Terms of Service
MANAGED FIREWALL Service

This Service is subject to and governed by Customer's separate signed master services agreement with CTS. This Agreement is entered into between you and CTS for the provision of CTS' Managed Firewall Services. For the purposes of this agreement "you" and "Customer" are used interchangeability and mean the entity to which CTS is providing service.

A. Service Description

Managed Firewalls protect your network from unauthorized access and malicious attacks. Firewalls are the critical gateway into a network, and firewalls managed by CTS come with the highest degree of attention and expertise to protect critical agency assets and provide protection at the agency perimeter.

Managed Firewall services are available in two categories:

- **Managed Firewalls** - are a fully managed firewall solution, including policy and configuration. The service is tailored to meet the customer's changing business requirements.
- **Delegated Administration** - is a solution for agencies that want their technical staff to maintain an active role in the administration of the agency perimeter firewall.

The Managed Firewall service will provide your agency with a CTS monitored, administered, and managed firewall. The service provides a firewall management solution for agencies that choose to take advantage of a CTS provided agency firewall that can either be managed by CTS technical staff or by agency technical staff The CTS services provides virtual firewall technologies attached to the State Government Network ("SGN").

B. Availability

CTS will use best efforts to have the service available 24-hours, 7-days a week.

C. Charges

Charges for firewall services are set forth below. The pricing is the same for both the delegated administration and the managed model.

Description	**Fee**
Managed Firewall for agencies that are included in the monthly Security allocation	$-0-/mo.
Managed Firewall for agencies/organizations not included in the monthly Security Allocation	$1,500/mo.
Managed Shared Firewall for small agencies with three (3) or less servers not included in the monthly Security Allocation	$150/mo.
No set up fee.	

Terms of Service
MANAGED FIREWALL Service

D. Responsibilities

CTS 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.

A. CTS Responsibilities

i. The service will be available 24-hours, 7-days-a-week.
ii. Management and configuration access is only granted to authorized CTS personnel.
iii. Tailor each site for customer-specific access lists and firewall rules.
iv. CTS will secure the platform against known security risks. Any observed security breaches or suspicious activity will be reported to the Customer.
v. Complies with State of Washington OCIO IT Security Policy and Standards.

B. Customer Responsibilities

i. Customer agrees to comply with Washington State OCIO IT Security Policy and Standards located at http://www.wa.gov/CTS/portfolio/itsecuritypolicy.htm at all times.
ii. 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.
iii. 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 agency by submitting a request to the CTS Service Desk.
    - The Customer Firewall Contact(s) will be the "central point of contact" for administration of the agency's perimeter firewall by agency staff in a delegated administration model. .
    - The Customer Firewall Contact(s) will report all Firewall Service problems to the CTS Help Desk Support telephone number (360) 753-2454 or 1-888-241-7597.
    - CTS will provide telephone support for the initial setup, installation, configuration and maintenance in collaboration with the Customer Firewall Technical Contact.

E. Special Terms

1. **DEVICE SET UP**
   CTS shall create Virtual Segmentation / Virtual Domain (VDOM) based on management or functional requirements per each firewall context

2. **FIREWALL VDOM MANAGEMENT**

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

3. NETWORK ADDRESS TRANSLATION

This Service Level Agreement does include support for network address translation provided by CTS to support agency 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 CTS Security Perimeter Group.
- The Customer Firewall Contact(s) will be the "central point of contact" for Network Address Translation (NAT) additions, rearrangements or changes.

4. SECURITY

Customer agrees to review with CTS the Customer's architecture, including any and all changes to the architecture that could compromise the security of CTS' systems or the State Government Network.

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 State servers by policy, rules, filters and/or other reasonable methods including agreements with contractors or other third parties. The filtering shall be documented showing the real Customer address (es), the address (es) of the State server(s) and the services (telnet, FTP, WWW, etc) allowed. In so doing, Customer agrees to comply with all applicable Washington State IT Security Policy and Standards and shall ensure that each and every Contractor or third party complies with all the conditions set forth herein as well as the applicable Washington State IT Security Policies and Standards.

Customer acknowledges that the State of Washington Auditor's Office may audit and/or inspect remote clients and/or servers accessed via the Service without any advance notice.

Customer acknowledges and accepts CTS' 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 State Government Network. If unauthorized access, malicious traffic caused by infection or abuse occurs, CTS and customer will attempt to resolve security issues to the satisfaction of CTS and customer. If no satisfactory resolution of security issues is identified, CTS reserves the right to terminate Service to Customer.

CTS 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. In the event that CTS becomes aware of a breach of the security of the system involving personal information maintained but not owned by CTS, CTS 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:

- Social security number; or
- Driver's license number or WA ID card 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.

5. FIREWALL DISCLAIMER

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

6. EXCLUSIONS

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

i. User support outside the State Network (supporting only access to systems within the State Network).
ii. Implementation and management of Customer LAN environment (i.e., firewalls, hubs, servers, workstations, etc.).
iii. Help desk support for client devices and applications.
iv. Internet Access is not provided pursuant to this agreement.
v. Remote Client Internet access.
vi. Data encryption within the State Network.
vii. Protocols other than IP (Internet Protocol).

7. FORTINET TERMS

CTS is providing this service to you based on a product we license from Fortinet. The following special terms are quoted from the contract CTS has with Fortinet:

A. Limitation on Use. You may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner; (c) except as provided in section 5, transfer assign or sublicense right to any other person or entity, or (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers.

B. Proprietary Rights. All rights, title, interest, and all copyrights to the Software and any copy made thereof by you and to any Product remain with Fortinet. You acknowledge that no title to the intellectual property in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific license as expressly set forth in section 1 ("License Grant") above.

Terms of Service
MANAGED FIREWALL Service

C. Term and Termination. Except for evaluation and beta licenses or other licenses where the term of the license is limited per the evaluation/beta or other agreement or in the ordering documents, the term of the license is for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet. The provisions of this Agreement, other than the license granted in section 1 ("License Grant"), shall survive termination.

D. Disclaimer of Other Warranties and Restrictions. EXCEPT FOR THE LIMITED WARRANTY BETWEEN CTS AND FORTINET, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

E. TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET, through its contract with CTS, CTS IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

F. EXPORT CONTROL LAW COMPLIANCE. You may not download, use, or otherwise export or re-export any Software associated with this TOS or any underlying information or technology except in full compliance with all United States and other applicable foreign laws and regulations. By using CTS, you represent and warrant that you are not located in, under the control of or a national or resident of any country on the U.S. Treasury Departments Specially Designated Nationals list or the U.S. Commerce Department Denied Persons List.