
# Maryland Mobile Device Security Policy

**Last Updated:** 06/02/2017

# Contents

## 1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of the Executive Branch of Maryland State government information technology (IT) networks, systems, applications, and data.

The State's use of mobile technology offers employees and contractors new options for work performance and environment, including location, but creates security challenges that include protecting the confidential information accessed by mobile devices. As mobile technology continues to advance, the State of Maryland will update its policies and processes to incorporate better standards and best practices to ensure data is protected from the latest threats. This policy utilizes the standards identified in NIST Special Publication (SP) 800-53AR4, SP 800-121, SP 800-124R1, and SP 800-114, as well as industry best-practices.

## 2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013), Section 10: Mobile Devices. This document also supersedes any policy regarding mobile device management or security declared prior to the 2017 Cybersecurity Program Policy, such as the DoIT Mobile Device Security Policy v1.0 (October 2011). This document will be reviewed annually and is subject to revision.

| Date | Revision | Policy Updates | Approved By: |
|---|---|---|---|
| 01/31/2017 | v1.0 | Approval of Draft | Maryland CISO |
| 06/02/2017 | v1.1 | Initial Publication | Maryland CISO |

## 3.0 Applicability and Audience

All Executive Branch agencies deploying or implementing mobile device solutions, either agency-owned or employee-owned, i.e., bring-your-own-device (**BYOD**), will ensure risks of data loss or compromise are mitigated in accordance with the requirements described in section 4.0 below.

## 4.0 Policy

Mobile devices offer opportunities to streamline agency functions and make employees more productive, but, as with any new technology, inherent vulnerabilities and the ease with which adversaries can exploit those vulnerabilities make implementing mobile solutions a significantly risky and challenging endeavor.

### 4.1 Mobile Device Definition

According to NIST, and for the purposes of this policy, mobile devices, have the following characteristics:

- **Small form factor**, i.e., relatively small size

- At least one wireless network interface, such as WiFi, cellular, or other technology, used to connect to other data networks
- Local built-in storage
- An operating system (OS) that is not a full-functioning desktop or laptop OS (though this may change as technology continues to evolve)
- Applications available from multiple sources, e.g., provided with the mobile device, available through an "app" store, downloaded via web browser or third-party installers

These devices are typically described as smartphones/iPhones, tablets/phablets/iPads, smartwatches, and personal data assistants (PDAs), and have one or more of the common, but optional, characteristics listed below:

- One or more wireless personal-area networks, such as Bluetooth or Near-Field Communications (NFC), as well as cellular and GPS services
- One or more digital cameras or video recording devices
- Microphone
- Support for removeable storage (e.g., micro-SD cards) and can be used as removeable storage by another computing device
- Built-in features for synchronizing data with different locations

The requirements described in the following sections will allow agencies to:

1) Identify and control how **confidential data** may be accessed by mobile devices
2) Ensure accountability through authentication controls
3) Ensure a **data loss prevention** (DLP) solution is in place to manage and track confidential information — this helps to identify the extent of a possible breach if the device is stolen or compromised
4) Utilize protective measures such as encryption or auto-wipe to prevent data loss or compromise

NOTE: If all four of these capabilities cannot be enabled, agencies should not deploy or allow mobile devices the ability to access to confidential data.

## 4.2 Mobile Device Implementation Plan

The DoIT Enterprise will develop a Mobile Device Implementation Plan to manage mobile device usage and to control data access through mobile devices. Non-Enterprise agencies are required to independently meet the requirements listed in the table below.

