



KAY IVEY
Governor

STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



JIM PURCELL
Acting Secretary

POLICY 638: Mobile Device Access Control

VERSION NUMBER	Policy 638-01
VERSION DATE	August 10, 2018
POLICY	Mobile Device Access Control
OBJECTIVE	<p>The objective of the Mobile Device Access Control policy is to establish governance for the use of mobile devices for authorized personnel conducting official state business, protecting the State of Alabama information technology (IT) resources and data from corruption or loss, and preventing unauthorized access or use of mobile devices.</p>
AUTHORITY	<p>The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of IT by state agencies, and exceptions to such authority, are derived from:</p> <p><i>Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (Acts 2013-68 and 2017-282).</i></p> <p>Policies of the OIT are approved and signed by the Governor.</p>
APPLICABILITY	<p>The requirements and responsibilities defined in OIT policies apply to all departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as <i>agency</i> or <i>agencies</i>) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of state IT.</p> <p>This policy applies to personally-owned and state-owned mobile devices, defined as any portable computing device that:</p> <ul style="list-style-type: none">• Has a small form factor such that it can easily be carried by a single individual• Is designed to operate without a physical connection (e.g., wirelessly transmit or receive information)• Possesses local, non-removable or removable data storage• Includes a self-contained power source

Mobile devices may also include voice communication capabilities and on-board sensors that allow the devices to capture information or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets.

This policy does not apply to personally-owned or state-owned personal computers or laptops, nor shall it apply to e-readers (e.g. Kindle, Nook, etc.) that do not sync email or access state data. Applicability should be determined by the Senior Agency Information Security Officer (SAISO) based on an assessment of usage and risk. Applicability may also be determined by the State Chief Information Security Officer (CISO) or by the Secretary of Information Technology.

STATEMENT OF POLICY

It is the policy of the OIT that:

- a) Mobile devices may be used by employees of the state (including contractors) for access to state IT, if the users comply with the standards, terms, conditions, and procedures for use established by the OIT, and as may be amended from time to time, to protect those resources from corruption and unauthorized access and use. Such access shall constitute acceptance of the statements, terms, conditions, and procedures established by the OIT.
- b) Use of mobile devices shall comply with all applicable state and federal laws, regulations, and policies including, but not limited to those covering the following data types:
 - U.S. Health Information
 - U.S. Financial Information
 - U.S. Personally Identifiable Information

Applicable protections are based on the data type(s) the device may process, transmit, or store. It is therefore the responsibility of the data owner or owning agency to determine applicable security controls (in addition to those described in this policy).

- c) The following five requirements, at a minimum, shall be enforced to allow a mobile device to securely connect to any state IT resource, which includes applications, data stores, and any application (including email) that can be used to store, process, or transmit state data:
 - Screen lock feature on the mobile device must be enabled
 - Ability to remotely track the mobile device enabled
 - Ability to remotely erase state data from the mobile device

- FIPS 140-2 compliant encryption for data in transit and at rest on the mobile device
- Applications loaded on the mobile device that access state data are managed by a mobile device container solution

OIT
RESPONSIBILITIES

To support and enforce this policy and promulgate standards governing the management of mobile devices.

AGENCY
RESPONSIBILITIES

Agencies shall enforce this policy within the agency. One agency may host access to state IT for other agencies, in which case the hosting agency may share these responsibilities with the implementing agency.

An agency hosting its own email system, or otherwise not utilizing the OIT's email service, shall perform regular monitoring of email service, at their own prescribed intervals, to identify any unauthorized mobile device. Unauthorized mobile devices shall be immediately removed or quarantined until authorization is obtained.

An agency hosting its own email system, or otherwise not utilizing the OIT's email service, shall ensure that applications installed on a mobile device that access state data are managed by that agency's mobile device management solution.

Agencies shall establish and disseminate written procedures for handling violations of this policy.

USER
RESPONSIBILITIES

Users shall comply with mobile device use standards set forth by the OIT and by the individual's agency.

SUPPORTING
DOCUMENTS

The following documents support implementation of this policy:

- [Standard 638S1: Mobile Device Management](#)
- [Standard 638S2: Mobile Device Use](#)

EFFECTIVE DATE

This policy shall be effective upon its approval by the Secretary of Information Technology and the Governor of Alabama as evidenced by the signatures of the Secretary and Governor being affixed hereto.

SUPERSEDES

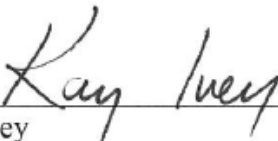
This policy supersedes OIT Policy 320: Use of POMD for State Business, which is hereby rescinded.

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 policy to be adopted as of the date on which the Governor has approved and signed it.



Jim Purcell
Acting Secretary of Information Technology

ORDERED



Kay Ivey
Governor

This 13 day of September, 2018.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
638-01	08/10/2018	Replaces OIT Policy 320: Use of POMD for State Business