PAETEC

MANAGED CPE FIREWALL SERVICE
TERMS & 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 Managed CPE Firewall Service provided to Customer by PAETEC.

I. *Managed CPE Firewall Service*

A. Overview: PAETEC's Managed CPE Firewall Service is customer premise based security offering providing the Customer an additional mechanism to be used in protecting the Customer's network. A CPE-based firewall device is a piece of hardware that is placed between the Customer's internal LAN and the Customer's internet access. PAETEC's Managed CPE Firewall Service, as with most security solutions, provides one layer of security for a Customer's network. In all instances, Customer is solely responsible for localized security protection within its own network.

B. Service Components:

- Equipment and Imbedded Software: PAETEC provides the Customer with a firewall device (the "Firewall Device"). The Firewall Device includes software to enable premise-based filtering of the incoming data traffic to assist in the protection of the premise LAN from a wide variety of threats.

- Device Availability Monitoring:
  - Automated Alarm Notification to PAETEC's Data Technical Assistance Center (TAC) in the event of a loss of Firewall Connectivity, which is defined as an interruption of all traffic flow through the Firewall Device due to firewall failure.
  - PAETEC will troubleshoot the cause of the failed firewall connectivity. PAETEC is not responsible for troubleshooting issues that are not directly related to the Managed CPE Firewall Service, the PAETEC Service or the PAETEC network, as determined by PAETEC in its sole discretion.

- Patch and Upgrade Management:
  - Maintaining and updating applicable patches and/or upgrades for the Firewall Device.
  - If a software patch and/or upgrade is released, PAETEC will assess the applicability of such release as to the Firewall Device. If an upgrade is completed on the Firewall Device, the Customer will be required to utilize the new version by default. PAETEC will use best efforts to inform Customer of any such upgrade prior to activating the changes.

- Change Management:
  - Managing configurations and any logical or physical faults related to the Firewall Device.
  - Adding, deleting or modifying Network Address Translations, Access Control lists and/or network routes.
  - The Customer must request such change through the opening of a trouble ticket. Customer must provide PAETEC a detailed description of the change. Customer is responsible for any security issues that may arise resulting from Customer initiated change requests.

C. Service Activation and Customer Responsibilities: Prior to installation of the Firewall Device, Customer must provide PAETEC with the following:

- Satisfactorily completed Network Assessment Sheet.
- All necessary IT department contact information related to both security responsibilities and internal network management as requested by PAETEC.
- All information necessary or requested for service activation including firewall rule sets, NAT / PAT translations, IP information and ACL lists.

Customer must also maintain physical site requirements for the Firewall Device as required by PAETEC (e.g., temperature, power, space). Customer must provide an internet router in front of the Firewall Device. The router will need to be configured to allow all traffic to pass to and from the Firewall Device. Customer must also subscribe to PAETEC's internet service or VPN service and must maintain internet connectivity between PAETEC's TAC and the Firewall Device.

II. ***Terms and Conditions***

A. The Firewall Device is provided on a rental basis and not for sale. Customer agrees to use the Firewall Device solely in connection with the PAETEC Managed CPE Firewall Service. PAETEC and/or its suppliers have and will retain all rights, title and interest in and to the Firewall Device, including any intellectual property rights therein. Use of the Firewall Device may be subject to end-user licenses that are included with the Firewall Device. Customer will not remove any identification tags or other markings on the Firewall Device and will not cause, create or suffer any claims, liens, charges or encumbrances or security interests in, on or to the Firewall Device.

B. Disclaimers; Warranties. CUSTOMER IS PROVIDED THE FIREWALL DEVICE ON AN AS IS BASIS AND PAETEC MAKES NO WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, AS TO THE MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, DESIGN OR CONDITION OF THE FIREWALL DEVICE, OR THE MANAGED CPE FIREWALL SERVICE, OR INTELLECTUAL PROPERTY RIGHTS (INCLUDING WITHOUT LIMITATION ANY PATENT, COPYRIGHT AND TRADEMARK RIGHTS, OF ANY THIRD PARTY WITH RESPECT TO THE FIREWALL DEVICE, WHETHER RELATING TO INFRINGEMENT OR OTHERWISE) WITH RESPECT TO THE FIREWALL DEVICE. PAETEC DOES NOT GUARANTEE THAT THE MANAGED FIREWALL SERVICE WILL PROTECT CUSTOMER FROM UNAUTHORIZED NETWORK INTRUSION OR SECURITY THREATS OR BREACHES.

