Mobile Device Security Policy

Policy Statement
The Maryland Department of Information Technology (DoIT) seeks to protect State of Maryland owned mobile devices from unauthorized access, use, alteration, modification, deletion, and/or destruction.

1.0 Purpose
This purpose of this policy is to prevent unauthorized disclosure of confidential information, reduce the risk of spreading viruses or malware, and to prevent unauthorized access to State owned computing and information infrastructure. Procedures must be developed to comply with the requirements set forth in this policy.

2.0 Scope
This security policy applies to any DoIT issued mobile device. Managers and supervisors are responsible for ensuring that users are aware of and understand this policy and all related procedures.

3.0 Policy
Built-in configuration settings and security features of DoIT issued mobile devices shall be standardized, documented and implemented.

All vendor recommended patches, hot-fixes or service packs must be installed prior to deployment and processes must be in place to keep system hardware, operating system and applications current based on vendor support recommendations (including patches, hot-fixes, and service packs).

Proper asset management procedures shall apply to all mobile devices.

Whenever possible, all mobile device application distribution and installation shall be centrally controlled and managed.

Whenever possible, all mobile device operating system and application security patch installation shall be centrally controlled and managed.

Mobile device options and applications that are not in use shall be disabled.

Whenever possible, Bluetooth settings should be configured to notify users of incoming connection requests and to receive confirmation before proceeding.

Whenever possible, all mobile devices must be password or PIN protected. Using the same password for a handheld device that is used for DoIT network access or access to other DoIT devices and applications is prohibited.

Whenever possible, all mobile devices should have timeout/locking features and device erase functions (including removable memory) enabled.

Whenever possible, all mobile devices should have anti-virus and/or firewall protection installed.

No confidential information shall be stored on mobile devices unless it is encrypted and permission is granted from the data owner.

Confidential information should be removed or sanitized from the mobile device before it is returned, exchanged or disposed of.

Whenever possible, mobile devices shall be scanned for viruses/malware before they can connect to DoIT systems.

The physical security DoIT issued mobile devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight. If a mobile device is lost or stolen, the employee is responsible for promptly reporting the incident to the DoIT Help Desk and proper authorities.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Confidential Information	Non-Public information that is deemed private, privileged or sensitive.
Private Information	Personally identifiable information (PII) that, if exposed, may cause harm to an individual. Harm, in this context, meaning any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality,
Privileged Information	Records protected from disclosure by the doctrine of executive privilege which may include but not limited to records: • Relating to budgetary and fiscal analyses, policy papers, and recommendations made by the Department or by any person working for the Department; • Provided by any other agency to the Department in the course of the Department's exercise of its responsibility to prepare and monitor the execution of the annual budget; • Relating to a State procurement when a final contract award has not been made or when disclosure of the record would adversely affect future procurement activity; • Of confidential advisory and deliberative communications relating to the preparation of management analysis projects conducted by the Department pursuant to State Finance and Procurement Article, §7-103, Annotated Code of Maryland.
Sensitive Information	Information that, if divulged, could compromise or endanger the citizens or assets of the State.