Managed Wi-Fi Product ("Managed Wi-Fi Product")

Managed Wi-Fi Product: If Customer elects to receive Managed Wi-Fi Product, Provider will provide a managed Wi-Fi solution with
wireless access points ("WAPs") deployed at the designated Product Location to enable designated users of the Customer's choice to wirelessly access the Internet as more specifically set forth in a Product Order. Managed Wi-Fi Product, or certain features, may not be available in all coverage areas and may change from time to time, in Provider's sole discretion.

Customer's use of the Managed Wi-Fi Product is subject to the following additional terms and conditions:

1. Wi-Fi Equipment. Provider will, and Customer grants Provider permission to, attach, install, maintain, operate and upgrade
Wi-Fi-related equipment, cables and devices on and within Customer's premises at the Product Location(s) identified in the
applicable Product Order.

2. Internet Access. Provider offers Managed Wi-Fi Product in association with Providers Internet Access Product. Customer requires advanced approval where Provider will not be the primary Internet access provider if Customer purchases an Internet access product from another source. Provider does not offer Managed Wi-Fi Product as a stand-alone product.

3. Connectivity to Local Area Networks. Configuration of the Managed Wi-Fi Product will be as agreed in the Wi-Fi questionnaire
completed by the Parties. Managed Wi-Fi Product may provide a separate SSID for employee Internet access if specified on the
Wi-Fi questionnaire. A second WLAN will be created on the wireless network with its own VLAN assigned. The aggregation
switch will be configured to hand off an Ethernet Product port to Customer. In this scenario, network functions (DHCP and NAT,
for example) may be handled by Customer's LAN. Customer will need to train and engage Customer's staff for all ongoing support
issues. The Managed Wi-Fi Product does not include support for connectivity to any device (printers, laptops, computers, routers,
etc.).

4. Security Limitations. This Product does not include features such as: locked down access for the WAPs, single username and
logins for each WAP, logging, content filtering or intrusion detection systems. All Provider-authorized personnel and vendors will
have access to log into the WAP devices on site. Provider is not responsible for security breaches that occur related to any
SSIDs. Provider does not monitor the traffic on any SSIDs and Customer has the sole responsibility and obligation to monitor
any traffic transmitted through use of the Managed Wi-Fi Product to protect Customer's and any user data. Provider can provide
a non-broadcast SSID if specified on the Wi-Fi questionnaire.