| # | Name | Requirement |
|---|---|---|
| A | Specify Data Access and Control Requirements | ▪ Identify what data or resources may be accessed by staff through mobile devices and determine which types of mobile devices will be permitted<br>▪ Determine what device management solution will provide the required access control and protections for the permitted devices |
| B | Determine Risk | Assess risks associated with mobile device access and identify mitigating controls to prevent or detect potential network compromise, such as network |

| # | Name | Requirement |
|---|---|---|
| | | credentials or data stored on the device, or potential data loss through the device connection. |
| C | Management Controls | Determine how the Agency will manage mobile devices, including access rules, device control procedures, and data management (which may also include asset allocation). Three models of mobile deployment are:<br>▪ Agency owned and issued to staff (see Appendix A)<br>▪ Agency owned and issued to staff but with personal use enabled, also referred to as "corporate owned, personally enabled" (**COPE**)<br>▪ Personally-owned devices (BYOD – sandboxed or unrestricted; see Appendix B) |
| D | Permitted Devices | Determine which devices and operating system versions will be authorized and managed through the device management solution (e.g., Apple iOS 9, Android 5.0). |
| E | Mobile Device Management (MDM) Software Solution | Implement Mobile Device Management (MDM) software that can track device configuration and can send device activity logs and data to the Enterprise **Security Operations Center** (SOC). The solution should manage:<br>▪ Cloud access and data synchronization<br>▪ Antivirus/anti-malware installation and maintenance<br>▪ Remote find and remote data-wipe<br>▪ Encryption support, for both data-in-motion and locally stored data-at-rest<br>▪ Device and network authentication controls (e.g., PIN, password, biometrics) |
| F | Data Loss Prevention | Ensure a DLP solution exists to monitor confidential data movement through mobile devices. This capability allows DoIT or an agency to identify whether users are downloading data and track the location of stored data (storage location may pose a risk of compromise or loss). |
| G | User Agreement and Acceptable Use | ▪ Ensure that users read and sign the Mobile Device and BYOD User Agreement (see Appendices A and B) and sign the *DoIT Acceptable Use Policy* before being granted access via any mobile device, either state-issued or a personal-owned device<br>▪ The Information System Security Manager (ISSM) will coordinate with Human Resources to ensure the agreement forms are kept on file |
| H | Monitoring & Compliance | Develop and implement a process to keep the DoIT SOC informed of mobile devices authorized to access State services and resources. |

## 4.3 Mobile Device Management Software

To mitigate many of the risks associated with using mobile devices, the DoIT Enterprise will utilize a mobile device management (MDM) solution to manage devices authorized to authenticate to the network and access resources. The MDM solution must enforce the controls listed in the table below and ensure all managed devices meet specified security configuration requirements.

| # | Name | Requirement |
|---|---|---|
| A | Determine Access Levels | Agencies will specify the level of access for each deployment model based on whether a device is agency-owned and issued or provided by the user (BYOD). |

| # | Name | Requirement |
|---|---|---|
| | | ▪ Agency-owned devices may be permitted broader access as they can have more rigorous security controls. |
| B | Endpoint Security | Ensure an endpoint security solution is implemented, including antivirus deployment and app verification. |
| C | Lock Security Settings | Lock or secure security settings so users cannot delete or change mandatory settings. |
| D | Password Strength | Enforce password complexity requirements per *DoIT Account Management Policy*, and use two-factor authentication or personal identification numbers (PIN). |
| E | Password Change Interval and History | Enforce the DoIT Account Management Policy regarding frequency of password changes and history requirements. |
| F | Device Lock Out | Configure devices to lock out access after a specified time with no activity or number of failed logon attempts. |
| G | Enable Auto Wipe | The MDM solution will manage devices so they automatically wipe (themselves) upon these conditions:<br>▪ After ten (10) unsuccessful password attempts<br>▪ After forty-five (45) days of non-communication with the management server |
| H | Disable Cloud Data Storage and Backup | The MDM will prevent agency data partitions (on a mobile device) from synchronizing to any personal or cloud storage area outside the Enterprise's control boundaries.<br>▪ Without this, users could "synchronize" State data to unauthorized devices or locations and expose confidential data, or accidentally sync personal user files to State storage systems, which may also result in data exposure or loss. |
| I | Enable Remote Wipe, Lock, and Locate | Enable remote locate, lock, and wipe functions for mobile devices in case the devices are lost, stolen, or denied authorized access; this functionality will help facilitate data protection and device recovery. |
| J | Enable Device Encryption | Encrypt data-at-rest, where technically feasible, with the appropriate encryption techniques.<br>Sandbox solutions or encrypted partitions can also add a layer of protection to data at rest. |
| K | Disable **Developer Debug Access** | Disable developer debug access to mitigate a common security-bypass technique. |
| L | Agency VPN Configuration and Monitoring | MDM solutions typically offer VPN options to allow user connections through an insecure network (e.g., coffee shop or airport WiFi) by creating an encrypted tunnel to State resources or services. This VPN connection should:<br>▪ Use certificates or other non-user-controllable authentication to prevent replication to an unauthorized mobile device, e.g., data download<br>▪ Monitor mobile devices accessing confidential resources |

