

Fusion Connect, Inc. Fusion Managed Switch Services Addendum

The additional terms and conditions set forth in this Fusion Managed Switch Service Addendum (the “**Managed Switch Services Addendum**”) apply to Fusion’s provision of Fusion Managed Switch services (the “**Services**” or “**Managed Switch 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 Switch Services Addendum, together with the MSA or Basic Terms and Conditions, as applicable, is herein collectively referred to as the Agreement. For purposes of this Fusion Managed Switch Services Addendum, Fusion means the subsidiary of Fusion Connect, Inc., a Delaware corporation, that provides the Service in the applicable state to Customer. Capitalized terms used in this Fusion Managed Switch 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 Switch Services to offer port density, switching and Power over Ethernet (PoE) Services to connect Customer Local Area Networks (LAN) devices to their Wide Area Network (WAN) high-speed wireless connectivity to Switch enabled devices such as laptops, tablets, smartphones and other Switch enabled devices. Fusion offers a variety of Switch Service plans to meet a wide range of Customer needs, ranging from Private Wireless LANs to Public Guest Access. Switch Services can leverage the same circuit used for the site’s VPN or Internet connectivity or can be provided on a circuit dedicated to the Switch Service (circuits priced separately). Managed Switch Services leverage both on-board Switch capabilities of Customer Premises Equipment (CPE) devices, as well as supporting multiple Access Points to provide comprehensive coverage within Customer venues. Managed Switch Services offer solutions that support local controller capabilities or cloud-based controller capabilities for management of Switch networks. Service descriptions for supported Switch offerings are detailed below.

(a) **Managed Switch HotSpot:** The Fusion HotSpot enables Customer venues to utilize a public Switch for public End-Users and devices accessing the internet. HotSpot access is segregated from private LAN traffic, such as Point of Sale traffic, via creation of separate Virtual LANs (VLAN) to help Customer adhere to PCI DSS requirements. Fusion provides Customer

with open authentication upon connecting to SSID and opening a web browser. After connecting to the HotSpot network and launching the web browser, Customers are presented with terms and conditions that are posted on the HotSpot “Welcome” page. Upon accepting the terms and conditions, End-Users will have access to the Internet. Upon acceptance of terms and conditions, Customer is redirected to the URL of Customer’s choosing to enable more Customer brand visibility.

(b) **Managed Switch WLAN:** The Fusion Switch Local Area Network (WLAN) Service enables Customer venues to utilize Switch for back-office use by authorized personnel and hand-held devices for accessing resources on the venue LAN. WLAN access is segregated from private LAN traffic, such as Point of Sale traffic, via creation of separate Virtual LANs (VLAN) to help Customer adhere to PCI DSS requirements. Fusion configures a static Switch Protected Access II (WPA2) key that is used to authenticate Customers. WPA2 key naming convention is dictated by Fusion. One key rotation per quarter is included in the Services and must be requested by Customer. If Customer requires additional WPA2 key changes, incremental professional services fees as set forth in the Fusion Basic Fees and Surcharges Guide or in the applicable Service Order or Statement of Work shall be billed to Customer for all requested changes. In addition to WPA2, Fusion configures Switch devices to communicate with optional Customer-provided radius servers (WPA2 Enterprise), enabling access to be denied when

authentication credentials fail to match records housed in Customer radius servers. Customer is responsible for providing Fusion with all necessary authentication information required to integrate Fusion services with Customer authentication fabric. Fusion's support scope of responsibility includes verifying connectivity to APs and Customer-provided radius servers. Customer authentication fabric account issues are the sole responsibility of the Customer. End user support is not included as part of Fusion Switch Services but can be made available for an additional Service fees that varies by Customer use case.

