

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 allow or block 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.
 - (k) **VNF** - Virtual Network Function is a network function running on Virtual Machines within another device
 - (l) **Antivirus** – Detecting and blocking known viruses in network traffic traversing the MNS Firewall.
 - (m) **Incident - Series of events that trigger rules that are based on pre-defined condition or circumstance (e.g., attempted, or actual unauthorized access, use, disclosure, modification, or destruction the monitored Customers systems or information).**
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.

MNS Cloud is available in the following tiers:

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

- ii MNS CPE is a premise 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.

WINDSTREAM ENTERPRISE

MNS CPE is available in the following tiers:

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

- iii MNS VNF is the software version of the MNS Services running on a Virtual Machine within in SD-WAN edge device as Virtual Network Function (VNF).

MNS VNF Services are available in the following tiers:

Advanced	Premium
- Firewall	- Firewall
- Application Control	- Application Control
- IPS	- IPS
- Web Content Filtering	- Web Content Filtering
- Report	- Threat Monitoring
	- Report

- (b) **Secured Remote Access (“SRA”)** consists of Remote Access and VPN that provide secured access to WIN MPLS via the Internet.
3. **MNS Service Activation.** Once MNS Service is ordered, WIN will determine the 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**
 - (a) 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.
 - (b) 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.
 - (c) MNS VNF is software only Firewall running on a Virtual Machine within in SD-WAN edge device; purchased from and managed by WIN. The terms and conditions of which are covered in separate service schedule.
 6. **Service Level Objectives** shall be as set forth in **Exhibit 1**, attached hereto and incorporated herein by reference.
 7. **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 back-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.
 8. **MNS Authorized Use.** Excessive log volume of Threat Monitoring may have a severe impact on SIEM performance, so the log

WINDSTREAM ENTERPRISE

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.

9. 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.
- (c) Antivirus Protection is a discretionary MNS service capability that automatically scans, deletes and removes known computer software virus from network traffic that traverses the firewall with the following exclusions, limitations and restrictions:
 - i MNS Antivirus protection is an optional feature of MNS and requires pre-approval by WIN before it's enabled.
 - ii MNS Antivirus protection provides additional layer of protection from Malware (i.e. malicious software) including computer viruses.
 - iii MNS Antivirus protection uses third-party vendor threat information databases for timely updates on the latest malware, virus, and other cyber threat definitions.
 - iv MNS Antivirus protection does not provide protection from zero-day vulnerability where software or hardware vulnerability is known but no patch exists.
 - v MNS Antivirus Protection isn't a substitute for a reliable and up-to-date endpoint* security (i.e. Antivirus) software.
 - vi Antivirus technology is not error free, especially against unknown threats.
 - vii Customer should use endpoint security on all their devices* with Internet connectivity.
 - viii Customer should maintain their endpoint security software with the latest malware, virus and other cyber threat definitions.
 - ix WIN does not provide endpoint security software for devices as part of the MNS service
*Technology used by organization including but not limited to PCs, Laptops, Tablets, Smartphones and IoT (Internet of Things) devices

10. Authorization to Perform Testing. Customer grants WIN the authority to access Customer’s networks and computer systems solely for the purpose of providing the Managed CPE Firewall Service (“Firewall”). Customer agrees to notify WIN and obtain any third party service provider’s (“Host”) consent to provide the Firewall on Host’s computer systems, which includes acknowledgement of the risks and acceptance of the conditions set forth herein and to facilitate any necessary communications and exchanges of information between WIN and Host in connection with the Firewall. Customer agrees to indemnify, defend and hold WIN and its suppliers harmless from and against any and all claims, losses, liabilities and damages, including reasonable attorney's fees that arise out of Customer’s failure to comply with this Section and from any and all third party claims that arise out of the testing and evaluation of the security risks, exposures, and vulnerabilities of the IP Addresses that Customer provides. Customer acknowledges that the Firewall entails certain risks including the following possible negative impacts: (i) excessive log file disk space may be consumed due to the excessive number of log messages generated by the Firewall; (ii) performance and throughput of networks and associated routers and firewalls may be temporarily degraded; (iii) degradation of bandwidth; and (iv) Customer computer systems may hang or crash resulting in temporary system unavailability and/or loss of data. WIN is not providing Information Technology (“IT”) consulting services and the configuration of Customer’s firewall, or any other IT systems, is the sole responsibility of Customer. Prior to the installation or use of the Generic Configuration, Customer should seek the advice and support of its own IT professionals or contractors as needed. WIN may offer, upon written request from the Customer and at WIN’s sole option, a non-specific, pre-configured, generic configuration (“Generic Configuration”) to Customer to aid in setting up the Customer’s MNS Firewall. Such Generic Configuration is provided “as is” without warranties of any kind, and WIN expressly disclaims any and all liability arising from Customer’s use of a Generic Configuration provided by WIN to set up the MNS firewall. Further, Customer agrees to indemnify, defend and hold WIN and its suppliers harmless from and against any and all claims, losses, liabilities and damages, including reasonable attorney's fees, that may arise out of the testing and evaluation of the security risks, exposures, and vulnerabilities of the generic configuration that WIN provides for Customer’s use.

WINDSTREAM ENTERPRISE

11. Managed Network Security Cloud Firewall only: As operational responsibilities of MNS Cloud service, WIN agrees that it will maintain all applicable PCI-DSS compliance requirements to the extent WIN handles, has access to, or otherwise stores, processes, or transmits Customer's cardholder data or sensitive authentication data, or manages Customer's cardholder data environment on behalf of Customer.

WINDSTREAM ENTERPRISE

Exhibit 1 Service Level Objectives

The Service Levels listed below will apply to the Services as of the first day of the first whole calendar month after the initial installation of the Service deployment.

MNS Change Request

- (i) Standard (Normal) Change Request – One (1) hour to begin addressing and within four (4) hours to complete.
- (ii) Urgent (Emergency) Change Request – Thirty (30) minutes to begin addressing and within one (1) hour to complete.

MNS Cloud Service Availability Up-Time

Cloud Firewall shall be available in accordance with 99.99%, of each calendar month during the Term (excluding scheduled outages of which WIN has notified Customer at least 24 hours in advance (“Scheduled Outages”), or changes made by the Customer).

Threat Monitoring Response for High Severity Incidents

For the Premium Tier of MNS Service only, the Service will initiate contact automatically to notify Customer only for an Incident within thirty (30) minutes of the determination by WIN, in its sole discretion, that an Incident has occurred and classified as security high severity of nine or above.