## 4.4 Application Management

Whether agency-owned or BYOD, mobile applications (commonly called "apps") installed on mobile devices can be the most direct vector for introducing malware and compromising the

security of agency data and networks. The level of control over application installation will determine how much access the mobile device will be granted to network resources.

In the case of BYOD, where feasible, the MDM should establish a secure partition (called a "container") on personally-owned devices; this containerization allows the greatest (MDM) control over where data is stored and shields State data from impacts of users' management and use of their own devices.

For State issued devices, users will not have management access to the device and will be restricted or managed in their use of apps.

Agencies will manage mobile applications per the requirements below:

| # | Name | Requirement |
|---|---|---|
| A | Application Approval | Establish a formal process for requesting specific applications to be made available through the MDM. |
| B | Application Purchase Account | ▪ Prevent app purchases from agency-owned devices, including COPE deployments; restrict app "purchases" to acquisition from the MDM<br>▪ For BYOD, determine methods for compensating users for approved app purchases if the MDM solution cannot provide the requested app |
| C | Approved App Sources | Approved apps will be provided through the MDM solution. If the MDM solution cannot provide an app, then the device-sanctioned app store shall be used (e.g., iTunes, Google Play); apps from third party sources are prohibited. |
| D | Application Security | ▪ Establish and document mobile application whitelists, including native apps like camera or Bluetooth<br>▪ Identify security and data access risks associated with native apps and required business apps; for instance, allowing Bluetooth functionality may open an attack vector through an insecure data connection that allows a nearby adversary to steal data |
| E | Application Development | If agencies develop in-house applications, ensure formal, mobile app coding and testing standards are established and processes followed. |

## 4.5 Loss Reporting and Disposal

Mobile devices are at higher risk of loss or theft than workstations. Each agency should require that staff report loss or theft of an authorized mobile device immediately. Agencies must also establish processes and procedures to quickly respond to lost or stolen devices.

Disposal of State issued mobile devices creates a risk of potential data compromise; therefore, the Enterprise asset manager must coordinate with the Enterprise Information System Security Manager and ensure proper device sanitization to prevent unauthorized data recovery. Equipment disposal processes and procedures to complete this final stage of the equipment lifecycle will be documented and maintained by the ISSM.

BYOD users are also required to report loss or theft of their personally-owned devices immediately to ensure access is revoked for that device and security protections are enabled. Users planning to upgrade devices or transition to new carriers must bring old, authorized devices to the (State) authorizing official to ensure the device is sanitized and access is revoked.

## 4.6 Training and Awareness

The DoIT SOC will coordinate with the ISSM to provide cyber security training and awareness for mobile users (see *Auditing and Compliance Policy*). As part of the annual training and awareness campaign, users will be provided information on topics such as, but not limited to:

- Common security configurations (expected to be deployed on their devices)
- How to identify potential phishing attacks, like malicious text messages
- Common mobile attack vectors, such as WiFi, NFC, and Bluetooth attacks, and best prevention practices
- How to report any suspicious activity or loss of the mobile device

# 5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy, then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

# 6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy
- Account Management Policy
- Auditing and Compliance Policy
- Public and Confidential Information Policy

