Bring Your Own Device – Cell Phone Standard

Introduction
State employees are allowed and encouraged to use their own personal mobile devices for work-related tasks to promote user flexibility and convenience while enhancing cost-effectiveness and maintaining security and productivity.

Purpose
This standard identifies the guidelines to be followed by all state employees who use their own personal cell phone device for work-related tasks and accessing state resources. These guidelines and security measures are set in place to safeguard sensitive state information while allowing employees the freedom to use their preferred devices for work.

All employees eligible for and participating in BYOD must adhere to this standard.

Definitions
BYOD – Bring your own device. A state employee using their personal mobile device for work-related tasks and accessing state resources.

Standard
BYOD options.

- Managed application – This method allows state employees with Apple or Android devices to utilize their personal phone or tablet, without the need to have it managed by OMES. State applications can be installed from the Apple Store with an Apple ID or from the Google Play Store with a Google account. Applications such as Microsoft Outlook and Microsoft Teams can be installed for state use. Once the app is installed, you will login to the application with your state credentials and OMES will manage only that application. Users can uninstall the application to be removed from OMES management.
- Dual sim – This method allows state employees with personal devices to have a second, state-issued SIM card added to their personal device. This separates work-related phone calls and text messages from your personal calls and texts. Users can then use the managed application method to add state-managed applications.
    - The dual sim method requires senior director approval and is for First Net users only.

Device requirement – The minimum OS for IOS is 17.1.2 and for android is version 10.

Data protection – Any lost or stolen device must be reported within 24 hours to the OMES Cyber Command at 405-522-5069.

Security measures – The use of strict passwords or biometric authentication is mandatory.

Support and maintenance.

- Employees are responsible for the maintenance and repair of their devices.
- OMES IS support is available for state-owned application issues only. OMES IS support cannot be provided for personal devices.

Employee responsibilities.

- Acknowledgement of understanding and adherence to BYOD standards.
- Prompt reporting of any security concerns to OMES Service Desk at 405-521-2444.
- Maintaining minimum operating system.

Non-compliance consequences – Violations may result in disciplinary action, including revocation of BYOD privileges.

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

- OMES Mobile Device Management.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 03/29/2024	**Review cycle:** Annual
Last revised: 03/29/2024	**Last reviewed:** 03/29/2024
Approved by: Joe McIntosh, Chief Information Officer	