PAETEC

Intrusion Detection and Prevention System 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 Intrusion Detection and Prevention System ("IDPS") Service provided to Customer by PAETEC.

1. Intrusion Detection and Prevention System (IDPS) Service

PAETEC's IDPS Service is a network-based security service which monitors network traffic and analyzes the network and application protocol activity to identify suspicious activity and mitigate security risks that arise from such activity.

A. Device and service availability:

(1) Automated alarm notification to PAETEC's Network Operations Center in the event of a loss of IDPS sensor/event correlation engine connectivity. Failed sensor/event correlation engine connectivity is defined as an interruption of all traffic flow through the sensor/event correlation engine. If IDPS Service is interrupted as a result of such failed connectivity the credits outlined in the PAETEC Service Level Agreement will apply.
(2) PAETEC will troubleshoot the cause of the failed connectivity. PAETEC is not responsible for troubleshooting issues that are not directly related to the IDPS Service, IDPS related equipment provided by PAETEC, other PAETEC Services or the PAETEC Network, as determined by PAETEC in its sole discretion.

B. Patch and upgrade management:

(1) PAETEC is responsible for maintaining and updating applicable patches and/or upgrades for the IDPS and devices.
(2) If a software patch and/or upgrade is released, PAETEC will assess the applicability of such release to the PAETEC IDPS device and supporting systems. If an upgrade is completed on the PAETEC IDPS devices and/or reporting systems, the Customer will be required to utilize the new version by default. PAETEC agrees to inform Customer of any such upgrade.

C. Change Management, Incidents, and Service Requests

(1) PAETEC is responsible for managing configurations and any logical or physical faults related to the IDPS Service. This includes configuration and change management, patch upgrades, and IDPS change requests.
(2) The Customer must request a change, report an incident, or submit a service request through the opening of a trouble ticket. Customer must provide PAETEC a detailed description of the change. Change requests can be submitted by contacting the Security Operations Center by phone at 877.340.2555 or by submitting a change request ticket through PAETEC Online.
(3) The PAETEC Security Operations Center assigns a priority to every incident, change, or service request initiated. Customer is responsible for providing and maintaining an accurate list of approved security contacts within that its organization to PAETEC. The SOC prioritization model is used to provide consistency with which an item needs to be resolved and to drive the assignment of resources. Prioritization depends on:

i. Time within which resolution is required (based upon alarm types described in this document).
ii. Resource availability.
iii. Size, scope, and complexity of an incident, change, or service request.

D. Hours of support:

(1) PAETEC's Network Operations Center and Security Operations Center operate 24x7 and offer support for all customer inquiries related to the IDPS product.

E. Customer Requirements:

(1) These terms and conditions and the parameters set forth within are valid only if Customer and their appointed security contact make themselves available to PAETEC as needed for consultation, resolution and to provide all security permissions reasonably required by PAETEC to appropriately protect the Customer's network.

2. Service Activation

A. PAETEC's provision of the IDPS Service is contingent upon Customer's agreement to make itself available to PAETEC as needed for consultation and to provide all security permissions reasonably required by PAETEC. Accordingly, prior to commencement of IDPS Service, Customer must provide PAETEC with the following:

(1) Satisfactorily completed Network Assessment Form, provided to Customer by PAETEC.
(2) All necessary IT department contact information related to both security responsibilities and internal network management as requested by PAETEC.
(3) All information necessary or requested for service activation.

B. Service Implementation and support includes:

(1) Consultation regarding security configurations that best fit the customer's needs.
(2) Any required activities to complete service installation.
(3) Configuration and support of hardware and software components.
(4) 24x7 technical support including centralized monitoring, management, and remediation through PAETEC's Security Operations Center.
(5) Customer notification of pre-identified critical events.
(6) Customer access to logs for the preceding 180 days unless otherwise agreed upon with Customer.
(7) Customer-defined security posture to meet Customer's security requirements, including periodic review of security policies to assure a secure Customer network environment.
(8) Documented processes for remediation workflow support and incident management.

3. Change Management

Scheduling of change requests will be completed within one (1) business day following (i) submission of a change request by Customer through the opening of a trouble ticket and (ii) PAETEC' s verification and validation of the change request with Customer.

Confirmation of completion of change requests will be sent to Customer within one (1) business day after completion.

Customer-requested change escalations carry a one-time escalation charge of $120.00/hour.