The following IPsec VPN Service and MPLS IPsec Advanced Service Supplemental Terms and Conditions ("IPsec VPN T&Cs"), are in addition to and supplement the terms and conditions set forth in the Agreement for Service or Master Service Agreement and applicable Customer Experience Guide between Windstream and Customer dated concurrently herewith ("Agreement"). By its use of the Services, Customer agrees to amend and/or supplement the Agreement as set forth herein. For purposes of this IPsec VPN T&Cs, "WIN" means the Windstream affiliate billing Customer that is/are certified to provide the Service(s) in the applicable state(s). Except to the extent set forth herein, or in any other agreement mutually agreed to between the parties, all of the terms and conditions set forth in the Agreement shall remain in full force and effect. Capitalized terms used herein but not otherwise defined shall have the same meaning assigned to such terms in the Agreement. In the event of any conflict between the terms set forth in this IPsec VPN T&Cs, the Agreement, and any other agreement executed between the parties, the terms of this IPsec VPN T&Cs shall prevail.

1**. Service Overview**. The IPsec VPN Service or MPLS IPsec Advanced Service ("Service") is a managed network offering using WIN-provided and managed hardware and software located on the Customer's premises ("Customer Premises Equipment" or "CPE"), between Customer's internal local area network ("LAN") and internet access. The Service provides site to site encrypted tunnels over the internet and has options which analyzes inbound and outbound traffic and takes action based on selected attributes (e.g. source and destination address, port, protocol, user or group and time of day), the Customer's security policy requirements and industry best practices, including Network Address Translation ("NAT") and Port Address Translation ("PAT").

**2. Service Components**. The Service is available in three packages - IPsec VPN tunneling only, IPsec VPN with Firewall (FW) and Intrusion Prevention Service (IPS) and IPsec VPN with FW/IPS, Content Filtering and Application Control.

a. The base IPsec VPN Service and MPLS IPsec Advanced Service include the following:

- CPE capable of establishing encrypted tunnels over the Internet to a central aggregation device in the WIN core or optionally for the IPsec VPN Service to establish tunnels to WIN managed aggregation CPE located on the customer premises;
- Configuration and shipment of the CPE;
- Configuration backup and restoration;
- Device and tunnel monitoring and reporting, auto ticketing and 24x7 email and telephone support

b. IPsec VPN and MPLS IPsec Advanced offer an optional FW/IPS Feature which includes, in addition to the components offered above, the following:

- 24 x 7 stateful packet filtering;
- Intrusion Prevention Service (IPS);
- Whitelist and Blacklist URL filtering;
- Intrusion Detection and prevention;
- 90 days of Firewall data retention;
- Firmware and signature updates as determined by WIN best practices;
- Basic reporting for included components;
- Customer self-service for basic configuration updates;
- PCI ROC provided upon request;

c. The optional Content Filtering and Application Control includes, in addition to the components offered above, the following:

- Category-based filtering (including subcategories);
- Application Control

d. Included with FW/IPS and Content Filtering/Application Control:

- Maximum of five (5) Capability Groups
- Maximum of five (5) configured security zones per capability group
- Standard reporting and self-service configuration updates

e. The following optional elements may also be available for an additional charge:

- Active directory integration for user- or group-based security policies
- Internet Access and Service
- Wireless Modem Extenders
- High availability (multiple CPE devices at a single location)
- Professional Services
- Managed Network Services
- Managed Security Monitoring
- Voice Service including Hosted Voice Service, SIP and Line Side
- Secure Wi-Fi

*Note: not all CPE can support all feature/functionality or optional components*

f. Custom services beyond the standard product offering, if provided, require a custom Statement of Work and will incur additional charges

g. Customers must select the package containing the features that they require but are not required to activate or use all of the available components. Event correlation, log storage and security event monitoring are not included with either Service package but are available if the Customer purchases the applicable Managed Security Monitoring product.

**3. Pre-Installation Technical Documentation**. Customer must assist in the completion of technical documentation prior to installation commencement. The documentation provides WIN with the information needed to design, establish and manage the Service, including, without limitation: access bandwidth, network/failover design, LAN design, number of users, security policies and requirements and contact information for individuals authorized to approve Service changes and to be notified in the event of a security incident (Customer must ensure that a listed contact is available 24 hours a day, 7 days a week).

