Mobile Device Policy

Effective Date:
July 14, 2026

Category:
Security

Scheduled Review:
July 2027

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Document Control

This document replaces, in its entirety, the *Mobile Device Policy*, dated January 6, 2025.

3. Purpose

This Information Technology Policy (ITP) establishes requirements, responsibilities, and security controls for the use, management, and protection of Mobile Devices that access, store, or transmit Commonwealth data or connect to Commonwealth IT resources and networks.

4. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

5. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

5.1 General Requirements

Mobile Devices shall not store or transmit class "C" or non-public information without the protective measures detailed in the *Data Classification Policy* and Agency or Delivery Center Information Security Officer (ISO) approval.

Commonwealth-issued Mobile Devices may not be connected to public Wi-Fi.

Mobile Devices shall adhere to established security controls, including but not limited to:

• Physical protection

• Access control mechanisms
• Cryptographic safeguards
• Data backups
• Virus protection
• Rules governing network connections

Mobile Devices used for official business shall not be Jailbroken or Rooted. Such activity is considered misuse of IT resources and may result in disciplinary action.

The use of Promiscuous Mode from a Commonwealth issued Mobile Device is prohibited. Additionally, the use of Promiscuous Mode from any device while connected to the Commonwealth Network is prohibited.

Mobile Devices containing Commonwealth Data shall be secured from access by unauthorized persons, through the use of locking devices, passwords, or other approved protection such as Mobile Device Management (MDM).

In the event a Commonwealth issued Mobile Device or privately-owned mobile device that contains Commonwealth Data is lost or stolen, it should be reported in accordance with the *IT Security Incident Reporting Policy*.

Commonwealth-issued devices may be wiped or have service suspended at any time as deemed necessary by the Office of Administration, Office for Information Technology (OA/IT).

Authorized users of Mobile Devices shall ensure all operating system and security updates are applied in accordance with the *IT Resource Patching Policy*. Devices may be locked or have service suspended if operating system and security updates are not applied once OA/IT vetting is complete and the update is approved for use.

5.2 Network and SIM Security

Mobile Devices connecting directly to the Commonwealth network via carrier integration must implement secure authentication mechanisms, including:

- eSIM or SIM cards with PIN protection, or
- Compensating controls such as SIM locking to device identifiers

5.3 Mobile Device Management (MDM) and Mobile Application Management (MAM)

The following table summarizes the required use of the MDM and MAM service offerings from OA/IT for Mobile Devices. Refer to the *Mobile Device Configuration Standard* for guidance on baseline configurations required for these service offerings.

Device Type	Mobile Device Management (MDM)	Mobile Application Management (MAM)
Commonwealth-issued devices	Agencies must leverage OA/IT service offering or obtain and submit an approved exception for an alternative.	Not Applicable

Privately-Owned devices / Bring your own device (BYOD)	Not Applicable	Users with Privately-Owned Devices are required to use MAM for Commonwealth applications to prevent disclosure of Commonwealth Data.

5.4 Commonwealth-Issued Mobile Devices

All Commonwealth-issued Mobile Devices shall be actively enrolled in the OA/IT-approved service offerings for MDM and mobile security prior to initial activation, configuration, or use. Devices shall remain continuously enrolled while issued, used, or in the possession of an authorized user.

Commonwealth-issued Mobile Devices shall comply with applicable security controls, including but not limited to remote lock and wipe capabilities, real-time threat detection, malware protection, operating system and security update enforcement, and secure configuration baselines established by OA/IT.

Use of a Commonwealth-issued Mobile Device is prohibited unless the device is actively enrolled in the required OA/IT-approved MDM and mobile security service offerings.

Agencies shall ensure that required licenses, subscriptions, and service entitlements are maintained and remain active without lapse.

Any attempt to disable, remove, bypass, circumvent, or otherwise interfere with required device management, mobile security, or other security controls on Commonwealth-issued Mobile Devices is prohibited and may be considered misuse of Commonwealth IT resources.

Lost, stolen, compromised, or non-compliant Commonwealth-issued Mobile Devices shall be reported in accordance with the *IT Security Incident Reporting Policy*.

Agencies shall work with their Information Security Officers to periodically review compliance with this policy.

Non-compliance may result in revocation of device privileges, billing agencies for replacement or recovery costs, and any other enforcement actions consistent with Commonwealth disciplinary and incident response procedures.

