PAETEC

NETWORK FIREWALL SERVICE
STANDARD 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 Network Firewall Service provided to Customer by PAETEC.

I. ***Network Firewall Service Overview*.**

PAETEC's Network Firewall Service is a network based security service offering Customer access to firewall functionality to or from Customer's network.

a. PAETEC Managed Network Option Firewall Service Components

- Device Availability Monitoring:
  - Automated Alarm Notification to PAETEC's Network operations center in the event of a loss of Firewall Connectivity. Failed firewall connectivity is defined as an interruption of all traffic flow through the Firewall. In the event of a failed firewall connectivity traffic will not be passed to the public internet until the connectivity is restored. If service is interrupted as a result of such failed connectivity the credits under the PAETEC SLA will apply.
  - PAETEC will troubleshoot the cause of the failed firewall connectivity. PAETEC is not responsible for troubleshooting issues that are not directly related to the Network Firewall, the PAETEC Service or the PAETEC network, as determined by PAETEC in its sole discretion.
  - Access to real time web portal to view the status / logs of customers network firewall.
- Patch and Upgrade Management:
  - Maintaining and updating applicable patches and/or upgrades for the network firewall devices.
  - If a software patch and/or upgrade is released, PAETEC will assess the applicability of such release as to the network firewall device. If an upgrade is completed on the network firewall device, the Customer will be required to utilize the new version by default. PAETEC agrees to inform Customer of any such upgrade.

- Change Management:
  - Managing configurations and any logical or physical faults related to the network firewall. This includes configuration and change management, patch upgrades and firewall change requests.
  - Adding, deleting or modifying Network Address Translations, Access Control lists and/or firewall 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. PAETEC shall not be responsible for designing or validating Customer policies and rule sets.

b. Customer Managed Network Option Firewall Service Components

- Device Availability Monitoring:
  - Automated Alarm Notification to PAETEC's Network operations center in the event of a loss of Firewall Connectivity. Failed firewall connectivity is defined as an interruption of all traffic flow through the Firewall. In the event of failed firewall connectivity traffic will not be passed to the public internet until the connectivity is restored. If service is interrupted as a result of such failed connectivity the credits under the PAETEC SLA will apply.
  - PAETEC will troubleshoot the cause of the failed firewall connectivity. PAETEC is not responsible for troubleshooting issues that are not directly related to the Network Firewall, the PAETEC Service or the PAETEC network, as determined by PAETEC in its sole discretion.
  - Access to real time web portal to view the status / logs of customers network firewall.

- Patch and Upgrade Management:
  - Maintaining and updating applicable patches and/or upgrades for the network firewall devices.
  - If a software patch and/or upgrade is released, PAETEC will assess the applicability of such release as to the network firewall device. If an upgrade is completed on the network firewall device, the Customer will be required to utilize the new version by default. PAETEC agrees to inform Customer of any such upgrade.

- Change Management:
  - The customer Managed version of the Network Based Firewall product does not include PAETEC change management. If such a service is needed using this option, additional charges may apply.

II. ***Service Activation.***

Prior to commencement of either the PAETEC Managed or the Customer Managed Network Firewall Service, as selected by Customer, Customer must provide PAETEC with the following:

- Satisfactorily completed Network Assessment Sheet, provided to Customer by PAETEC.
- All necessary IT department contact information related to both security responsibilities and internal network management as requested by PAETEC.
- Confirmation that Customer has configured its CPE equipment to allow transmission of all earmarked traffic through the network firewall appliance residing on the PAETEC network.
- All information necessary or requested for service activation including firewall rule sets, NAT / PAT translations, IP information and ACL lists.

IV. ***Service Level Objective.***

PAETEC's 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 either Customer's PAETEC Account Manager (if applicable) 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 Network 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 Network Security 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 Network Firewall Service and under no circumstances shall a failure of the Network Firewall Service be deemed a breach of the Agreement.

a. PAETEC Managed Network Option Firewall Service Guarantee and Remedy

Scheduling of Change requests completed within one (1) business day following (i) submission of a Change request by Customer through the opening of a trouble ticket and (ii) within one (1) business day of PAETEC's verification and validation of the Change request with Customer.	$1/30^{th}$ of the Network Firewall Service MRC
Confirmation of completion of Change Requests to Customer within one (1) business day after completing such Change Request	$1/30^{th}$ of the Network Firewall Service MRC