OKLAHOMA
Office of Management
& Enterprise Services

International Travel Standard

Introduction

Traveling with technology presents concerns and challenges. When travel involves crossing an international border, concerns center on securing data and devices and safeguarding the integrity of state systems and networks. International travel increases the risk that sensitive data may be exposed, or the device in use may become infected with malicious software. The risk is especially high when a foreign government operates and manages internet connectivity, or the device is out of the traveler's control.

Purpose

This document provides the minimum requirements for safeguarding State of Oklahoma information systems for all employees and contractors while traveling outside of the United States.

Definitions

State device – Any state-owned assets including general storage devices, PCs, laptops/notebooks, mobile devices, tablets and any other devices used to store or access state data or infrastructure.

Standard

Traveling internationally involves special consideration to reduce the risk of theft of state assets and/or data. To this end, OMES discourages international travel with state devices. OMES prohibits international travel with state assets to countries on the US Department of State Travel Advisory List for level three and above and also prohibits access to state systems and networks while visiting those countries.

When international travel is required to countries classified as level two and below, the approving manager must notify Oklahoma Cyber Command ten business days prior to the travel date to ensure appropriate security measures are in place. Oklahoma Cyber Command monitors all international connections into state infrastructure and will terminate any international connection that is not pre-approved.

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.

References

- US Department of State Travel Advisory List.
- Partnering with Information Services.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 01/31/2022	**Review cycle:** Annual
Last revised: 01/31/2022	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	