**4. Ancillary Services**. The Customer's Internet connection may be provided by WIN or by a third party. If Customer provides their own Internet access through a third party ISP for this service WIN will have no responsibility for configuring or troubleshooting the ISP modem or router. Additionally, the third party ISP service will need to be ordered to specific requirements provided by WIN and must be in a working condition prior to Service installation. If the third party ISP connection is not fully functioning and properly configured at the time of the scheduled installation the customer may be charged for a second installation attempt after the connection is properly functioning if the Customer requires WIN to install the Service. The ISP-provided termination device should be running in routed mode or, if running in bridged mode, Customer must have a device on the network responsible for authenticating to the ISP network. WIN will not store username and password or authenticate to the ISP network. Service requires a dedicated, ISP provided, public IP address which is assigned to the WAN port of the CPE device, which Customer should order as part of the Internet service.

**5. CPE Installation and Configuration**. CPE selection is based on the bandwidth, number of users, and Service requirements of the Customer. WIN will provide guidance to correctly size the CPE based on the requirements provided by the Customer. CPE is shipped to Customer's premises for installation by Customer with telephone assistance from WIN if required. If the requested telephone assistance troubleshooting results in an issue with the WIN provided service there will be no charges, however, if the troubleshooting uncovers an issue related to Customer provided hardware or configurations a charge will be incurred. Should the Customer require an WIN dispatch to complete the installation the Customer will be charged for a Professional Installation or a Custom Installation (defined below) The Service will be considered Installed and Sent to Billing 5

days after shipment from WIN to the Service location and the service term will begin at that time. Prior to shipment, WIN will fully configure the CPE in accordance with Customer's Technical Services Agreement (TRA) and Security Requirements Document (SRD). WIN will not be liable for damages resulting from delays in requested or specified Service dates or the inability to provide any Service due to causes beyond its control. In the event that the CPE ordered is not adequate for the Customer's purposes and a different device is required applicable monthly and non-recurring charges will apply. Alternative Installation Options – should the Customer choose to have WIN install the CPE at the Customer premises there are three (3) options to choose from. Not all options will be available in all cases. WIN on-site installation is available in the continental United States for standard rates. On site installations in Alaska, Hawaii, Puerto Rico and Canada are also available at an increased cost to the Customer, however, WIN may not be able to service all locations in those territories. For all WIN on-site installations, the Customer is responsible for the following:

- Obtain any licenses, approval and permissions required by a landlord, building manager or governmental authority for the installation and meet any insurance requirements related to the installation
- Provide a securable location suitable for electronic equipment within 6' of a 110V 15A AC power outlet
- Connection of all devices to the appropriate Ethernet ports on the WIN CPE

**Professional Installation**

Professional Installation is optional at Customer locations and can be purchased as a monthly recurring charge (MRC) or as a non-recurring charge (NRC). Professional installation is available in all cases as long as it conforms to the territory restrictions above. With a professional installation WIN will dispatch a technician to site to perform the following activities:

- Place and power the CPE in a suitable and safe location specified by the Customer
- Extend the WAN connection from the CPE to the specified access termination hardware
- Test the connectivity of the CPE to the Internet and to the aggregator
- For the Professional Installation included materials include:
    - Up to 150 feet of Ethernet Cable
    - Up to 15 feet of AWG ground wire as needed
- For the Professional Installation the included time on site is 1.5 Hours

In the event that Professional installation is insufficient for Customer's installation requirements, and WIN cannot transition to Custom installation during the Professional installation truck-roll, WIN may, at its discretion, attempt to meet expanded requirements through time and materials charges (for example, installing extra wiring). WIN also may, at its discretion, reevaluate Customer requirements and document the requirements in a revised, executed SOF, which may result in additional Customer charges.