Agencies shall ensure that users who are issued Commonwealth Devices opt in to the enterprise emergency notification system.

5.4.1 Supported Mobile Devices

OA/IT will maintain a Mobile Device Certification List (available via the Telecommunication Management Officer (TMO) SharePoint site). Only approved devices may be procured and deployed.

5.4.2 Interconnected Devices and Wearables

Agencies shall complete an *IT Risk Acknowledgement Form* for each interconnected device or wearable prior to adding the device to the Supported Mobile Device Certification List.

As part of the risk assessment, agencies shall assess and document:

- All communication capabilities, including but not limited to cloud connectivity, near field communication (NFC), wireless networking (WLAN), and other communication vectors
- Privacy risks associated with data that is transmitted and/or stored by the device

Additionally, all applicable end-user license agreements (EULAs) shall be reviewed and approved by legal counsel.

5.4.3 Mobile Satellite Devices

Mobile satellite devices shall be enrolled in Mobile Device Management (MDM) in instances where it is technically possible, and the device is compatible with the Commonwealth's MDM service offering.

Agency personnel planning to utilize mobile satellite devices while traveling for Commonwealth business outside of the United States shall ensure they are aware of and comply with any local laws and regulations related to the possession and usage of mobile satellite devices including any applicable license agreements or usage terms.

5.5 Privately Owned Mobile Devices

The use of privately-owned devices, including privately-owned mobile devices, is governed by the *Privately Owned Device Standard*.

5.6 Mobile Applications

Mobile Applications can be developed internally by an agency or developed by an external third-party entity. Applications developed by a third-party entity usually have their own end-user license agreement (EULA) with separate terms and conditions.

A list of third-party applications that have been reviewed and approved by OA/IT for use by all Agencies will be made available on the TMO SharePoint site. All other third-party applications shall be reviewed and approved at the agency level as follows:

- Any Agency hosting a third-party developed Mobile Application within its own application repository is responsible for ensuring that the application is vetted with appropriate Agency IT, executive, and legal approvals. The Agency accepts all financial, security, and legal risks associated with that decision.

- Third-party applications that duplicate capabilities within existing third-party applications previously reviewed and approved by OA/IT are prohibited. Third-party applications the Agency is considering must add functionality that is required and unavailable within the current list of OA/IT reviewed and approved third-party applications.

- The management and approval of third-party applications for installation on Commonwealth-issued Mobile Devices must be approved by both the Agency CTO and Agency ISO and have an executed agreement. OA/IT shall maintain agency and business area specific application catalogs within the MAM/MDM primary service offering.

- Agencies shall submit requests for new third-party mobile applications through the OIT Procurement Intake process and attach written approval from the Agency CTO/ISO to the OIT Procurement Intake request (only agency submitters can complete this request).

- When procurement intake approval is granted, the system will automatically send an approval letter

to the submitter.

- After obtaining CTO, ISO, and OIT Procurement Intake approval agencies shall submit requests for new mobile application via the Enterprise ITSM System. The CTO and ISO approval and OIT Procurement Intake Approval Letter must be attached to the request.

Direct access to consumer app stores by the end user is prohibited on Commonwealth-issued Mobile Devices.

5.7 Mobile Email Management

Agencies requiring access to CWOPA (Exchange) email from Commonwealth issued or privately-owned mobile devices shall use the OA/IT Mobile Application Management (MAM) Messaging service, which provides a secure, containerized email solution.

All other email messaging applications not explicitly authorized in this policy are prohibited; including, but not limited to, web mail scrapers, non-Commonwealth- issued Virtual Desktop Interface (VDI) clients, or any other non-Commonwealth-issued messaging applications that access Commonwealth IT Resources.

6. Contact

Questions or comments may be directed via email to OA, IT Policy.

7. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

8. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document
Revision	07/14/2026	• Clarified that devices may be locked or have service suspended if required updates are not applied • Updated mobile application approval process • Clarified that agencies are to procure devices exclusively through the established OA/IT telecommunications process • Added requirement that users of Commonwealth-issued devices enroll in the enterprise emergency notification system • Relocated privately owned device requirements to a separate standard document • Removed the section related to unsupported devices • Other general clarifications and grammatical updates • Added requirements for Commonwealth-issued Mobile Devices to remain continually enrolled in MDM, maintain active licensing or subscriptions, comply with mobile security controls, and undergo periodic compliance review. • Added requirements around the new mobile security service offering.