Service Specific Term for Managed Firewall Service

This service is subject to and governed by customer's separate signed Master Services Agreement (MSA), with FirstNet Technology Services, calling itself FirstNet for short. This agreement is entered into between the customer and FirstNet for the provision of managed firewall services.

1. **Service Description -** Managed firewalls protect the customer network from unauthorized access and malicious attacks. Firewalls are the critical gateway into a network, and firewalls managed by FirstNet come with the highest degree of attention and expertise to protect critical customer assets and provide protection at the customer perimeter.

1.1 Managed Firewall services are available in two categories:

1.1.1 **Managed Firewalls -** are a fully managed firewall solution offered by FirstNet exclusively, including policy and configuration. The service is tailored to meet the customer's changing business requirements.

1.1.2 **Delegated Administration -** is a solution for customers that want their technical staff and managed service providers external to FirstNet to maintain an active role in the administration of the customers perimeter firewall.

2. **Service Availability -**

FirstNet will use best efforts to have the service available 24 x 7.

3. Responsibilities -

3.1 FirstNet shall furnish the necessary personnel, equipment, material and/or services and otherwise do all things necessary for or incidental to the performance of work as set forth below.

3.1.1 **FirstNet Responsibilities -**

- The service will be available 24 x 7. Unless a maintenance window has been scheduled with the customer in which case the uptime availability counter will stop and restart after the maintenance window.
- Management and configuration access is only granted to authorized FirstNet personnel.
- FirstNet will tailor each site for customer-specific access lists and firewall rules.
- FirstNet will secure the platform against known security risks. Any observed security breaches or suspicious activity will be reported to the Customer.

3.1.2 **Customer Responsibilities -**

- Customer agrees that Customer shall utilize the service to engage only authorized servers and networks. Any attempt to utilize the service to access unauthorized servers or networks is strictly prohibited and may result in the termination of services.

- The Customer acknowledges that use of FirstNet equipment at their premises is at their own risk and is responsible for insuring such equipment against loss or damage.
- Customer will designate at least one primary and one back up technical resource (the "Customer Firewall Technical Contact") authorized to execute the following responsibilities:
- The Customer Firewall Technical Contact(s) will submit Firewall requests to set up, change or remove access control lists and firewall rules for their firewall instance by submitting a request to the FirstNet support Center.
- The Customer Firewall Contact(s) will be the "central point of contact" for administration of the perimeter firewall by FirstNet staff in a delegated administration model.
- The Customer Firewall Contact(s) will report all Firewall Service problems to the FirstNet Help Desk Support number.
- FirstNEt will provide telephone support for the initial setup, installation, configuration and maintenance in collaboration with the Customer Firewall Technical Contact.

4. Special Terms -

4.1 Device set up

FirstNet shall create virtual segmentation / virtual domain (VDOM) based on management or functional requirements per each firewall context.

4.2 Firewall VDOM management

FirstNet shall build each VDOM with a base rule set including High Availability modes (FGCP / ELBC).

4.3 Network address translation

This Service Level Agreement does include support for network address translation provided by FirstNet to support a customers use of private address space under IETF RFC 1918.

The Customer Firewall Technical Contact(s) will provide all NAT requirements to set up change or remove configuration entries, working directly with the FirstNet Security Perimeter Group.

The Customer Firewall Contact(s) will be the "central point of contact" for Network Address Translation (NAT) additions, rearrangements or changes.

5. Security –

5.1 Customer agrees to review with FirstNet the customer's architecture, including any and all changes to the architecture that could compromise the security of FirstNet's systems or network.

5.2 Customer accepts sole accountability for all use of the service by customer's systems and users. Customer further agrees to assume full responsibility for restricting access to servers by policy, rules, filters and/or other reasonable methods including agreements with contractors or other third parties.

5.3 The filtering shall be documented showing the real Customer address (es), the address (es) of the server(s) and the services (telnet, FTP, WWW, etc) allowed. In so doing, Customer agrees to comply with all applicable IT Security Policy and Standards and shall ensure that each staff member or contractor complies with all the conditions set forth herein.

5.4 Customer acknowledges and accepts FirstNet's right to suspend service without prior notice upon detection, confirmation, or notification of any unauthorized access, malicious traffic caused by infection or abuse deemed harmful to the FirstNet Network. If unauthorized access, malicious traffic caused by infection or abuse occurs, FirstNet and the customer will attempt to resolve security issues to the satisfaction of FirstNet and the customer. If no satisfactory resolution of security issues is identified, FirstNet reserves the right to terminate the service to the customer.

5.5 FirstNet provides a security system infrastructure that reasonably protects its customers from unauthorized external access to or broadcast on the Internet of the customer's intellectual property, proprietary and confidential data.

5.6 In the event that FirstNet becomes aware of a breach of the security of the system involving personal information maintained but not owned by FirstNet, FirstNet shall immediately notify the agency that owns the information. Breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Personal information is a person's first name or first initial and last name plus any of the following:

ID number; or

Driver's license number or;

Account number or credit or debit card number, and a code or password if a code or password is required to obtain access to the account or use the credit or debit card.

6. Firewall Disclaimer -

6.1 This FirstNet service is designed to prevent outsiders from gaining access and will provide an effective method of monitoring and limiting access. However, it may not prevent some instances of dedicated hackers, or an employee from gaining unauthorized access to the Internet or to confidential information stored on the network. FirstNet does not and will not accept liability for any losses or damage to

Customer's business or data that arise as a result of the Firewall not preventing unauthorized access.

6.2 The FirstNet service does provide a high standard of protection and service, but no system can claim to be completely secure.

7. Exclusions -

FirstNet does not support the following services. The following items are the sole responsibility of the Customer:

- Implementation and management of Customer LAN environment (i.e., switches, mobile devices, servers, workstations, etc.).
- Help desk support for client devices and applications.
- Internet Access is not provided pursuant to this agreement.
- Remote Client Internet access.
- Data encryption within the Network.
- Protocols other than IP (Internet Protocol).