**Concurrent Installation**

Concurrent Installation is optional at Customer locations and can be purchased as a monthly recurring charge (MRC) or as a non-recurring charge (NRC). In order to qualify for the Concurrent Installation option, the Customer must also be ordering and installing a service that includes a truck roll for installation at the same time as the Service is installed. In the event that the Customer orders Concurrent Installation and changes the installation date of one of the services so they will no longer be installed in the same truck roll the Customer will be charged for a Professional Installation for the Service. With a Concurrent Installation WIN will dispatch a technician to site to perform the following activities:

- Place and power the CPE in a suitable and safe location specified by the Customer
- Extend the WAN connection from the CPE to the specified access termination hardware
- Test the connectivity of the CPE to the Internet and to the aggregator
- For the Concurrent Installation the materials provided are part of the Professional Installation scope; no incremental materials are provided

- For the Concurrent Installation included time on site is an additional one (1) hour to the Professional Installation scope

In the event that Professional installation is insufficient for Customer's installation requirements, and WIN cannot transition to Custom installation during the Professional installation truck-roll, WIN may, at its discretion, attempt to meet expanded requirements through time and materials charges (for example, installing extra wiring). WIN also may, at its discretion, reevaluate Customer requirements and document the requirements in a revised, executed SOF, which may result in additional Customer charges.

**Custom Installation**

For installation requirements that fall outside the scope above WIN Customers can choose Custom Installation. For Custom installation the Customer will provide the required scope and WIN will provide a flat rate or time and materials rate to perform the installation at each location. As stated above, Customers who purchase Professional or Concurrent Installation who end up having installation needs outside the scope of those products can be converted to a Custom installation with the applicable charges.

**Installation Exclusions** – in no cases will the following activities be performed as part of a Professional, Concurrent or Custom installation:

- Drilling through masonry or exterior walls
- Installing wiring in attics or crawl spaces
- Wiring externally to the suite or building, including drilling through the outside of a building
- Installing wiring through multiple floors or from a DMARC to a suite in a multi-tenant unit (MTU)
- Accepting or utilizing site surveys provided by the Customer or from a third party
- Installing wiring or equipment in a location or manner that in WIN reasonable opinion would create a safety hazard including work in, above, or near food preparation areas

If any of the above are required to complete the Installation, it is recommended that the Customer utilize WIN Professional Services for such installations.

**6. Change Management**. Each Service includes support for standard policy-based configuration changes. Standard configuration changes are policy changes determined by WIN to be common, low-risk changes that do not result in significant modifications of the basic configuration design. Non-standard and complex configuration changes must be approved by WIN and, if approved, are subject to WIN's change control management procedure and applicable professional services fees and material charges. Certain changes may be expedited for a fee as determined by WIN. CPE changes only may be made by WIN. Customer is responsible for security issues resulting from Customer change requests that deviate from WIN's certified configuration. Customer is responsible for obtaining required internal approvals, following internal change control practices and validating that the requested changes do not violate PCI requirements or to have documented compensating controls in place, per PCI requirements.

**7. CPE Replacement and Return**. During the Term, WIN will replace failed CPE with an equivalent device for no additional charge. WIN will maintain a backup copy of Customer's configuration so that it may be promptly restored following replacement. Upon Service termination, or CPE replacement, Customer must request a Return Material Authorization ("RMA") from WIN and return the CPE (using the shipping labels provided) within 30 days of the termination, or replacement, or pay WIN for its replacement costs. Customer is responsible for the security of the CPE while it is on the Customer's premises and will be charged a replacement cost for any CPE or ancillary hardware, such as a wireless USB modem, that is stolen, lost or damaged.

**8. PCI Certification**. WIN will ensure that the management infrastructure and management practices of the CPE and the standard base configuration are certified annually for PCI compliance. WIN will also provide a base configuration for the

Service which has been certified for PCI compliance. The PCI certification will be limited to the CPE and Management infrastructure only and will not be extended to any other WIN services or hardware such as Hosted Phones, Managed Switches or access termination hardware. The Certification will require that the customer purchase the FW/IPS option available with the Service. For the purpose of clarity any non-IPsec VPN/MPLS IPsec Advanced hardware, provided by WIN or the Customer, in the Customer's Cardholder Data Environment (CDE) will be outside the scope for WIN's PCI certification.

Any Customer requested changes to the WIN certified configuration should be reviewed and documented through the Customer's internal change order process for PCI purposes and the configuration should be validated by the Customer's auditor to ensure PCI compliance. WIN cannot advise on the suitability of the Customer's requested changes as WIN will have no insight into the Customer's compensating controls or internal processes. If the Customer requires additional design assistance WIN provides products and services to meet that need.

**9. Network Data Usage.** The Service includes data collection and reporting on the MyLink portal for WIN management of the service and for Customer reporting and analytics. This data collection requires the use of Internet bandwidth to transfer the data between the CPE and the Management System. WIN will not be responsible for any data usage or associated charges, including any cellular wireless usage fees, incurred to facilitate the data collection and reporting.

