Managed Network Security Terms and Conditions Schedule

In addition to the Service Agreement between WIN and Customer, including any document incorporated by reference therein (collectively the "Agreement"), of which this Schedule is a part, Customer agrees that the following terms and conditions apply to the Managed Network Security ("MNS") Service provided to Customer by WIN. Unless otherwise defined herein, capitalized terms shall have the same meaning as defined in the Agreement.

1. MNS Service - Definitions. The following definitions apply to the MNS Service features outlined in Section 2(a) below:
   (a) Firewall – Stateful inspection with support for network address translation and demilitarized zone. Firewall policies are defined leveraging port, protocol, and IP address.
   (b) Virtual Private Network ("VPN") – Site to site Internet protocol security ("IPsec") VPN connectivity. Standard support for up to ten (10) IPsec connections per location firewall instance.
   (c) Remote Access – End user VPN (IPsec or secure sockets layer ("SSL")) connectivity. Online interface available for Customer to manage end user accounts (i.e. username and password). Integration with Customer-owned and managed Microsoft directory service ("Active Directory") for end user authentication is also supported.
   (d) Application Control – Identifies common layer 7 web applications for reporting and incorporation in firewall policy for enforcement.
   (e) Intrusion Prevention System ("IPS") – Focused signature library to protect against network attacks.
   (f) Web Content Filtering – Control of web access by end users via predefined and curated site categories and site level support for white or black list.
   (g) Threat Monitoring – Monitors security events detected by security information and event management ("SIEM") platform, which collects log data from MNS Firewalls and the pre-qualified customer owned devices ("Customer Device"). The categories of Customer Device that WIN supports are Active Directory, Windows Server, and Unix/Linux Server. The default log retention provided as part of the Threat Monitoring is twelve (12) months. Additional log retention can be purchased up to six (6) years and log retention periods are required to be twelve (12) month increments.
   (h) MPLS - Multiprotocol label switching network.
   (i) SD-WAN - Software defined wide area network.
   (j) CPE – Customer premises equipment.

2. Description of MNS Service.
   (a) **MNS Cloud and MNS CPE**
      i MNS Cloud is a WIN network-based multitenant MNS Service designed to provide MNS for WIN MPLS and SD-WAN. High availability ("HA") is included as part of the MNS Cloud Service.
      ii MNS CPE is a premises-based MNS Service that leverages a security appliance installed on the Customer's premises. The security appliance is procured, activated and managed remotely to deliver the MNS Service. HA is available as an option by implementing two (2) security appliances in active/passive configuration.
      iii MNS Cloud and MNS CPE Services are available in the following tiers:

Basic	Advanced	Premium
- Firewall - VPN - Remote Access - Report	- Firewall - VPN - Remote Access - Application Control - IPS - Web Content Filtering - Report	- Firewall - VPN - Remote Access - Application Control - IPS - Web Content Filtering - Threat Monitoring - Report

   (b) **Secure Remote Access ("SRA")** consists of Remote Access and VPN that provide secure access to WIN MPLS via the Internet.

3. MNS Service Activation. Once MNS Service is ordered, WIN will determine the appropriate MNS configuration based on a questionnaire form (the "Form") to be completed by the Customer. A WIN security operations center ("CSOC") engineer will then configure and activate the MNS Service via a scheduled activation call with the Customer.

4. MNS Service Support. CSOC provides 24x7 support to aid Customers in questions regarding the MNS Service, issue resolution, or change requests.

5. MNS Service Availability and Service Level Response Times.

(a) **MNS Service Availability.**

(i) MNS Cloud service availability will be maintained by connecting every Customer location to a primary and secondary security gateway. In the event the primary gateway becomes unavailable, Customer's traffic will be automatically rerouted to the secondary gateway.

(ii) MNS CPE's default setup is comprised of a single security appliance installed at the Customer's facility. If the service becomes unavailable due to a device failure, a replacement device will be shipped next business day to Customer's location and installed remotely when received. A HA option is available to prevent downtime due to device failure.

(b) **Service Level Responses.** The service level responses for change requests and incident response times are as follows:

(i) MNS Change Request.

a. Standard (Normal) Change Request – One (1) hour to begin addressing and within four (4) hours to complete.

b. Urgent (Emergency) Change Request – Thirty (30) minutes to begin addressing and within one (1) hour to complete.

(ii) Threat Monitoring Response for High Severity Incidents - Thirty (30) minutes to respond.

6. Customer's Obligations. Customer agrees to: (i) reasonably cooperate with WIN and provide the Form and additional information regarding Customer's systems and applications that are connected to MNS to help tuning of monitoring as requested; (ii) ensure information for all authorized points of contact remains current; (iii) notify WIN of any network security architecture changes (e.g. unscheduled bank-ups, anticipated increase in legitimate inbound web traffic) that could generate false alerts at least twenty-four (24) hours before such a change; and (iv) provide estimated log volume and/or average events per second of Customer Device when Threat Monitoring is required to monitor the Customer Device.

7. MNS Authorized Use. Excessive log volume of Threat Monitoring may have a severe impact on SIEM performance, so the log volume of Threat Monitoring per device should be no more than an average of ten (10) events per second ("Max EPS"). Customer must consult with the CSOC before maintaining a log volume over the Max EPS. WIN reserves the right to modify, terminate or otherwise amend the MNS Service if the Customer is in breach of this Section 7 and/or if Customer's excessive log volume damages the MNS Service.

8. Exclusions, Limitations and Restrictions

(a) Any equipment provided by WIN as part of the MNS Service remains the property of WIN and must be returned to WIN upon termination of MNS Service in accordance with the terms and conditions of the Agreement. The security appliance provided by WIN will be managed and maintained solely by WIN and Customer will not have direct terminal access to the security appliance when WIN is responsible for configuration management. Any cold spare equipment obtained through the MNS Service will not receive any firmware or configuration updates. Out-of-territory locations (i.e. geographic locations in which WIN does not have a field operations presence) will receive best-effort break/fix and issue resolution support, regardless of purchased MNS Service tier.

(b) Customers who provide Customer-owned equipment for the MNS Service will not receive support from WIN and are responsible for contacting the equipment manufacturer to place a service request when a hardware failure determination is made by WIN.