the Service issue is resolved and the trouble ticket is closed.

   (e) **Security Policy Mean Time to Change** – The Security Policy Mean Time to Change measurement for the Service is defined as the average amount of time in a calendar month it takes Fusion to implement a security policy change on 1) the Fusion Cloud Managed Security platform; or 2) a site level policy change on the Fusion CPE-based Managed Security platform. The time measurement begins when Customer opens a trouble ticket requesting a Security Policy change and ends when the change is implemented and reported via the trouble ticket. The Minimum Service Metric related to a specific policy change request is based on the severity of the security threat, as reasonably determined by Fusion, as outlined below:

      i) **High Severity:** When a critical error causes the Services at a Customer location to fail. During a High Severity security incident, normal day-to-day business is not possible (e.g. system failure, or an inaccessible or inoperable production system). High Severity threat levels also include suspected malicious network activity that require urgent action by Fusion's Security Operations Center. Common changes in response to High Severity threats include blocking IP address(s) and/or modifying IDS/IPS signatures to prevent propagation of attacks.

      ii) **Medium Severity:** When an isolated error impacts the functions of the Services at Customer's location but there is no important impact on the day-to-day business (e.g. the addition of new devices requiring firewall rule updates to enable new devices to function). Firewall policy changes resulting from the modification of network elements such as adding

additional subnets to a solution require vetting by Fusion's engineering team prior to implementing changes to ensure continued Service functionality.

iii) **Low Severity:** When a customer requests a change to allow or deny communication with specific sources, destinations, ports, as well as Web Filtering and White List/Black List changes. During a Low Severity incident, there are no problems with the Services at a Customer location, and there is no immediate impact on the production environment. Common changes to a Low Severity threat include modifications to content filtering profiles by Fusion's Security Operations Center in lieu of having Customer modified changes implemented through the Customer portal.

3. **Service Credits.** Subject to the Additional Terms and Exclusions set forth herein, in the event that a Service fails to meet the Minimum Service Metrics, Customer will be eligible to receive the amount of Service Credits as set forth in the tables below (the "**Service Credit**") which Service Credits shall be Customer's sole and exclusive remedy arising from such Service failure.

Cloud Managed Security Services*

Category	Minimum Service Metric	Service Credit
Availability	100%	No Credit
	99.5%-99.9%	5% of the monthly recurring charge ("MRC") for the affected Service
	<99.5%	10% of the MRC for the affected Service
Mean Time to Respond	<4 Business Hour**	No Credit
	>4 Business Hour <8 Business Hours	5% of the MRC for the affected Service
	>8 Business Hours	10% of the MRC for the affected Service
Mean Time to Repair	<4 Business Hours	No Credit
	>4 Business Hours ≤8 Business Hours	5% of the MRC for the affected Service
	>8 Business Hours	10% of the MRC for the affected Service

*The SLAs associated with the Cloud Managed Security Services apply to the Cloud Managed Security gateways and Cloud Management and Reporting infrastructure only.
**For the purposes of this SLA, Business Hours are Monday – Friday 8:00 a.m. to 5:00 p.m. local time.

Managed Security CPE Services

Category	Minimum Service Metric	Service Credit
Mean Time to Respond	<4 Business Hours*	No Credit
	>4 Business Hours <8 Business Hours	5% of the MRC for the affected Service

	>8 Business Hours	10% of the MRC for the affected Service
Mean Time to Replace	Next Business Day**	No Credit
	2 Business Days	5% of the MRC for the affected Service
	>2 Business Days	10% of the MRC for the affected Service

* For the purposes of this SLA, Business Hours are Monday – Friday 8:00 a.m. to 5:00 p.m. local time.
**Replacement equipment provided by Fusion will be shipped for next business day delivery for Customer self-installation so long as (i) the trouble is isolated to the Fusion provided and managed equipment, and (ii) the root cause of the failure is identified by Fusion by 2 p.m. local time Monday – Friday, excluding federal holidays.

Security Policy Mean Time to Change

Threat Level	**Service Metric**	**Service Credit**
High Severity	<8 Business Hours*	No Credit
	>8 Business Hours <16 Business Hours	5% of the MRC for the affected Service
	> 16 Business Hours	10% of the MRC for the affected Service
Medium Severity	<16 Business Hours	No Credit
	>16 Business Hours <24 Business Hours	5% of the MRC for the affected Service
	>24 Business Hours	10% of the MRC for the affected Service
Low Severity	<24 Business Hours	No Credit
	>24 Business Hours <32 Business Hours	5% of the MRC for the affected Service
	>32 Business Hours	10% of the MRC for the affected Service

* For the purposes of this SLA, Business Hours are Monday – Friday 8:00 a.m. to 5:00 p.m. local time.

4. **Additional Terms.** In order to receive Service Credits, Customer must email Fusion at **customersupport@fusionconnect.com** and provide the following information: Customer name, account number, location affected, Service affected, trouble ticket number (if applicable) and a detailed description of the credit request. Upon validation of the request, a Service Credit will be applied to Customer's account. In no event will the Service Credits issued in any given month exceed the MRC associated with the affected Service(s). If a single Service issue arises out of two or more SLA categories, such as Availability and Mean Time to Repair, Customer will only be entitled to a Service Credit for one of the Service Metrics.

5. **Exclusions**. Fusion shall not be liable for any Service Credits for any delay or failure to meet the Minimum Service Metrics that is attributable to any of the following exclusions (the "**Exclusions**"):

   (a) Force Majeure events;

(b) Service disruption and additional time to repair resulting from connectivity issues;

(c) Service disruption and additional time to repair for Services utilizing Internet connectivity or local loop facilities provided by third parties;

(d) Customer's delay or failure to provide sufficient IP information;

(e) breach of Customer's responsibilities under the Agreement;

(f) lack of Customer site readiness for installation, maintenance or repair, as may be reasonably determined at Fusion' sole discretion;

(g) Customer's breach of requirements specified in the Service installation letter from Fusion;

(h) delays cause by the LEC (local exchange carrier) or other third party carriers;

(i) Service issues due to failure of Customer-provided equipment;

(j) Service issues due to configuration changes made by Customer to Fusion or Customer-provided equipment;

(k) Service issues arising during a scheduled maintenance window;

(l) Service issues arising from Fusion's inability to access required facilities or equipment;

(m) "No Trouble Found" trouble tickets; or

(n) trouble tickets that remain open due to delays caused by slow responses from Customer for requests for feedback.