**10. Term.** The Service can be ordered for a term of one (1) through five (5) years as set forth on the AFS ("Term"). Each Term is site- specific, commencing on the earlier of when the CPE at a particular location has been installed and the Service is available for use or five (5) days after CPE delivery ("Service Commencement Date"), and is not dependent upon the delivery of other CPE or activation of another Service location or of other services provided by other providers. Upon expiration of the Term, Customer must renew Service for another one (1) through five (5) year term prior to expiration of the Term to continue receiving maintenance support on the security software loaded on the CPE (e.g. IPS/Virus signature updates and web content category information), unless Customer or WIN has provided written notice of termination at least thirty (30) days before expiration of the Term. Thereafter, Customer or WIN may terminate the Service with thirty (30) days advance written notice prior to the end of the term. Customers who do not renew for a new term of one (1) to five (5) years, the Service Term shall automatically and continually renew for a term of one (1) year until either Party terminates the Service(s) by giving the other Party not less than thirty (30) days prior written notice of termination. WIN may increase the price of any Service renewed in a one (1) year Service Term.

**11. Billing and Payment.** The Service is provided for one or more non-recurring set up fee(s) and monthly recurring charges ("MRCs") as set forth on the AFS, which does not include taxes, fees, surcharges and other similar charges that may apply. Service Commencement Date shall be defined as the earlier of (i) the date that an WIN representative has determined the Service in production and ready for use, or (ii) all necessary equipment and/or network elements has been delivered to Customer, Invoicing will commence within five (5) days from the Service Commencement Date. Service Commencement Date shall be defined as the date in which the Service is up and running and in production or equipment has been delivered to Customer in which billing will commence within five (5) days of shipping. In the month following the Service Commencement Date, WIN will begin invoicing Customer monthly in advance for MRCs, prorated for partial months, and in arrears for non-recurring charges. All invoiced amounts must be paid within thirty (30) days, in full and in accordance with the Agreement. Customer agrees to reimburse WIN for reasonable travel and other out-of-pocket expenses incurred by it in connection with providing the Service.

**12. Summary of Features and Responsibilities.** Additional information concerning certain features of the Service and the respective responsibilities of WIN and Customer with respect to those features is summarized in the attachment to this Service Schedule ("Exhibit A"), which is incorporated into, and made a part of, the Agreement.

**EXHIBIT A**

**TO SERVICE SCHEDULE FOR IPsec VPN**

This Exhibit A supplements the Service Schedule for IPsec VPN as follows:

| IPsec VPN Features and Responsibilities | | | | | |
|---|---|---|---|---|---|
| **Service Item** | **Package** | **WIN** | **Customer** | **N/A** | **Feature Details** |
| **Management of the IPsec VPN CPE in a PCI Compliant Manner** | All | X | | | WIN will ensure that the management infrastructure supporting the IPsec VPN CPE is managed in a PCI compliant manner and will provide the ROC annually to the Customer upon request. |
| **Uninterruptible power supply, cooling, and secure environment** | N/A | | X | | Customer is responsible for providing adequate space, power, and cooling for the equipment in a physically secure environment. Damage or loss of equipment and ancillary hardware is the Customer responsibility and they will be billed for loss or damage. |
| **Network connectivity** | N/A | Optional | X | | If network connectivity is supplied by a third party, WIN does not provide a network availability SLA and will not have access to manage or monitor the device in the event of a network outage unless a backup connection is supplied. In such a case the Customer is responsible for providing adequate bandwidth for the Internet services being consumed and for management and monitoring. Customer can purchase WIN provided and managed primary or backup access and the same backup caveats as above apply. |
| **Device installation** | All | Optional | X | | Customer, with telephone assistance from WIN, is responsible for installing, cabling, and powering on the device. Customer can purchase WIN on-site installation. |
| **Customer Premises Device (CPE)** | All | X | | | WIN provides the physical hardware device, which remains WIN property and must be returned at the end of contract. Shipping is provided by WIN and Customer is responsible for packaging and delivering the box to the shipping company in the event of a RMA/ARA or cancellation. If the hardware is not returned Customer will be billed applicable charges. |
| **Firewall hardware maintenance** | FW/IPS | X | | | WIN provides hardware support and maintenance through the device vendor, with 8x5xNBD replacement, shipping provided by WIN and Customer is responsible for packaging and delivering the box to the shipping company in the event of a RMA/ARA. Maintenance contract is owned by WIN. |
| **Applicable Firewall UTM Licenses** | FW/IPS and CF/AC | X | | | Licensing is owned by WIN provided as part of the managed service. |
| **Stateful packet filtering, NAT, PAT** | FW/IPS | X | | | WIN will configure the firewall device to perform basic stateful packet filtering to restrict both inbound and outbound traffic using best common practices and customer requirements, including the use of Network Address Translation (NAT) and Port Address Translation (PAT). |
| **IPsec VPN** | All | X | X | | WIN will take full responsibility if both endpoints are on WIN-managed equipment. If one end is managed by |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | the Customer or a third party, customer will make appropriate arrangements to supply a technical resource familiar with the equipment to set up the remote end of the VPN in coordination with WIN. WIN does monitor VPN tunnels for up/down. WIN will take reasonable efforts to restore a down tunnel but will not troubleshoot a non-WIN provided access issue unless the Customer has purchased Managed Network Services (MNS). WIN's PCI compliance does not extend to IPsec VPN tunnels to non-WIN provided and managed end points. Customers are responsible for validating the PCI compliance of any vendor that connects to their IPsec VPN network. |
| **Category-based web content filtering** | CF/AC | X | | | WIN will configure the firewall device to restrict web traffic to categories and subcategories as per Customer's business, security, and compliance requirements. |
| **URL filtering (whitelist/blacklist)** | FW/IPS | X | | | WIN will configure the firewall device for additional website whitelisting or blacklisting as per the Customer's specifications. |
| **Application Control** | CF/AC | X | | | WIN will configure the firewall device to permit or block categories or specific applications as per the Customer's business, security, and compliance requirements. |
| **Intrusion Prevention Service (IPS)** | FW/IPS | X | | | WIN will configure the firewall device to monitor for known attack signatures, either alerting or blocking matching traffic as per vendor recommendations and best practices. |
| **Configuration backup and restore** | All | X | | | WIN will maintain a backup copy of the Customer's configuration so that it may be restored in the event of a device failure and replacement. In event of device failure, it will be replaced and the configuration restored in accordance with WIN's SLA for Managed Security Device Replacement. |
| **Firmware and signature updates** | All (where applicable) | X | | | WIN will test and install device firmware updates in a timely manner (within thirty (30) days of vendor release) during scheduled maintenance windows. Signature updates for UTM services will be pushed automatically as issued by the vendor. |
| **Proactive monitoring of device** | All | X | | | WIN will monitor the firewall for availability and proper functioning up to the Ethernet LAN interfaces, and will resolve any maintenance issues to that point of demarcation. |
| **Incident response** | All | X | X | | WIN will assist in mitigating security incidents through the modification of firewall perimeter policy. Customer is responsible for mitigation beyond the firewall LAN interface demarcation point. |
| **Security contacts** | All | | X | | Customer will provide a list of security contacts to be notified in the event of a critical issue, device event, or outage, who are authorized to approve changes, and who are authorized to change the list of approved contacts. |
| **Security policy and requirements** | All | Best Practices | X | | Customer will supply sufficiently detailed information about network infrastructure, assets, and security requirements to allow design and implementation of appropriate device policies. |
| **Standard reporting** | All | X | | | WIN will supply standard reports for the included services via email on the schedule requested by |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | the Customer. |
| **24x7x365 support** | All | X | | | WIN will provide assistance and troubleshooting, as well as make any required standard configuration changes on the device, where standard configuration changes are low-risk changes which do not change the basic design of the service. |
| **Security Assessment** | | X | | | WIN will perform a basic external vulnerability assessment after the device is installed and configured, to verify that no well-known vulnerabilities are exposed to the Internet. |
| **Performance Data Retention** | FW/IPS and CF/AC | X | X | | WIN will retain ninety (90) days of Firewall data available for retrieval in .csv format and provide reporting in the MyLink portal. Customers who require longer data retention or real time access to logs can stream the logs to a collection server of their choice or can purchase the service through the Managed Security Monitoring (MSM) portfolio. If the Customer chooses not to stream logs or purchase MSM from WIN for log retention WIN is *not* able to provide historical log data for export/import. |