OKLAHOMA
Office of Management
& Enterprise Services

Kiosk Workstation Security Standard

Introduction

The State of Oklahoma utilizes kiosk workstations for generally shared devices that require easy accessibility by state users or private citizens. Kiosk workstations must adhere to State of Oklahoma standards and policies to ensure a safe computing environment.

Purpose

The document establishes minimum requirements for kiosk devices.

Definitions

Kiosk – A specialized, specific use workstation designed to provide a service to multiple users, displaying information or utilization by private citizens.

Standard

Kiosk workstations must adhere to the following security requirements:

- When kiosk mode is required, the approving manager shall notify Oklahoma Cyber Command to ensure appropriate security measures are in place.
- State records and any regulated or sensitive data must not be downloaded or stored on devices in kiosk mode.
- Regulated or sensitive data, electronic or paper, must not be left in an accessible location to prevent unauthorized viewing and must be secured when unattended.
- All kiosk mode devices connecting to state information, accessing state data or state records must comply with state security policies and standards.
- All kiosk mode devices must have all applicable security software installed, kept up-to-date and currently enabled.
- Full disk encryption must be enabled for increased protection of the device.
- Systems must be segmented on the network and not intermingled with other systems.
- All kiosks must have appropriate physical security measures in place to protect against theft, manipulation and unauthorized access.

State agencies that provide kiosk workstations are required to take measures to reduce risk to kiosk users, state systems and networks. Failure to meet these requirements will result in immediate suspension of network access. Restoration of access will be at the sole discretion of the state CIO or state CISO.

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

- Network Acceptable Use Standard.
- System Acceptable Use Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/26/2022	**Review cycle:** Annual
Last revised: 10/21/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	