



International Network Traffic Blocking Standard

Introduction

The State of Oklahoma utilizes an established filtering process that identifies and blocks potential cyberattacks while permitting the flow of legitimate network traffic. The state defines the type and nature of network traffic, which is allowed or denied, to help maintain the stability and security of state data and systems.

Purpose

This document establishes the standard for international network traffic to help protect state information asset availability, confidentiality and integrity from outside intrusion and hacking activities.

Standard

The State of Oklahoma prohibits traffic to and from countries on the State Sponsors of Terrorism list. OMES IS reserves the right to prohibit additional countries based on available threat intelligence.

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 ensure efficient, secure, and cost-effective delivery of essential public services, all state agency IT purchases and projects must receive central approval. This allows the Chief Information Officer to evaluate agency needs and capabilities, strengthen data protection and security, and streamline and consolidate systems to reduce costs for taxpayers.

References

- [State Sponsors of Terrorism](#).

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 10/28/2026	Review cycle: Annual
Last revised: 10/28/2026	Last reviewed: 10/28/2026
Approved by: Dan Cronin, Chief Information Officer	