Maryland DEPARTMENT OF INFORMATION TECHNOLOGY	Information Technology Policy and Standards	Approved: DocuSigned by: Michael G. Leahy 7820D075CBE64C5... Michael G. Leahy, Secretary — 09/22/2020 Date
# 20-12	***Mobile Device Management***	

Area(s): ☐ Process ☐ Procurement ☒ Security ☒ Hardware ☐ Web ☐ Facility ☒ End-User ☒ Software ☐ Network ☐ Data ☒ Voice ☐ Audit ☐ Other

Replaces Other Policy: ☐ No ☒ Yes: Maryland Mobile Device Security Policy, DoIT, June 2017

Purpose: Provide procedures for State agencies to use in managing mobile IT devices issued by the agency or provided by the employee, including technical settings, security controls, inventory, and financial elements.

Policy Statement: Utilization of mobile computing and communication devices by State agencies continues to increase, be incorporated into core mission processes, and be connected to State information technology (IT) systems. These devices include those provided to employees by DoIT, other State agencies, and BYOD units that the employees own and want to operate with State IT systems in a manner that may or may not qualify for State BYOD reimbursement programs. To provide the proper level of operational, security, asset management, and financial controls, DoIT has established a Mobile Device Management (MDM) Program that State agencies and employees must comply with to be approved to use mobile devices with State IT systems, be issued devices, or receive BYOD cost reimbursements.

Applicable Law & Other Policy: Annotated Code of Maryland, State Personnel and Pensions Article, Section 2-308, Code of Maryland Regulations, Title 17, Subtitle 04, Chapter 11, Section .02 B(1)(a). DBM, *Maryland State Telework Policy* (2019); Annotated Code of Maryland, State Personnel and Pensions Article, Section 2-308, Code of Maryland Regulations, Title 17, Subtitle 04, Chapter 11, Section .02 B(1)(a).

Scope and Responsibilities: All executive branch units of State government, except those identified in Maryland Code, SF&P § 3A-302. Agency executives, managers and staff shall ensure compliance with this policy, procedures, and standards when ordering, using, or returning mobile devices.

Key Terms:

Bring-Your-Own-Device (BYOD): A mobile device that is personally owned and is properly authorized to connect to State IT systems (voice, data, video).

Department of Information Technology (DoIT): An executive branch unit of Maryland state government, organized according to Maryland Code, State Finance and Procurement Article, § 3A.

Mobile Device: a portable and/or wearable hardware device that enables communication and/or computing capabilities, such as cell phones, tablet computers, smart watches, virtual reality goggles, and headsets.

Policy: A statement of jurisdiction and methods to guide agencies in the management of IT resources and services.

Specifications: See Attachment 1.

Policy Review: By the DoIT IT Policy Review Board annually or as needed.

Contact Information: Chair, IT Policy Review Board, doit-oea@maryland.gov 410-697-9724. The Policy #20-12 steward is the DoIT Director, End User Services.

Attachment 1

Mobile Device Management Procedures

Hardware: DoIT seeks to provide a standardized mobile device offering for the benefit of DoIT employees that will also be able to accommodate the varying needs of DoIT employees while avoiding excessive variability of hardware and cost. Device standards are based on suitability for state-wide use, performance, functionality, and ease of maintenance.

Procurement: To realize cost savings based on economies-of-scale for procurement, maintenance, and support, DoIT has standardized on preferred vendors. DoIT regularly reviews the hardware options from its preferred vendors and updates standard equipment standards to best leverage the latest technology and cost. These standards are available on the DoIT website at (URL).

Software: State-issued mobile devices are standardized on Android and Apple platforms. Smartphones, tablets, and other devices must run current, supported versions of the Android operating system or iOS.

Agency Responsibilities:

- Adhere to an Agency Policy that is consistent with the Statewide Policy to include:
  1. An official request by the employees Supervisor for each mobile device.
  2. Written, signed acknowledgement by the employee assigned the mobile device indicating awareness and acceptance with the provisions of the Statewide Policy and Agency Policy.
  3. Written approval for each device assignment by the agency head or designee.
- Ensure the cost-effective use of mobile devices.
- Require that state issued mobile devices be used primarily for State business.
- Maintaining an inventory of agency-issued mobile devices and accessories using DoIT inventory procedures.

Employee Responsibility for State-owned devices:

- State-issued equipment is to be used for the benefit of the Agency and that personal use shall be minimal.
- Abide by the state issued Acceptable Use policy.
- Always keep the device secure to avoid theft, loss or damage and to use reasonable care in its use
- The storage of confidential information on mobile devices is prohibited unless prior written approval has been granted by the Agency Secretary or delegated authority.
- Employee may not alter devices without specific written authorization from the Agency Secretary or delegated authority.
- Mobile devices shall not be “rooted” or have unauthorized software/firmware installed.
- Stolen, physically damaged, or lost equipment must be reported to the DoIT ServiceDesk in writing immediately if possible and no later than 24 hours following the date on which the employee discovers the theft, damage, or loss. The employee should include their full name, the make and model of the devices, carrier, and any other relevant information. If equipment is stolen, a police report must be initiated by the employee as soon as possible after the theft is discovered with a copy provided to DoIT.
- At the end of employment, the Employee shall return the equipment in good working order.

Employee Responsibility for Bring-Your-Own-Device (BYOD):

- Agencies and users will adhere to the DoIT IT Security “Rules of Behavior” available at (URL).
- Abide by the State-issued Acceptable Use policy.
- Keep device secure at all times to avoid theft, loss or damage and to use reasonable care in its use
- The storage of confidential information on mobile devices is prohibited unless prior written approval has been granted by the Agency Secretary or delegated authority.
- Employee may not alter devices without specific written authorization from the Agency Secretary or delegated authority. Mobile devices shall not be “rooted” or have unauthorized software or firmware installed.

- Stolen, physically damaged, or lost equipment must be reported to the DoIT ServiceDesk in writing immediately if possible and no later than 24 hours following the date on which the employee discovers the theft, damage, or loss so that it may be removed from DoIT's BYOD program. The employee should include their full name, the make and model of the devices, carrier, and any other relevant information.
- At the end of employment, the Employee shall produce the personal device for inspection. All state data on personal devices will be removed by IT upon termination of employment.