



SECURETEC Private IP-VPN Standard Terms and Conditions

In addition to the general terms and conditions contained in the service agreement between PAETEC and Customer (the "Agreement"), of which this Schedule is a part, Customer agrees that the following terms and conditions apply to the Virtual Private Network Service provided to Customer by PAETEC.

1. Private IP-VPN Service

PAETEC Private IP-VPN Services includes IPSec, (Internet Protocol Security), MPLS, (Multi-protocol label switching), and MPLS with QoS (Quality of Service.). Customer must chose between Managed and Unmanaged Router Configuration Service service which are defined further in this document

PAETEC shall provide, and Customer shall accept and pay for, Private IP Virtual Private Network Service at the rates set forth on the Rate Schedule of the Agreement. Private IP VPN Service provides a data connection between Customer sites for the purpose of permitting Customer's employees, business partners, and customers to receive and transmit data via a secure connection. PAETEC's Private IP-VPN Service offers both dedicated (e.g., via T1) and remote access options..

(a) Dedicated Access

- i. Hub and Remote Locations. Customer's primary physical location for its Private IP-VPN Service connection to the PAETEC network (hereinafter the "Hub Location") must be located within the serving area of a PAETEC switch (hereinafter "On-Net"). All Customer Remote Sites connected to the Hub Location through the Private IP-VPN Service must also be located within the PAETEC Private IP-VPN service area, unless otherwise agreed by the Parties in writing. As used herein, the term "Remote Site" means any Customer location where the Private IP-VPN Services are to be provided, which location is not the Hub Location. Connectivity to an off-net Remote Site must be available from one of PAETEC's network partners in order for PAETEC to approve an off-net Remote Site for inclusion in the Private IP-VPN Service.

(b) Remote User Access

- i. For an additional fee, Customer may subscribe to the remote access feature of the Private IP-VPN Service to allow individual employees of Customer that are not located at a fixed Remote or Hub site location ("Remote User") to connect to the Private IP-VPN Managed Service. For the avoidance of doubt, the provisions of Section 2B or 3B below do not apply with respect to support of the Remote User equipment or devices.
- ii Remote users access their Private IP-VPN network via PAETEC's RADIUS server utilizing the Cisco client software. The RADIUS server via a username and password authenticates remote users. PAETEC shall establish a Customer Administrator Account to allow Customer's Administrator to set up usernames and passwords for remote access to the Private IP-VPN Service. PAETEC shall provide Customer's Administrator with Cisco remote client software that Customer's Administrator can install on designated computers to allow remote user access to the Private IP-VPN Service using 3DES encryption. If the Customer requires non-standard encryption, Customer shall be required to obtain the software directly from Cisco in accordance with the provisions above. PAETEC shall not be responsible for provisioning or maintaining the Internet connectivity for a remote user. The Cisco software does not provide any security

measures or replace the need for Customer to establish its own security measures (e.g. firewalls or antivirus schemes) for its remote users.

2. Provision of Managed Router Configuration Service

Managed Router Configuration for Private IP-VPN Service is defined as service in which PAETEC maintains the configuration of the Customer routers (including passwords) that are used to connect to the Service.