# 7.0 Definitions

| Term | Definition |
|---|---|
| **Bring Your Own Device (BYOD)** | The practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes. |
| **Confidential Data** | Confidential information is non-public information that, if disclosed, could result in a negative impact to the State of Maryland, its employees, or citizens and includes the following sub-categories:<br>▪ Personally Identifiable Information<br>▪ Privileged Information<br>▪ Sensitive Information<br>For more information on confidential information see *DoIT Public and Confidential Information Policy*. |
| **Corporate Owned, Personally Enabled (COPE)** | A practice in which an organization provides its employees with mobile computing devices and allows the employees to use them as if they were personally-owned notebook computers, tablets or smartphones. |

| Term | Definition |
|---|---|
| **Developer Debug Access** | A capability in mobile devices to enable debugging options in which users can change security and performance functionality on the device. This also allows users to "root" or "jailbreak" the device (removing the default security restrictions and essentially gaining root access). |
| **Data Loss Prevention (DLP)** | Process and capability of discovering data-in-transit and locating data-at-rest, discovering and tracking the movement of information, and blocking the export of information from a network. |
| **Security Operations Center (SOC)** | Continuous monitoring cell that collects system logs and network traffic information for security analysis and incident handling (see *Continuous Monitoring Policy*). |
| **Small Form Factor** | Term used to describe the physical dimensions of a computing device…small form factor being attributed to mobile technologies such as tablets and smartphones due to the smaller size in comparison to desktop and laptop computers. |

## 8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing the security of mobile devices and protecting the data accessed by them within the Enterprise. Agencies not directly managed by DoIT must comply with the requirements detailed in section 4.0 unless an agency has completed a Policy Exemption Request Form and received approval from DoIT. Agencies must manage mobile device security and ensure data is properly protected from breach or loss.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to comply within a reasonable time before the issue is reported to the Secretary of Information Technology. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any attempt to circumvent this management policy, such as intentionally bypassing mobile device management software, attempting to circumvent the device operating system (rooting or jailbreaking the device), or placing data at risk through negligent behavior will be considered a security violation and subject to disciplinary action which may include written notice, suspension, termination, and possible criminal and/or civil penalties.

# Appendix A: State-Issued Mobile Device User Agreement

After reviewing the User Responsibilities in Part I below, fill out parts II through V, and submit to your agency authorizer for mobile devices.

**Part I – User Responsibilities**

The user identified in Part II of this form (the recipient of the assigned device) hereby assumes responsibility to safeguard the device against physical loss or theft and agrees to abide by the following general rules governing State-owned mobile devices:

- State-owned hardware and software (including mobile devices) may be used only for official duties
- Only authorized individuals may use State-issued mobile devices
- Users will not make any changes to the device that prohibit the Mobile Device Manager (MDM) from properly operating
- Devices losing the mobile-device-management function must be returned to the issuing authority for technical support before accessing the network
- User accounts not active after 30 calendar days will be marked as inactive and may be disabled or deleted from the MDM
- Confidential data will not be stored on the device (See the Enterprise ISSM for information on exceptions)
- Users will safeguard confidential information, such as that accessed through State-issued email via the mobile device, as described in the *DoIT Public and Confidential Information Policy*

Additionally, mobile-device users:

- Will have a signed agreement to *Acceptable Use Policy* on record and will use the mobile device per the Policy
- Will ensure security updates, including installed-app updates, are routinely installed by connecting to the MDM
- Will not install unauthorized software (including apps) or hardware nor intentionally introduce any malicious code (e.g., Trojan-horse programs, viruses, worms)
  - The Enterprise or Agency Configuration Manager maintains a list of authorized applications
  - Downloading unauthorized apps will result in the user's device being flagged for noncompliance, and the device will be prevented from accessing the network
  - Should the user require specific apps that are unavailable from the MDM solution, an application-approval request must be submitted, including approval from the user's direct supervisor to the authorizing official (see section 4.4, item A)
- Will not connect the State-owned device to a non-State-owned system (e.g., the user will not connect the mobile device to a personal laptop) either through wireless connection, such as Bluetooth, or wired connection, such as USB — not even to charge the device

  NOTE: Certain mobile accessories may be authorized, such as a Bluetooth headset; refer to the Enterprise or Agency Configuration Manager for approved accessories.

