State of Oklahoma 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 provide 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 is 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, nonremovable data storage; and (iv) is powered-on for extended periods of time with self-contained power source.

Approved mobile devices
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 SW2012.

Mobile device management
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 mobile devices used to access, transmit or store state data are required have the state MDM product installed. If using a personal device, the employee is required to allow OMES IS to install the state MDM product on their device prior to accessing state email or systems or conducting state business. In addition, users may not take steps to circumvent the security policies put in place by the MDM software.

References
4. OMES Personal Device Standard.