Application Delivery Controller Standard

Introduction
Application Delivery Controllers are critical tools in proxying and load balancing Internet-sourced traffic. ADCs receive traffic requests from the Internet and distribute those requests to an appropriate server relative to the user's geolocation or reject traffic requests that present an identifiable security risk. To streamline network operations and support and take advantage of available technological interoperability advancements, OMES Information Services utilizes specific ADC platforms depending on physical network and cloud requirements.

Purpose
This document formalizes the OMES network team's decision to standardize the application delivery controller platforms for physical networks and cloud environments.

Definitions
ADC – application delivery controller.

OEM – original equipment manufacturer.

Standard
The designated OEM for on-premises deployments is F5, and the designated ADC platform is BIG-IP.

The designated OEM for private and hybrid virtual cloud environments is VMware, and the designated ADC platform is VMware AVI or NSX Advanced Load Balancer.

The designated ADC for Microsoft Azure is Application Gateway or Network Load Balancer.

The designated ADC for Google Cloud Platform is Application Load Balancer or Proxy Network Load Balancer.

The designated ADC for Amazon Web Services is Application Load Balancer or Network Load Balancer.

Primary functions include, but are not limited to, the following:
- Full reverse proxy.
- Traffic load balancing.
- Global DNS.
- Web application firewall.
- SSL offloading.
- Centralized certificate endpoint and management.
- Identity and access management.
- Web policy enforcement.

Platforms and models are individually selected based upon availability and the identified requirements of the enterprise-wide environment, associated projects or specific agencies. No device platforms or models by the OEM are exclusively reserved for use only within a specific environment.

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: 04/12/2022	**Review cycle:** Annual
Last revised: 02/09/2026	**Last reviewed:** 02/09/2026
Approved by: Dan Cronin, Chief Information Officer	