State of Alaska

Office of Information Technology

Information Security Policies

Title:	Firewall Use	Effective:	7/1/2017
		Last Review:	7/1/2017
		Next Review:	Annually
Number:	ISP-179		
Version:	1.01	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To establish requirements for firewalls in the State of Alaska (SOA) wide area network (WAN) system and prohibit the Departments from implementation of firewalls without proper coordination with the State Security Office (SSO). All external facing SOA servers must be protected by firewalls in a Demilitarized Zone (DMZ) to ensure security of SOA internet and internal networks.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- SOA firewall requirements; and
- Department firewall requirements.

5.1. SOA Firewall Requirements

5.1.1 State Security Office (SSO) Ownership of All Firewalls

The SSO must retain ownership of all firewalls within the State's wide area network (WAN) and Departments, except for specific firewalls required by federal regulation, for which the SSO may provide an MOU for the management control or shared access of such firewalls.

5.1.2 Intrusion Detection System (IDS)/Intrusion Protection System (IPS) on Internal and External Interface

IDS/IPS solutions must be installed and operated on both the internal and external interfaces for all firewalls. Logging of all IDS/IPS solutions must be performed at the enterprise level and sent to the SSO's enterprise logging solutions. Departments must install department level logging and reporting solutions; the device must dual report to both Department and Enterprise level monitoring and reporting solutions.

5.1.3 Network Address Translation (NAT) & Port Address Translation (PAT)

SOA IP scheme must be used and NAT or PAT solutions are prohibited.

5.1.4 Firewalls Must Not Impede View, Operational Tools or Service of the SSO and ETS

No firewall will be deployed that adversely affects the SSO's solutions or proposed solutions for the management, monitoring, auditing, logging, or reporting within the SOA WAN or Local Area Network (LAN) environments. The SSO must evaluate all firewall requests on a case by case basis for adverse affects.

5.1.5 Firewalls Log to Enterprise Solutions

All firewalls within SOA environments must log to the SSO enterprise logging solutions. The SSO will provide Departments with the required information necessary to complete this requirement during the implementation phase of approved firewalls.

5.1.6 Firewalls Ensure Incorporation into Security Operation Center Services

All firewalls must be incorporated within the Enterprise Security Operation Center Services.

5.1.7 Firewalls Compliant with SOA Standards

All firewall solutions must be compliant with TMC or other SOA governance standards for hardware and software.

5.2. Department Firewall Requirements

5.2.1 Firewalls are Prohibited within Departments

Firewalls are prohibited within Departments local area network (LAN) environments. Firewalls may be deployed within a Department main data center environment, in compliance with SOA policies. For Departments to purchase or deploy a firewall within their department, written authorization from the TMC and the SSO is required. Requestors are required to provide a business justification for all requests.

5.2.2 Department Firewall Requests

No firewall solution requests will be accepted for the purposes of, or which have the affect of, performing isolation within the State's combined network infrastructure (WAN/LAN environments). Departments can ONLY obtain data center firewalls. LAN or Host based requests will NOT be authorized or accepted.

5.2.3 Department Firewall Costs

Departments assume all costs for the operation and management of the entire infrastructure that is used to support a department firewall. These costs must include all equipment, licensing, network bandwidth and systems utilization, managing, maintenance, monitoring, reporting, logging and training costs at a minimum. Full burden costs will be developed by the SSO, once a solution request has been initially approved by the TMC.