OKLAHOMA
Office of Management
& Enterprise Services

Mobile Device Platform Standard

Introduction

OMES Information Services takes all necessary measures to ensure the security and acceptable performance of the State of Oklahoma mobile device network. This standard defines the criteria for accessing state information assets from mobile devices. Any mobile device connecting to state information assets must comply with this standard, regardless of whether the device is personal or state-issued.

Purpose

This document establishes guidance for mobile technology management of state-issued and personal-owned mobile devices.

Definitions

Mobile device management – The software and service provided device management, security and monitoring in order for the smart device to be eligible to connect to the state network.

Mobile device – For the purpose of this standard, a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection; (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with self-contained power source.

Microsoft Intune – Cloud-based, endpoint management solution. It manages user access to organizational resources and simplifies app and device management across many devices, including mobile devices, desktop computers and virtual endpoints.

Standard

The state standard for mobile device management is Microsoft Intune.

To mitigate security threats, OMES has established minimum hardware and software requirements for state-issued mobile devices. The mobile device standard for the State of Oklahoma is Apple iOS devices. Apple iOS devices are the only mobile devices authorized to authenticate to the state network and access resources. Any authorized device authenticating to the state network must be running an iOS version for which Apple still offers standardized technical support. In addition, all mobile device hardware must be within two major releases and must be purchased from a service provider listed on the statewide contract.

To mitigate many of the risks associated with using mobile devices, OMES IS utilizes a mobile device management solution to manage a device’s authorized access to state network, systems and other enterprise resources. All state mobile devices used to access, transmit or store state data are required to have the state MDM product, Microsoft Intune, installed. In addition, users may not take steps to circumvent the security policies put in place by the MDM software.

Any exceptions to the above require annual state CIO approval.

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

1. Statewide Mobile Device Contract – SW1012.
2. OMES Personal Device Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/16/2021	Review cycle: Annual
Last revised: 10/04/2023	Last reviewed date: 10/04/2023
Approved by: Joe McIntosh, Chief Information Officer	