(a) Customer Obligations

- (1) Customer must provide PAETEC with the ability to remotely access the configuration on Customer's Equipment in order for PAETEC to fulfill its obligations (as defined in Section 2B).
- (2) For IPsec and MPLS Private IP-VPNs, Customer must furnish and maintain a PAETEC approved CPE device. Customer should consult with the PAETEC assigned account team.
- (3) For both MPLS and IPsec services, a router must be used to terminate the dedicated connection (e.g., T1, DS3, Ethernet, etc...) from PAETEC. For IPsec service, the Customer equipment must be capable of terminating an IPsec tunnel. This equipment may be the router used to terminate the dedicated connection or a separate firewall.
- (4) For Customer Equipment at the Hub Location and each Remote Site, customer must maintain a maintenance agreement through PAETEC Integrated Solutions Group, Inc. ("ISG"). Cisco equipment can be supported via an Onsite SMARTnet maintenance agreement and Adtran equipment can be supported via the ACES or via the CPE Maintenance Agreement.
- (5) Software and Applications. Customer shall be responsible for installing, supporting, and maintaining applications that utilize the Private IP-VPN Service (e.g., email service, database applications). In the event PAETEC provides assistance to Customer, at Customer's request, regarding these applications, Customer agrees to pay PAETEC for such services on a time and materials basis.
- (6) Encryption. For the IPsec Private IP-VPN Managed solution, PAETEC shall provision and maintain the IPsec tunneling with standard, publicly released and general available encryption software (i.e., currently 3DES encryption) between Customer's Remote Sites and the Hub Location. Customer shall be responsible for registering for and supplying to PAETEC any non-standard encryption software and for complying with all use obligations and restrictions related to such non-standard encryption software (including without limitation export restrictions).
- (7) Customer acknowledges that PAETEC shall not be liable for CPE that is not purchased and maintained through PAETEC, which includes credits associated with service interruptions caused by the customer owned CPE.

(b) PAETEC Obligations

- (1) For Dedicated Customer applications (i.e. Customers that utilize IPsec and/or MPLS), PAETEC shall provide the following configuration services as part of the Managed Router Configuration Service on the customer equipment located at the Hub and Remote Sites. PAETEC will not provide the following services for any Remote Users (defined in the Introduction).
 - (a) Reload/install software as deemed necessary by PAETEC
 - (b) Reconfigure LAN interface per customer requests
 - (c) Reconfigure WAN interface per customer requests
 - (d) Reconfigure existing software-based services including:

- IPSec services (software based)
 - Access Lists
 - Network Address Translation (NAT)
 - Port Address Translation (PAT)
 - Security services (software-based)
 - Firewall services (software-based)
 - DHCP Server service (software-based)
 - Secondary Interfaces
 - Quality of Service (QoS)
- (e) Add new software-based services including:
- Network Address Translation (NAT)
 - Port Address Translation (PAT)
 - Security services (software-based access lists)
 - Firewall services (software-based) (provided that existing software supports firewall)
 - DHCP Server service (software-based)
 - Secondary Interfaces
 - Quality of Service (QoS)
- (f) Test all configuration changes and additional services as required
- (g) PAETEC will maintain a backup copy of the router configuration and logs used to track access to the router and changes made to the configuration.

(2) Router Access Rights

PAETEC is responsible for the Configuration, IOS updates (when PAETEC deems it necessary for an upgrade), and security configuration of the CPE gear. The customer will not be allowed access to the router configuration from either VTY access, console connection or auxiliary connectivity. If requested, Customer can get a restricted level of read access to the router where they can view the status of the interface only. Read access to view the configuration or version of code of the router will not be permitted. If a copy of the configuration is needed, PAETEC can supply an electronic copy of the configuration with the sensitive information removed. Unauthorized access to the router without PAETEC's permission is in violation of the Managed Router Configuration agreement.

- (a) Customer can obtain Read-only SNMP and Syslog information from the router.

SNMP information will include alarms for:

- (i) Up/down interface
- (ii) Environmental and CPU processing

Syslog information will include:

- (i) All configuration log error messages.

Note: the customer must provide PAETEC with a server IP Address to pass on the information to as well as the SNMP read-only community string. The server must reside on the customer LAN and not traverse the Internet (this is for security reasons). If for any reason the router has been tampered with, the CPE will be taken off of Managed Services and treated as a billable account for any changes.

- (b) Customer must have explicit written permission from PAETEC to access or configure the router. All activities performed on the router may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. "Unauthorized access" is defined above. Customer agrees to defend and hold harmless PAETEC from any unauthorized access of the network device.

3. Provision Unmanaged Router Configuration Service

Unmanaged Router Configuration for Private IP-VPN Service is defined as service in which only the customer has access to the configuration (including passwords) of the customer routers that are used to connect to the Service.

