STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

OIT Policy 320

Use of Personally Owned Mobile Devices for State Business

POLICY NUMBER	OIT Policy 320-01
VERSION DATE	June 24, 2016
POLICY TITLE	Use of Personally Owned Mobile Devices for State Business.
OBJECTIVE	Establish the governance for the use of Personally-Owned Mobile Devices (POMDs) by authorized personnel for state business while protecting State Information Technology (IT) resources from corruption and unauthorized access and use.
AUTHORITY	The authority of the Secretary of Information Technology to create and enforce policies relating to Information Technology is derived from the following legislation: *The Code of Alabama, Sections 41-28-1 through 41-28-8, (Act 2013-68)*
TERMS AND DEFINITIONS	The terms and definitions listed below will further clarify and explain the terminologies used in this policy.

- Centrally Managed – Managed by the Active Directory Forest owner.
- Container Solution – A software solution that has the ability to separate personal applications and data from State applications and data.
- Mobile Device – Any 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 (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained

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

- Personally Owned Mobile Device (POMD) – Any Mobile Device owned and used by a State of Alabama employee or contractor to conduct State of Alabama business / access the state network.

APPLICABILITY AND SCOPE

Personnel eligible to accrue overtime or compensatory time are NOT authorized to use their POMD to conduct state business outside of their normal work schedule without written authorization from their supervisor in advance. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls. Violation of this provision may result in disciplinary action, up to and including termination.

In addition, the requirements and responsibilities defined in this policy apply to all departments, agencies, offices, boards, commissions, bureaus, authorities, and authorized individuals in the employment of the state responsible for the management, operation, or use of State IT resources.

This policy shall not apply to counties, municipalities, the Alabama State Port Authority, or institutions of higher education governed by a separate board of trustees, unless these entities or institutions enter into cooperative agreements and/or contracts related to Information Technology efforts with the State, in which case they will be bound by this policy and the standards implementing its application and enforcement.

In addition, this policy shall not apply to the use of:

- State-Owned Devices
- Personally-Owned PCs, Desktops, Laptops, E-Readers, etc.
- Outlook Web Access

STATEMENT OF POLICY

It is the policy of the Office of Information Technology (OIT) that mobile devices which are personal property of individuals in the employment of the state (including contractors) may be used for

access to State IT resources, provided the user complies with the standards, terms and conditions and/or procedures for such use that are established by the Secretary of Information Technology, 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 Secretary of IT.

The usage of POMDs must comply with all applicable State and Federal laws, regulations, and policies including, but not limited to those covering the following:

- Health Insurance Portability and Accountability Act (HIPAA)
- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Criminal Justice Information (CJI)
- Federal Tax Information (FTI)
- Federal Educational Rights and Privacy Act (FERPA)
- Data protected by Code of Alabama, Alabama Administrative Code, or written agency policy.

The following requirements, at a minimum, must be enforced in order to allow a POMD to securely connect to any state email system and/or network:

1. Screen lock feature on the POMD must be enabled.
2. Ability to remotely track the POMD.
3. Maintain State data separate from personal data.
4. Ability to remotely wipe State data from the POMD.
5. FIPS 140-2 compliant encryption for data in transit and at rest on the POMD.

AGENCY RESPONSIBLITIES

The following are the responsibilities of each Agency for allowing use of a POMD by their personnel:

1. Enforce this Policy within the Agency. Note that one Agency may host access to State IT resources for other Agencies, in which case the hosting Agency may share these responsibilities

with the implementing Agency based upon mutual written agreement.

2. Perform regular monitoring of email service, at their own prescribed intervals, in order to identify any unauthorized POMD users.
3. Establish a written procedure for handling violations of the POMD Policy.
4. Ensure this policy is available to each Agency employee with access to State IT resources.
5. As part of the Agency's employee authorization process, obtain signed acknowledgement from each Agency employee who requests authorization to utilize their POMD, certifying that they have received, read, understand, and will comply with the policy. This acknowledgement shall be maintained in the employee's official department personnel file.
6. Within ten working days of the Effective Date of any amendment or addendum to this Policy, notify every Agency employee authorized to utilize POMD of the amendment or addendum,
7. An agency may decide to offer or not offer POMD access to State IT resources based upon operational needs, technical abilities, or other reasons. An agency wishing to offer POMD shall:
    a. Implement acceptable technical means and/or methods to allow a POMD to securely connect to State IT resources in accordance with:
        i. OIT Policy 320: Use of Personally Owned Mobile Devices for State Business
        ii. OIT Form 320F1: POMD User Agreement Form
    b. Establish a means for authorizing and tracking POMD usage, to include validating the POMD meets operating system and security setting software standards prior to activation.
    c. Document the level of POMD technical support capabilities, if any, within the Agency.
    d. At its discretion, cover the cost of additional data usage, or the installation of applications deemed necessary by the Agency to ensure security and POMD management.
    e. Use/deploy a Centrally-Managed Container Solution that meets all of the requirements as defined in this policy.

f. Ensure applications loaded on the POMD that access State data are managed by the Container Solution.

USER RESPONSIBLITIES

Specific User Responsibilities are defined in OIT Form 320F1 - Personally Owned Mobile Device User Agreement Form, and subject to the requirements of this policy.

IMPLEMENTATION AND ENFORCEMENT

The Office of Information Technology, under the authority of the Secretary of Information Technology, will promulgate standards governing the use of POMDs that support and enforce this Policy.

OIT shall:

(1) Identify categories of data requiring special security handling;

(2) Require an Agency that elects to permit use of POMDs by its employees to enforce this policy and every amendment thereto, to each person seeking authority to use, or using a POMD for State business; and

(3) Require that every person seeking authority to use or using a POMD for state business must provide written confirmation that the applicable Policy has been received and is understood, and provide a specific acknowledgment of the waiver of privacy for personal data residing on the POMD, and affirmatively agreeing to comply with the Standards. However, access shall also constitute acceptance.

SUPPORTING DOCUMENTS

The following document support this policy:

- OIT Form 320F1: Personally Owned Mobile Device User Agreement Form
- Policy 662S2: Client Systems Security

EFFECTIVE DATE

This Policy 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 policy 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 Policy to be adopted as of the 24th day of June 2016.

JOANNE E. HALE, Ph.D.
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Release Date	Comments
320-01	6/24/2016	Initial version