STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

STANDARD 638S2: Mobile Device Use

VERSION NUMBER	Standard 638S2-01
VERSION DATE	August 10, 2018
STANDARD TITLE	Mobile Device Use
GOVERNING POLICY	This standard is governed by Policy 638: Mobile Device Access Control, regardless of revision.
OBJECTIVE	This standard establishes the usage requirements and responsibilities of mobile device users accessing State of Alabama (hereinafter *state*) information technology (IT) resources (state data and information systems, including email).
REQUIREMENTS	Any state employee or contract personnel wishing to access state IT resources on a mobile device must activate the device in an enterprise mobility management system administered by the host agency or the Office of Information Technology (OIT).

1. Minimum Device Requirements:
   - 1.1. Android mobile device, version: 4.0 or newer
   - 1.2. iOS mobile device, version: 8.0 or newer
   - 1.3. Device must not be jailbroken or rooted

2. Mobile device users should be aware that activation of mobile device management (MDM) enforces the following device behaviors:
   - 2.1. All state data on the device will be encrypted.
   - 2.2. A passcode or PIN will be required to unlock the device after two minutes of inactivity.
   - 2.3. Managed applications will be encrypted and sandboxed from other non-managed applications. This sandboxing will permit or deny the following actions:
     - 2.3.1. Cut, Copy, and Paste operations will be allowed from non-managed applications to managed applications.

2.3.2. A Cut and Copy command from a managed application will only allow the clipboard contents to be pasted into another managed application.

2.4. Non-managed applications such as Facebook will not be allowed to contact a managed application such as Outlook.

2.5. State data can only be saved to state-approved cloud storage.

2.6. After 10 consecutive failed unlock attempts, the device will no longer be authorized.

2.7. After 90 days of inactivity, the device will no longer be authorized.

2.8. The MDM application may require that Microsoft Outlook be used to access state email. Third-party and device-native email applications may not be permitted. See section 3.3.

3. Mobile Device User Requirements:

3.1. Authorized Use: Use of mobile devices to access state IT resources is allowed when authorized by the employing agency of the device user (includes state employees or contract personnel on a state-issued contract).

3.2. Mobile devices shall be secured using containerization software that keeps state applications and data separate from personal applications and data and allows use of the personal applications and data even when the state container is secured. Personal data should not be at risk.

3.3. If the device owner desires or requires use of an application that cannot be containerized, then the entire device must be containerized. Under this condition, the user will not be able to use the device if it were locked down by the device management application and wiping the device will likely remove state and personal data.

3.4. The device user is responsible for any cost(s) associated with a personally-owned mobile device for additional data usage, or for the installation of applications not provided by the host agency but deemed necessary by the agency to ensure device and data security.

3.5. The user must keep the device locator functions turned on and security settings configured as specified by the MDM administrator, making no changes to any agency-configured security settings without prior agency approval.

3.6. The user shall use only vendor-supported operating systems (OS) on the mobile device and shall update the mobile device OS and security software when updates are provided by the vendor or by the MDM host agency.

3.7. The user shall immediately report to the agency's MDM administrator the loss, theft, or suspected compromise of a mobile device, and assist the agency in any resulting investigation.

3.8. Mobile device users shall:

3.8.1. Restrict access to their mobile device to only themselves and other authorized individuals

3.8.2. Not disclose mobile device logon information to unauthorized individuals

3.8.3. Remove all state data and state applications prior to disposal of a mobile device

4. No Expectation of Privacy: Mobile device users are hereby informed that MDM administration personnel may access personal information incidental to an investigation or during resolution of a device technical issue. All reasonable efforts will be made to limit any access to personal information.

5. Release from Liability: The state shall not be held liable for damage, loss of use, or loss of personal data on an employee's mobile device.

SUPPORTING DOCUMENTS

The following documents support this standard:

- Policy 638: Mobile Device Access Control
- Standard 638S1: Mobile Device Management

EFFECTIVE DATE

This standard shall be effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES

This is the initial standard and does not supersede a previous version.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this standard to be adopted as of the 28 day of August, 2018.

Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
638S2-01	08/10/2018	Initial version