(a) Customer Obligations

(1) Customer will be responsible for configuring and maintaining their own router hardware. PAETEC will consult with customer on the initial configuration of the router. Ongoing configuration assistance after the initial turn-up will be charged on a time and material basis.

(2) PAETEC will not have access to the customer's router configuration and will not be able to track access to the router and changes made to the configuration. PAETEC will not maintain a backup copy of the customer router configuration. Backup configuration copies are the responsibility of the customer.

(3) QoS Configuration. If the Customer needs to make a change to the original Quality of Service (QoS) settings, the customer is required to report those changes to PAETEC by calling Customer Service and opening a trouble ticket. QoS policy changes need to be reported so PAETEC can make the necessary modifications on the Provider Edge (PE) router to ensure that QoS will work as expected.

(4) For PRIVATE IP-VPN MPLS & IPSec Services, Customer must furnish and maintain a PAETEC approved CPE device. Customer should consult with the PAETEC assigned account team. For Unmanaged IPSec VPN's, PAETEC will set the IPSec and isakmp policies.

(5) Software and Applications. Customer shall be responsible for installing, supporting, and maintaining applications that utilize the PRIVATE IP-VPN Service (e.g., email service, database applications). In the event PAETEC provides assistance to Customer, at Customer's request, regarding these applications, Customer agrees to pay PAETEC for such services on a time and materials basis.

(6) Customer acknowledges that PAETEC is not liable for CPE that is not purchased and maintained through PAETEC, which includes credits associated with service interruptions caused by the customer owned CPE.

(b) PAETEC Obligations

(1) Installation of Service. PAETEC shall be responsible for ordering, provisioning and installing the PRIVATE IP-VPN network, including the local loop. PAETEC will work with the customer and/or customer's vendor to activate the IPSec, MPLS, or MPLS with QoS service for each location.

(2) Support. The customer shall call PAETEC's Customer Service to initiate standard troubleshooting procedures. As part of standard troubleshooting procedures, the PAETEC Network Operations Center will:

(a) Loop the NIU, (Network Interface Unit) or local loop. If the T1 facility (local loop) requires maintenance, PAETEC will refer the trouble to the LEC (Local Exchange Carrier).

(b) Loop up the CSU (Channel Service Unit). If PAETEC determines that the customer CSU requires maintenance, PAETEC shall advise the customer to refer the trouble to their vendor.

(c) Check status on PAETEC's network aggregate router. Once it has been determined that the PAETEC network and/or the local loop is not the source of the problem, the customer will be advised to contact their vendor if applicable.

PAETEC may require that the customer temporarily allow access to the router to perform diagnostics and determine a solution during troubleshooting.

If the customer requires additional support after it has been determined that the source of the problem does not reside within the PAETEC network and/or the local loop, the customer will be given the option to continue to work with PAETEC technical support for a fee or to work directly with their vendor, if applicable.

4. Router Installation and Configuration Charges

- (a) Initial Configuration, Installation and Maintenance
 - (i) PAETEC Provided Router – As per the ISG Order Form
 - (ii) Non-PAETEC provided and Supported Router - \$175 per hour, with a 2-hour (\$350) minimum.
 - If on-site installation is required the minimum is 8 hours.

PAETEC shall charge \$99.00 per hour, with a minimum of two hours for trouble resolution that does not require a dispatch.

