



Office of Information Technology Services

Service Level Agreement

Firewall & Virtual Private Network (VPN)

November 12, 2013 v2.1



Firewall & Virtual Private Network (VPN)

Service Description

The Firewall and VPN Service is a fully managed solution for customers interested in an additional layer of security for their network. This service manages all phases of a firewall and VPN security solution, including architectural validation, implementation, operations, and ongoing configuration management. This service provides access control and standards-based encryption technology as the foundation for secure, high-performance data communications. ITS network security analysts will provide consultation and recommend security best practices to aid in establishing the desired security policy to protect your data assets.

Service Commitments

The general areas of support (such as Incident and Change Management) applicable to every ITS service, are specified in the ITS Global Service Levels document.

Firewall and VPN Service Availability Targets:

- Target Service Availability is 99.9%

Hours of Availability

This service is available to customers 24 x 7 and adheres to the maintenance window schedule listed in the ITS Global Service Levels document.

ITS Responsibilities

- Service delivery occurs within 45-60 days upon successful completion of consultation and design activities; the requirement of an operational WAN connection at the site may delay service delivery
- ITS will conduct a design and consultation session with the customer
- ITS will configure and support the Firewall/VPN device installed at the customer premise
- ITS will maintain the installed Firewall/VPN device with the latest security patches and software releases, according to vendor recommendations
- ITS will store customer firewall logs and retain the logs for a period of 1 month
- 24 x 7 centralized monitoring and management via ITS Network-Security Operations and the ITS Service Desk



Customer Responsibilities

- Consents to pay the OSBM-approved rate for the term of this agreement. This agreement will be in effect for three years from the date service is declared operational. This agreement will be automatically renewed on a month-to-month basis thereafter.
- Perform a security vulnerability assessment and a risk analysis of own environment, prior to the initial consulting meeting.
- Complete the Firewall/VPN Implementation Checklist that will be used (together with a current diagram of customer's network) as input to the joint development of the initial security policy by ITS and the customer.
- Provide a secure physical facility with access control restrictions for the placement of the Firewall and VPN Service components, preferably co-located with the ITS provided WAN Service router. The secure facility requires customer coordinated 24 x 7 accessibility for authorized ITS staff.
- Provide ITS with a 24 x 7 Point Of Contact (POC) list for reporting and coordinating outages or emergency maintenance.
- This POC list will include the authorized contacts for security related issues, including the approval of the initial security policy and requesting policy changes.
- The POC will provide ITS with VPN group administrators who are responsible for assigning group membership to users.
- Implement remote access security policies that enforce the use of sound security practices to keep VPN client system(s) secure against unauthorized access and other security threats and that comply with the statewide information security standards.
- Contact the ITS Service Desk to report problems or request assistance.
- Work with ITS on a mutually agreed schedule to allow required maintenance services to be performed in a timely manner.

Service Level Agreement Scope

This agreement specifies only the standard operational service commitments and responsibilities of ITS and its customers. Customer-specific deviations from these commitments and responsibilities will be specified in an accompanying Memorandum of Understanding. Service rates are outside the scope of this agreement and are specified in financial documents.



Signatures of Approval and Agreement Date

Customer Signatures

Agency Head or Designee:

Name	Title	Signature	Date

Agency Chief Financial Officer:

Name	Title	Signature	Date

ITS Signature

State Chief Information Officer:

Name	Title	Signature	Date
Chris Estes	State CIO		