C. If Customer is unable or unwilling to schedule or accept delivery or installation on the date PAETEC tenders delivery or installation, PAETEC shall have the right to initiate billing for the amounts due hereunder as of the date delivery was tendered.

D. With regard to any software components of the Firewall Device, Customer agrees it will not: (i) use or make any copies of the software; (ii) reverse engineer, decompile, or disassemble the software; (iii) sell, resell, transfer, license, sublicense, or distribute the software; or (iv) create, write, or develop any derivative software or other software program that is based on such software. Customer agrees to indemnify, defend and hold PAETEC 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 the foregoing.

E. Customer shall be solely responsible for the return of the Firewall Device to PAETEC, in good repair, condition and working order, ordinary wear and tear excepted, within thirty (30) days of termination or expiration of the Agreement. If Customer fails to return the Firewall Device within that period, PAETEC shall have the right to: (a) invoice Customer for the full replacement value for the Firewall Device; and/or (b) pursue any other right it may have at law or in equity.

III. ***Authorization to Perform Testing; Associated Risks.*** Certain laws and regulations prohibit the unauthorized penetration of computer networks and systems. Customer hereby grants PAETEC the authority to access Customer's networks and computer systems solely for the purpose of providing the Managed CPE Firewall Service. Customer acknowledges that the Managed CPE Firewall Service constitutes permitted access to Customer networks and computer systems. In the event one or more of the IP Addresses Customer gives to PAETEC are associated with computer systems that are owned, managed, and/or hosted by a third party service provider ("Host"), Customer agrees to: (i) notify PAETEC of such Host arrangement prior to the commencement of any Managed CPE Firewall Service; (ii) obtain Host's written consent for PAETEC to provide the Managed CPE Firewall Service on Host's computer systems, which includes acknowledgement of the risks and acceptance of the conditions set forth herein; (iii) provide PAETEC with a copy of such consent, acknowledgement and acceptance; and (iv) facilitate any necessary communications and exchanges of information between PAETEC and Host in connection with the Managed CPE Firewall Service. Customer agrees to indemnify, defend and hold PAETEC 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. Customer will indemnify and hold PAETEC and its suppliers harmless 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 Managed CPE Firewall Service entail 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 Managed CPE Firewall Service; (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.

IV. ***Service Level Objective.*** PAETEC will provide (i) Scheduling of Change Requests and (ii) Confirmation of the completion of Change Requests to Customer within certain periods of time in accordance with the chart in this section. Subject to the provisions of the Agreement, failure to meet these parameters will result in a credit allowance to Customer, upon written request of the Customer no later than ten (10) business days after the occurrence of the failure to notify, schedule and/or confirm such Change Request event to the PAETEC Account Manager handling Customer's account or to the PAETEC Customer support center in Fairport, New York. Credit allowances will be calculated and applied on a pro rata basis against the monthly recurring charge ("MRC") for the Managed CPE Firewall Service as follows, with the understanding that for calculating credit allowances, every month is considered to have 30 days. In no event will the credit(s) provided hereunder (either individually or on a cumulative basis) in any billing period exceed the total monthly recurring charge for the Managed CPE Firewall Service. The credits set forth in this section shall be PAETEC's sole liability and Customer's sole remedy in the event of any failure of the Managed CPE Firewall Service and under no circumstances shall a failure of the Managed CPE Firewall Service be deemed a breach of the Agreement.

a. PAETEC Managed CPE Firewall Service Guarantee and Remedy:

Scheduling of Standard Change requests completed within one (1) business day of submission by Customer through the opening of a trouble ticket	1/30th of the Managed CPE Firewall Service MRC
Scheduling of complex change requests (such as alteration of network topology, adding a new server / application) completed within four (4) business days of submission by Customer through the opening of a trouble ticket	1/30th of the Managed CPE Firewall Service MRC
Notification to Customer within 60 minutes, of firewall service affecting events.	1/30th of the Managed CPE Firewall Service MRC