5. Acceptable Uses

- (a) Customer agrees to adhere at all times to the PAETEC Acceptable Use Policy (the “AUP”), as such AUP may be modified by PAETEC from time to time. The current AUP is available for review at <http://www.paetec.com/aup>. PAETEC has the right to modify its AUP at any time without prior notice to Customer. Customer is responsible for monitoring the website at <http://www.paetec.com/aup> for changes to the AUP. Customer shall be bound by such modified AUP.
- (b) Customer shall be responsible for enforcing the AUP for any third parties (including its customers or end users) that access the Internet through Customer’s use of the PAETEC Internet service. Customer shall defend and indemnify PAETEC with respect to all claims related to Customer’s or any such third parties’ use of the Internet service in violation of the then-current AUP.
- (c) PAETEC has the right to immediately and without regard to any cure periods that may be set forth elsewhere in the Agreement, suspend and/or terminate the Internet service to Customer, or to take any other action that PAETEC determines, in its sole discretion, is appropriate in response to Customer’s, or Customer’s end user’s or any other customers of Customer failure to comply with the requirements of PAETEC’s then-current AUP.
- (d) Customer and its customers and end users are responsible for the security of their own networks and machines. PAETEC assumes no responsibility or liability for failures or breach of protective measures on Customer’s network, whether implied or actual, even in the event that the security measures have been installed or configured by PAETEC. Security problems on Customer’s systems that affect the PAETEC network or cause any system abuse or any other violations of the AUP may result in suspension of the Internet service or account access by PAETEC. Customer shall solely be responsible for addressing problems on Customer’s network escalated to PAETEC for resolution that involves compromise of Customer’s security.
- (e) Customer acknowledges that the transfer and use of products, Services and technical information outside the United States are subject to U.S. export laws and regulations. Customer shall not use, distribute, transfer, or transmit the products, Services or technical information (even if incorporated into other products) except in compliance with U.S. export laws and regulations. At PAETEC’s request, Customer shall sign written assurances and other export-related documents as may be required for PAETEC to comply with U.S. export regulations.

6. Maintenance

PAETEC periodically performs maintenance on its network. In some cases, a maintenance window may result in a temporary service interruption to PAETEC customers. PAETEC will use all reasonable efforts to provide notification of the network maintenance on the PAETEC website at <http://www.paetec.com/maintenance>. Customers have the option to receive notification of a network maintenance window via email by subscribing to a mailing list at the PAETEC website listed in the foregoing sentence. The capability to subscribe to the mailing list is provided for customers who would prefer to receive an email regarding a maintenance window versus checking the PAETEC website. (Customers also have an option to unsubscribe to the mailing list at the PAETEC website.)

A description of the various types of network maintenance classifications is set forth below. Each maintenance description specifies when notification will be provided prior to the start time of the scheduled maintenance. Maintenance notification will include a list of the cities affected, a description of the maintenance, and the duration of the maintenance window. The maintenance window for backbone devices is between midnight and 6:00 a.m., local time zone at the affected sites.

Customer acknowledges that PAETEC shall not be liable for service interruptions that may occur due to maintenance activity as described herein or for failure to provide advance notice of the maintenance on PAETEC's website or in an email to subscribers to the email maintenance list.

Maintenance Classifications:

Normal Scheduled Maintenance - Normal Scheduled Maintenance is defined as maintenance that will enhance the reliability of the network. This includes, but is not limited to upgrading code, reloading routers, and adding new equipment. Notification for this type of maintenance will be provided 72 hours prior to the start of a Normal Scheduled Maintenance window.

Urgent Scheduled Maintenance - Urgent Scheduled Maintenance is defined as maintenance that is performed when the potential for router or network failure exists without the scheduled maintenance. This includes, but is not limited to hardware and software upgrades, and router debugging. Notification for this type of maintenance will be provided 48-72 hours prior to the start of an Urgent Scheduled Maintenance window.

Emergency Maintenance - Emergency Maintenance is performed when catastrophic events have occurred on the network. This is limited to maintenance necessary to correct the event that occurred during an unplanned outage. Notification for this type of maintenance will be provided on a best effort basis.

7. Billing and Payment

(a) The rates and charges for the Private IP-VPN Service are set forth in the Rate Schedule to the MSA. Additional On-Net locations may be added at any time during the Term of the Agreement at the rates set forth in the Rate Schedule. Off-Net locations shall be priced subject to availability on an ICB basis.

(b) Billing (loop and port MRC and NRC), shall commence once any site has been installed. The customer is required to coordinate with PAETEC to install the hub site first, with each remote site to follow.