(c) **Fusion Managed Switch Features.**

- i. **Switch Networks:** Fusion configures wireless access points with service set identifiers (SSIDs), often referred to as a network name, which uniquely names a WLAN. This name allows wireless enabled devices to connect to the desired network when multiple independent networks operate in the same physical area. Customer may choose for SSIDs to be broadcast publicly or require wireless devices to be manually configured to detect non-broadcast SSIDs. Selection of broadcast or non-broadcast will be applied across all Customer WLAN locations, as Fusion does not support both broadcast and non-broadcast SSIDs within a single Customer for WLAN Service. Multiple SSIDs are supported by the Service to segment Switch devices access capabilities to specific WLANs.
- ii. **Rogue Wireless Detection/Wireless Intrusion Detection:** is included in the WLAN Service to help Customer meet PCI DSS requirements. Rogue Wireless Detection entails monitoring the radio spectrum of Switch APs for the presence of unauthorized APs. Upon detecting the presence of an unauthorized AP, an alert is triggered and sent to the Customer for analysis and action.
- iii. **Monitoring and Support:** Fusion proactively monitors the availability and health of Switch Access Points and provides alerts when outages and/or health issues are determined. Upon trouble ticket creation by Customer, Fusion network operations works with a Customer contact

to troubleshoot Switch outages and/or health issues to determine cause and restore Service. If a Switch access point is determined to be faulty, Fusion will ship a preconfigured replacement device via overnight shipping to remedy the outage. End user support is not included as part of Fusion Switch Services but can be made available for additional service fees that vary by Customer use case. If Customer requires troubleshooting of wireless devices attempting to access the WLAN, Fusion will, at the Customer's request, dispatch an on-site technician to troubleshoot the Customer's ability to connect to the Switch network. Standard time and materials rates, as set forth in the Fusion Fees and Surcharges Guide or as set forth in the applicable Service Order or Statement of Work will apply for all dispatches.

- iv. **Bandwidth Shaping:** Fusion provides the ability to rate limit throughput by SSID to prevent Switch networks from consuming bandwidth that is needed for non-Switch related services. Quarterly updates to bandwidth shaping policies such as limiting the amount of bandwidth by SSID are included in the Service. Incremental fees may apply for additional updates.

2. Service Elements. All Fusion Managed Switch Services are fully managed by Fusion networking professionals. The Managed Switch Services includes:

- i. Three (3) global changes per quarter required by Customer, subject to the technical limitation of the Switch. Examples include Re-configuration of Switch, such as additions or changes to SSIDs, bandwidth shaping adjustments and rotation of WPA2 keys;
- ii. On-going reactive support for the Switch;
- iii. All firmware and subscription updates provided Customer devices have active licenses to enable updates;
- iv. Managed Switch Services reporting such as bandwidth utilization, time of day reports, user reports. Reporting capabilities vary based on underlying architecture selected by Customer; and

- v. Optional Web Filtering: requires purchase of Fusion Managed Security services.

3. Bring Your Own Broadband Disclosure and Notice.

In the event that Customer shall use the Services (i) in combination with any service not provided by Fusion, (ii) with any other software and/or service provide by the Customer or any source other than Fusion, which may be installed to integrate with the Services, including but not limited to broadband access, voice services (local, long distance, toll) or any IP solutions (Internet Access, 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

(b) Customer understand that it may experience quality of Service issues or Service degradation resulting from Customer's equipment and that the Service Level Agreement set forth herein shall not apply.

4. Incompatibility With Other Services. The Services may not be compatible with existing network security configurations and may require changes by the Customer to enable the Service to function properly.

5. Activation and Installation. Managed Switch requires Fusion Professional On-Site Installation. Customer personnel will need to be at the Customer premises to facilitate the professional installation technician. A Professional On-Site Installation includes installation of the Fusion Managed Router and confirmation of Managed Switch functionality. Any wiring or additional services required at that site are not included in the Professional On-Site Installation Fee, and separate fees will apply. Once the Fusion technician determines that the Managed Switch 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 Fusion

Fees and Surcharges Guide or the Fusion Service Order or Statement of Work.

6. Technical and Administrative Support.

Support services for the Services are provided on a Tier 2 level, with the 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.

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

8. CPE Warranty. (a) Purchased CPE. 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 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.

(b) Rented CPE. During the Service Term, Fusion will replace defective rental CPE with an equivalent

device for no additional charge. At qualified locations, Fusion will advance-replace defective rental CPE that will be shipped out the same business day as long as a request is made early enough in the day. Customer must return defective rental CPE to Fusion within fifteen (15) days from the date of receipt of the replacement CPE in order to avoid being charged late penalties. Fusion reserves the right to bill for any CPE not shipped within such time period. Upon Service termination, or CPE replacement, Customer must return the rental CPE using Fusion supplied return labels.

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. Service Level Agreement. The Service is provided on a best effort basis and no Service Level Agreement applies.