STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

STANDARD 638S1: Mobile Device Management

VERSION NUMBER	Standard 638S1-01
VERSION DATE	August 10, 2018
STANDARD TITLE	Mobile Device Management
GOVERNING POLICY	This standard is governed by Policy 638: Mobile Device Access Control, regardless of revision.
OBJECTIVE	The objective of this standard is to state the technical and configuration requirements of mobile devices for access to 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 Requirements:
   - 1.1. A state user account and email address
   - 1.2. Approved authorization for using a mobile device for state business purposes
   - 1.3. Android mobile device, version: 4.0 or newer
   - 1.4. iOS mobile device, version: 8.0 or newer
   - 1.5. Device must not be jailbroken or rooted

2. Enterprise Mobile Device Management (MDM) system activation shall enforce 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. If the device owner desires or requires use of an application that cannot be containerized, then the entire device must be containerized.

SUPPORTING DOCUMENTS	The following documents support this standard: • Policy 638: Mobile Device Access Control • Standard 638S2: Mobile Device Use
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
638S1-01	08/10/2018	Initial version