Fusion Managed Wi-Fi Service Addendum

The additional terms and conditions set forth in this Managed Wi-Fi Service Addendum (the "**Managed Wi-Fi Service Addendum**") apply to Fusion's provision of Managed Wi-Fi services (the "**Services**" or "**Managed Wi-Fi 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 Wi-Fi 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 Managed Wi-Fi Service 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 Managed Wi-Fi 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 provides Managed Wi-Fi (802.11) Services to offer high-speed wireless connectivity to Wi-Fi enabled devices such as laptops, tablets, smartphones and other Wi-Fi enabled devices. Fusion offers a variety of Wi-Fi Service plans to meet a wide range of customer needs, ranging from private wireless Local Area Networks ("LANs") to public guest networks. Managed Wi-Fi Services can leverage the same circuit used for a location's virtual private network ("VPN") or Internet connectivity, or can be provided on a circuit dedicated to the Managed Wi-Fi Service (circuits priced separately). Managed Wi-Fi Services leverage both on-board Wi-Fi capabilities of customer premises equipment ("CPE") devices, as well as supporting multiple access points to provide comprehensive coverage within Customer venues. Managed Wi-Fi Service offers solutions that support local controller capabilities or cloud-based controller capabilities for management of Wi-Fi networks. Fusion's Managed Wi-Fi Service offerings and a list of Service features are detailed below:

(a) **Managed Wi-Fi HotSpot**: Fusion HotSpot enables Customer venues to utilize public Wi-Fi for public end-users and devices accessing the Internet. HotSpot access is segregated from private LAN traffic, such as point of sale traffic, via the creation of a separate Virtual LANs ("VLAN") to adhere to industry specific security 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, Customer is 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 Wi-Fi WLAN**: Fusion Wi-Fi LAN ("WLAN") Service enables Customer venues to utilize Wi-Fi for back-office use by authorized personnel and hand-held devices for accessing resources on the LAN. WLAN access is segregated from private LAN traffic, such as point of sale traffic, via creation of a separate VLAN to adhere to PCI DSS requirements. Fusion configures a static Wi-Fi 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 with the Service and must be requested by Customer in writing. If Customer requires additional WPA2 key changes, incremental services fees specified in Fusion's Fees and Surcharges Guide apply. In addition to WPA2, Fusion configures Wi-Fi 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 the Services with Customer authentication fabric. Fusion's support includes verifying connectivity to access points and Customer-provided radius servers. Customer authentication fabric account issues are the sole responsibility of Customer. End-user support is not included with the Managed Wi-Fi Services, but is offered by Fusion for an additional fee that varies based on the Customer's requirements.

(c) **Fusion Managed Wi-Fi Service Features**.

i. **Wi-Fi 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 settings will be applied across all Customer WLAN locations, as Fusion does not support both broadcast and non-broadcast SSIDs for a single customer for WLAN Service. Multiple SSIDs are supported by the Service to segment Wi-Fi devices access capabilities to specific WLANs.

ii. **Rogue Wireless Detection/Wireless Intrusion Detection**: is included in the WLAN Service to meet PCI DSS requirements. Rogue wireless detection entails monitoring the radio spectrum of Wi-Fi access points for the presence of unauthorized access points. Upon detecting the presence of an unauthorized access point, an alert is triggered and sent to Customer for analysis and action.

iii. **Monitoring and Support**: Fusion proactively monitors the availability and health of Wi-Fi access points and provides alerts when outages and/or issues are detected. Upon trouble ticket creation by Customer, Fusion will work with a Customer contact to troubleshoot Wi-Fi outages and/or other Service issues to determine cause and restore the Service. If a Wi-Fi 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 this Service, but is available for an additional fee that varies based on the Customer's requirements. 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 issue. Standard time and materials rates, as set forth in Fusion's Fees and Surcharges Guide shall apply to any such dispatch.

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

2. Use of the Service. 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 Service. Customer is responsible for any unauthorized use of the Service.

3. Support Services. Managed Wi-Fi Services are fully managed by Fusion. Support for Managed Wi-Fi Services includes:

i. three (3) global changes per quarter, as requested by Customer, subject to technical limitations of the Wi-Fi. Examples include re-configuration of Wi-Fi, such as additions or changes to SSIDs, bandwidth shaping adjustments and rotation of WPA2 keys;
ii. on-going reactive support for the Wi-Fi;

iii. reporting (reporting capabilities vary based on underlying architecture selected by Customer); and
iv. optional Web Filtering (requires purchase of Managed Security Services from Fusion).

Support for the Services is 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.

4. 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 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

(b) Fusion will not be liable or responsible for quality of Service issues or Service degradation resulting from Customer's equipment.

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

5. Activation and Installation. The Services require that a Fusion technician provide on-site installation. Customer personnel will need to be at the Customer's premise to facilitate the installation. Wiring or additional installation services not set forth in the Service Order may be purchased from Fusion for an additional fee. Once the Fusion technician determines that the Service meets the predefined requirements, the Service will be considered installed and billing will commence. Customer shall pay the setup fee and installation fees as set forth in Fusion Fees and Surcharges Guide.

6. 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.

7. Service Level Agreement. The Services are provided on a best efforts basis and no Service Level Agreement applies.