State of Alabama
Office of Information Technology

OIT Form 320F1
Personally Owned Mobile Device User Agreement Form

I. Authorized Use

At the discretion of their employing Agency, the use of POMDs to access State of Alabama IT resources is allowed for authorized State employees and contract personnel under a state-issued contract (collectively "User"), unless otherwise stated in OIT Policy 320: Use of POMD for State Business or in this form.

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.

II. Personal Responsibility

The following are the responsibilities of each individual User using a POMD to access State IT resources. The user agrees:

1. Allow and install state-approved and agency IT provider supported containerization software on their POMD before using device for state business purposes;
2. Any cost(s) associated with additional data usage, or the installation of applications deemed necessary by the Agency to ensure security and POMD management that are not covered by the Agency, are the responsibility of the individual User;
3. To promptly deliver the POMD, together with all passwords required to unlock the POMD and other information necessary to access State IT resources:
    a. When directed by the Agency for such purposes as may be deemed necessary for protecting State IT resources;
    b. Upon separation of service with the Agency for the purpose of wiping State data, deactivating State applications and any other action determined necessary to safeguard State IT resources;
4. Keep locator functions turned on, and security settings as specified in OIT Policy 320: Use of POMD for State Business;

5. Screen lock feature on the POMD must be enabled.
6. To use only vendor-supported operating systems (OS) on the POMD, and to update the POMD OS and security software when updates are provided by the vendor to keep POMD licenses and software at current vendor-supported version;
7. To immediately report to the hosting Agency the loss, upgrade, replacement, compromise, or theft of a POMD, and assist the Agency in any resulting investigation;
8. No changes shall be made to any agency-configured security settings without prior agency approval;
9. No modification of POMD functionality shall be made unless required or recommended by the hosting agency;
10. No device shall be utilized that is jail-broken, "rooted" or has been subjected to any other method of changing built-in protections;
11. To remove State data and State applications prior to disposal of POMD;
12. To follow the employee or contractor Agency's policies regarding POMD utilization if they are more restrictive or provide additional requirements; and
13. To consent to remote "wipe" of data, de-activation of State application or any other action necessary to protect State resources, including action which may result in loss of personal data.

III. Security

User agrees to protect State IT resources from corruption or unauthorized access, to include, but is not limited to, the following:

Restricting use of the POMD to only themselves and those State IT resources specified in this policy.

Not divulging information that allows access to the POMD to anyone other than State IT resources specified in this policy.

Keeping State data containerized. POMD's can only use State approved containerization software. This software will keep state apps and data separate from personal data and allow the use of personal apps and data even if the state container is locked down. Personal data should not be at risk. The one exception is that if state mandated the use of an app that could not be containerized then the entire personal device must be containerized. Under these conditions the user would not be able to use their phone if it were locked down by the state and wiping the phone would remove state and personal data.

IV. Inappropriate Use

Inappropriate use of a POMD to access State of Alabama networks is defined in Policy 630: System Use.

V. No Expectation of Privacy

User grants a waiver of privacy to personal data on their POMD only to the extent necessary to resolve any security or technical issue. User understands support personnel may access personal information incidental to an investigation or technical issue.

VI. Release from Liability

By accessing State information and application through a POMD, User agrees and expressly releases the State from any and all liability damage or loss of use of an employee's POMD to include personal data or information on the POMD. User expressly releases and holds the State harmless.

VII. Consequences of Inappropriate Use

Any employee or contractor found to be in violation of the requirements of this agreement may face disciplinary action, up to and including termination. This action would, at a minimum, include termination of the agreement allowing the individual to access State IT resources on their POMD. In addition, they may also face Agency or State Personnel disciplinary action. In extreme cases, the employee or contractor could face criminal or civil action based on State and Federal laws regarding the care and use of PHI and PII data.

VIII. Authority

This User Agreement form is promulgated under the authority of the Secretary of Information Technology in accordance with the Code of Alabama, Sections 41-28-1 through 41-28-8, (Act 2013-68).

IX. Acknowledgment and Agreement

By signing this document, I am agreeing to abide by each point listed above, and that I have read and understand the Policy governing this agreement form. I further agree to uphold the highest standards in using my personal electronic device. I understand that by failing to abide by this agreement that I will be subject to the consequences as defined in this form, along with any further disciplinary actions which may include termination by the state.

Employee Name: _____

Email: _____

Employee Signature: _____ Date: _____

As Witnessed:

Witness Name: _____

Witness Signature: _____ Date: _____