- Will adhere to the password complexity requirements (see *DoIT Account Management Policy*) when provisioning the device; this feature must remain enabled
- Will not connect or access personal accounts (e.g., personal Gmail) from the device; this will prevent accidental "syncing" of personal account data to the State network or spilling State data into a personal account
- Will not forward private calls from a personal residential or cellphone to the State-owned device
- Will not introduce unauthorized removeable media, such as a micro-SD card, or remove any issued removeable media
- Will not attempt to disable required security features or bypass the MDM system policies
- May use the State-owned device to tether a mobile connection to another State-owned device (e.g., connecting an agency issued laptop during travel)
- Must promptly report any device theft, loss, suspected compromise, or suspicious behavior to the DoIT Service Desk, as well as degradation or interruption of service

  NOTE: Be aware that data owners will be notified of potential unauthorized information access or data breach (from mobile users) that may trigger a security investigation
- Will present the device to the issuing authority at least twice a year to ensure any major security updates for either the device or the MDM are installed and properly configured

## Part II – Personal Information

| | | |
|---|---|---|
| Name (Last, First, MI): | Dept. or Agency: | Division: |
| Location (Street, City, Zip): | Position/Title: | Room or Desk #: |
| Email Address: | | Work Phone: |
| Immediate Supervisor – Name, Phone, Email Address: | | |

## Part III – Equipment Information

| | | | |
|---|---|---|---|
| Device Information:<br>[ ] Cellphone/Smartphone [ ] Tablet/iPad [ ] Mobile Router/Hotspot [ ] Other: | | | |
| SIM Card Number: | Assigned Phone Number: | Device IMEI Number: | Device MAC Address: |
| Manufacturer Name/Model: | Serial Number: | Asset ID: | Account Number: |
| Issuing Dept. or Agency: | Supervisor Approval: | | Work Phone: |

## Part IV – User Agreement

| | | |
|---|---|---|
| By signing below, I acknowledge receipt of the described State-owned mobile device, issued in good working condition and compliant with current configurations and policies. In addition, I understand that this issued device is subject to review and monitoring per established policy. My signature below indicates I have read and understand Part I – User Responsibilities of this form, read and signed the *DoIT Acceptable Use* form, and agree to these conditions. | | |
| Receiver Signature: | Receiver Printed Name: | Date of Issuance: |

## Part V – Issuing Authority Verification

| | | |
|---|---|---|
| The original form signed by the receiver will be kept on file by the issuing unit authority per the *DoIT Mobile Device Security Policy*. A copy will be provided to the receiver upon receipt of the issued device and again upon return of the issued device. | | |
| Equipment Issued | | |
| Printed Name of Issuer: | Signature of Issuer: | Date of Issuance: |
| Equipment Returned | | |
| Printer Name of Issuer: | Signature of Issuer: | Date of Equipment Return: |

# Appendix B: Personally-Owned Device (BYOD) Agreement

After reviewing the User Responsibilities in Part I below, fill out the forms of parts II through V, and submit to your agency authorizer for personally-owned mobile device access to State resources, i.e., BYOD deployment model.

**Part I – User Responsibilities**

The authorized use of personally-owned devices within the DoIT Enterprise is a privilege granted to Enterprise and agency staff by the executive management of the Department of Information Technology (DoIT), who reserves the right to revoke this privilege at any time, without warning or notification, either individually or at large. The use of their own devices allows staff greater mobility, enhanced services, and improved productivity but does present significant challenges in protecting the network and its data from attack and compromise.

Authorization for BYOD is based on the following criteria:

- Sensitivity of the accessed data
- Regulatory compliance prohibiting or limiting usage of mobile devices
- The type and model of device being used
- Agreement to Mobile Device Management (MDM) solution terms and conditions
- Other technical or eligibility requirements identified by DoIT management

An approved BYOD Agreement authorizes a staff member to use a specific, personally-owned mobile device (as defined in the DoIT Mobile Device Security Policy) to access State services or resources as approved by the staff member's direct supervisor.

Terms and Conditions (personal device users):

- Will have a signed agreement to the DoIT Acceptable Use Policy on record and will use the mobile device per the policy
- Will safeguard confidential information as described in the DoIT Public and Confidential Information Policy, such as that accessed through State-issued email via the mobile device
- Acknowledge the device and the State data accessed is subject to monitoring per policy
- Will authorize the installation and configuration of the DoIT MDM solution to manage and maintain data access and protections
- Will configure their mobile devices with security features (e.g., passwords) required to protect information and the access they maintain
- Will not modify or disable configuration settings of the MDM solution
- Are responsible for protecting their mobile device from loss or theft
- Will promptly report loss, theft, or possible data compromise to the DoIT Service Desk, including when the device is no longer valid for the approved access (e.g., user upgrades device or changes carriers).
- Must submit a new agreement form if the identified, approved mobile device is changed, such as the user upgrading to a new model or changing carriers

- Will, if replacing an approved device, wipe the old device before disposal, e.g., the user upgrades to a new device and turns in the old (approved) device for sanitizing
- Must be the owner-of-record for the approved device
- Must not share or otherwise allow access to the device by others
- Must have an approved mobile carrier (i.e., T-Mobile, AT&T, Verizon, etc.) and cannot use a disposable device or a device in which the user purchases minutes as used
- Must not "jail break" or "root" the device and must protect it from all attempts to bypass the standard operation and security configuration of an authorized-access mobile device
- Understands that DoIT will not provide technical support for the device other than for MDM configuration issues
- Must submit an application-approval request to the authorizing official (see section 4.4, item A) to acquire an app that is unavailable from the MDM solution; the application must include approval from the user's direct supervisor
- Must accommodate the DoIT recommendation to use security partitions which may be available within the MDM solution, such as Android's Secure Folder or Samsung's Fort Knox, to maintain a defensive layer between the user's personal apps and data and limit the risks associated with accessing the DoIT networks and data with a personally-owned device
- Users will immediately report any loss, theft, or suspicious device behavior as well as degradation or interruption of service to the DoIT Service Desk

  NOTE: Be aware that data owners will be notified of potential unauthorized information access or data breach (from mobile users) that may trigger a security investigation

Depending on the solution and the access being granted, DoIT may provide additional terms and conditions to this agreement which will require additional initials or signatures of acknowledgement

## Part II – Personal Information

| | | |
|---|---|---|
| Name (Last, First, MI): | Dept. or Agency: | Division: |
| Location (Street, City, Zip): | Position/Title: | Room or Desk #: |
| Email Address: | | Work Phone: |
| Immediate Supervisor – Name, Phone, Email Address: | | |

## Part III – Equipment Information

| | | | |
|---|---|---|---|
| Device Information:<br>[ ] Cellphone/Smartphone [ ] Tablet/iPad [ ] Mobile Router/Hotspot [ ] Other: | | | |
| Carrier Name: | Account Number: | Device IMEI Number: | Device MAC Address: |
| Manufacturer Name, Model, and Model Number: | | Serial Number: | Phone Number: |
| Supervisor Approval: | | Date: | Work Phone: |

## Part IV – User Agreement

| | | |
|---|---|---|
| By signing below, I acknowledge acceptance of the DoIT terms and conditions associated with using a personally-owned mobile device to access services and resources provided by DoIT. In addition, I understand that those services and resources provided by DoIT are subject to monitoring as defined by policy. My signature below authorizes DoIT to exercise and enforce its security, privacy, and management controls to protect confidential data from loss or compromise. These controls may include device geo-locating, disabling the device, and remote data wipe. DoIT does not assume any liability for the loss of personal data, interruption in service, or expenses (such as carrier data charges) incurred by the MDM solution or the enforcement of its security measures. | | |
| Employee or Contractor Signature: | Printed Name: | Date: |

## Part V –Authorizing Official

| | | |
|---|---|---|
| The original form signed by the user will be kept on file per the *DoIT Mobile Device Security Policy*. A copy will be provided to the user upon authorization of access and again upon revocation of access. | | |
| Authorization Granted | | |
| Printed Name of Authorizing Official: | Signature of Authorizing Official: | Date of Authorization: |
| Authorization Revoked | | |
| Printed Name of Authorizing Official: | Signature of Authorizing Official: | Date of Revocation: |