



Firewall Security Standard

Introduction

In an effort to streamline firewall management operations, leverage volume purchasing discounts and take advantage of available technological interoperability advancements, OMES Information Services is standardized on a single firewall equipment vendor to securely control access to all networking segments, rather than attempting to support a multi-vendor solution.

Purpose

This document formalizes the OMES firewall team's decision to standardize on a single firewall security platform.

Standard

The designated firewall equipment vendor is Palo Alto Networks.

Platforms and models are individually selected based on their availability and the identified requirements of the project at hand. No device platforms or models are exclusively reserved for use only within a specific environment. Firewall policies must follow the OMES Change Management process for assessment and approval of the scheduled implementation. Security approval is provided by Oklahoma Cyber Command.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 03/05/2022	Review cycle: Annual
Last revised: 03/05/2022	Last reviewed: 08/08/2023
Approved by: Joe McIntosh, Chief Information Officer	