Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Mobile Device Policy

1.0. Statement

1.1. The Office of Information Technology (OIT) takes all necessary measures to ensure the security, and acceptable performance, of the State network. This Policy defines the criteria for access to State Information Assets from mobile devices. Any mobile device that connects to State Information Assets must comply with this Policy, irrespective of whether such a device is personal or State-issued.

2.0. Definitions

2.1. *Bring Your Own Device* (*BYOD):* BYOD permits State personnel (both employees & contractors) to use personally owned mobile devices in the workplace, and to use those devices to access State Information Assets. This is subject to the approval of the Agency Management.

2.2. *Information Assets:* The full spectrum of all I.T. products, including business applications, system software, development tools, utilities, appliances, etc.

2.3. *Mobile Device Management (MDM):* The dedicated back-office application that provides the following functions for mobile devices: software distribution, policy compliance, inventory management, security management, service management, etc.

2.4. *Mobile Devices:* Computing and/or communication devices, running a mobile operating system (such as Google Android and Apple iOS), as opposed to a workstation operating system (such as Microsoft Windows, Mac OS, Ubuntu, etc.). Includes, but is not limited to, smartphones and tablets.

2.5. *Personally Identifiable Information (PII):* Information that can be used on its own, or in combination with other information, to identify, contact, or locate a single person, or to identify an individual in context. Refer to Paragraph 6 of Maine Public Law 10 MRSA § 1347[1] for a more detailed definition. PII includes, but is not limited to, Protected Health Information (PHI), Federal Tax Information (FTI), and Federal Education Rights and Privacy Act (FERPA) Information.

[1] http://www.mainelegislature.org/legis/statutes/10/title10sec1347.html

3.0. Applicability

3.1. This policy applies to:

3.1.1. Any mobile device connected to State Information Assets, irrespective of ownership. Registration with OIT is *mandatory* for any personal BYOD, or State-issued, mobile device that connects to State Information Assets. Registration is on a per-user, per device basis;

3.1.2. All State of Maine personnel, both employees and contractors;

3.1.3. Executive Branch Information Assets, irrespective of hosting location; and

3.1.4. Information Assets from other Maine State Government branches that use the State network.

4.0. Responsibilities

4.1. *Agency Management:*

4.1.1. Authorize requests to acquire, and connect, State-issued mobile devices to State Information Assets.

4.1.2. Authorize requests to connect personal BYOD mobile devices to State Information Assets.

4.1.3. Authorize Mobile Device Management support costs for mobile devices that are authorized by the Agency for business use. This includes the cost of all necessary product licenses for the mobile device.

4.1.4. Notify OIT Customer Support as soon as possible regarding any transition (transfers, terminations, etc.) of any mobile User.

4.1.5. Collect back any State-issued mobile device when it is no longer required for business use.

4.1.6. Provide reimbursements (if applicable) toward official use of personal BYOD mobile devices.

4.2. *User (Mobile Device Holder):*

4.2.1. Protect the mobile device from theft, damage, abuse, and unauthorized use.

4.2.2. Ensure that they remain the only one User of that mobile device.

4.2.3. Attest that they have read, and accepted, the terms and conditions of this Policy.

4.2.4. Exercise additional measure (see 5.8 below) should the mobile device store, even temporarily, *Personally Identifiable Information (PII),* or any other sensitive data.

4.2.5. Coordinate assistance from the wireless carrier, if necessary.

4.2.6. Ensure that no modification occurs to either the mobile device, or its operating system, that could potentially void the manufacturer's warranty, or alter the manufacturer's standard security configuration. This includes, but is not limited to, "jail breaking" an iOS device, or "rooting" an Android device.

4.2.7. Immediately notify OIT Customer Support of any lost, misplaced, or stolen mobile device that is registered with OIT.

4.3. *OIT Computing Infrastructure & Services:*

4.3.1. Owns, executes, and enforces this Policy.

4.3.2. Registers and manages State-issued and personal BYOD mobile devices that are authorized to connect to State Information Assets.
4.3.3. Install the MDM client on the mobile device.
4.3.4. Wipe (format), or lock, the mobile device in the event of a security issue. This includes, but is not limited to,
4.3.4.1. Wiping State data and applications from the device; and
4.3.4.2. Locking any device that exceeds the maximum number of consecutive, unsuccessful device-login attempts.

5.0. Directives

5.1. Supported mobile operating systems include currently-supported versions (by the original equipment manufacturer) of Google Android and Apple iOS.

5.2. Mobile devices must be locked through Pins. The Pin must have at least six (6) digits. The Pin may be non-expiring. For personal BYOD mobile devices, if the technology allows, the pure phone feature may remain unlocked.

5.3. Mobile devices must lock after a maximum of 15 minutes of inactivity. The Pin is necessary to unlock the mobile device.

5.4. After ten (10) consecutive, unsuccessful login attempts, the mobile device will be wiped (formatted).

5.5. For any mobile devices that is reported as lost, misplaced, or stolen, at a minimum, OIT will remotely uninstall any state-installed application. Upon specific request either by the User, or the Agency Management, OIT will also attempt to remotely wipe (format) the device.

5.6. All relevant State, Agency, and OIT policies, including FOAA for State contents (Title 1, Chapter 13)[2] and the Notice of Risk to Personal Data Act (Title 10, Chapter 210-B)[3], apply to the State contents on the mobile device, irrespective of whether the devices is State-issued, or personal BYOD.

5.7. Any mobile device used to access State Information Assets is subject to all State, Agency, and OIT Acceptable Usage, Security, and Privacy policies, irrespective of whether the devices is State-issued, or personal BYOD. Thus, for instance, even for a personal BYOD mobile device, the H.R. Directors and the Assistant Attorneys General may initiate forensic audits. Additionally, any application on any mobile device used to access State Information Assets may be quarantined (i.e., rendered inoperable) and/or banned (i.e., forcibly uninstalled).

[2] http://www.mainelegislature.org/legis/statutes/1/title1ch13sec0.html
[3] http://www.mainelegislature.org/legis/statutes/10/title10ch210-bsec0.html

5.8. Should the mobile device store, even temporarily, *Personally Identifiable Information (PII),* or any other sensitive data, the mobile device must be encrypted to the AES-256 strength.

5.8.1. Additionally, any mobile device that stores, even temporarily, either TLP: Amber or Red[4] data must be State of Maine-owned; and joined to the Enterprise Intune. The use of the approved Authenticator app for MFA to the State network on BYOD devices continues to remain approved.

5.9. For the purpose of access audit to State Information Assets, each mobile device must have one, and only one, designated user. As a pre-condition for the mobile device to access State Information Assets, the designated user *must* explicitly vouch that they do *not* share the mobile device with any other person (including family members).

5.10. Since OIT does not actually maintain the mobile devices, OIT's troubleshooting assistance can only be on a best-effort basis.

5.11. Should Agency policy, or statutory restrictions, prohibit particular agency stakeholders from accessing specific state Information Assets from non-state devices, then this policy does *not* modify that.

5.12. The State is held harmless for any damage resulting from a personal BYOD mobile device being used for State business.

5.13. Failure to comply with any of the above provisos may lead to the blacklisting of the mobile device, and/or the termination of the User's access to State Information Assets.

6.0. Document Information

6.1. Initial Issue Date: 24 October 2011
6.2. Latest Revision Date: 20 March 2024
6.3. Point of Contact: Enterprise.Architect@Maine.Gov
6.4. Approved By: Chief Information Officer, OIT
6.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[5]
6.6. Waiver Process: Waiver Policy[6]

[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[5] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf