pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Mobile Device Security Policy

ITP Number	Effective Date
ITP-SEC035	March 13, 2014
Category	**Supersedes**
Security	ITP-SYM007 (rescinded)
Contact	**Scheduled Review**
ra-ITCentral@pa.gov	July 2022

1. Purpose

This Information Technology Policy (ITP) establishes the accepted practices, responsibilities, and procedures for the use of Commonwealth-issued and/or personally owned Mobile Devices that are authorized to leverage Commonwealth IT Resources and/or networks.

2. Scope

This Information Technology Policy (ITP) applies to all offices, departments, boards, commissions and councils under the Governor's jurisdiction (hereinafter referred to as "agencies") or other entities connected to the Commonwealth network.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Definitions

3.1 Active Directory: A management tool for managing directory-based identity-related services.

3.2 Commonwealth Data: Any information, regardless of form, the media on which it resides or the method of capture, that is owned, managed, processed, generated or stored by the Commonwealth, which may be protected by law, order, regulation, directive or policy and may be sensitive or confidential so that it requires security controls and compliance standards.

3.3 Jailbreak/Rooting: The process used to modify the operating system on a Mobile Device. The act of "jailbreaking" or "rooting" a Mobile Device allows the user control over the device including removing any vendor-imposed restrictions on the products.

3.4 Mobile Application: A computer program designed to run on Mobile Devices and as an add-on to existing applications

3.5 Mobile Application Management (MAM): The process of developing, procuring, deploying and managing the configuration, distribution and access of in-house and commercially developed mobile apps through an enterprise app virtual marketplace or a consumer app store.

3.6 Mobile Communication Device (Mobile Devices): Any mobile phone, smartphone, or tablet that transmits, stores, and receives data, text, and/or voice with a connection to a wireless local area network (LAN) and/or cellular network that are authorized to leverage

Commonwealth IT Resources and/or networks. These devices do not utilize or cannot utilize the enterprise authentication services nor desktop management tools and require provisioning through a mobile device management solution for access to Commonwealth IT Resources.

3.7 Mobile Device Management (MDM): Software technologies that secure, monitor, manage and support Mobile Devices deployed across the enterprise. By controlling and protecting the data and configuration settings for all Mobile Devices in the network, MDM can reduce support costs, security, and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime.

3.8 Mobile Email Management (MEM): Controls which Mobile Devices can access email, prevents data loss, encrypts sensitive data and enforces compliance policies.

3.9 Promiscuous Mode: A mode for a network controller (a server that manages authentication requests) that causes the controller to pass all traffic it receives to the device rather than passing only the frames that the controller is intended to receive. This mode is normally used for packet sniffing.

4. Policy

No Mobile Device may store or transmit non-public or sensitive information without protective measures approved by the agency Information Security Officer (ISO). Physical protection, access controls, cryptographic techniques, backups, virus protection, and the rules associated with connecting Mobile Devices to networks and guidance on the use of these devices in public places must be applied to all Mobile Devices. These requirements extend to, and cover, removable/mobile media associated with Mobile Devices.

Mobile Devices containing Commonwealth Data are not to be left unattended. Mobile Devices must be secured from access by unauthorized persons, through the use of locking devices, passwords, or other appropriate protection. Commonwealth-issued or personal Mobile Devices used for official business cannot be Jailbroke or Rooted. A Commonwealth-issued device that is Jailbroken or Rooted is deemed "misuse of IT resources" and personnel may face disciplinary actions due to non-compliance with Management Directive 205.34 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

4.1 Mobile Device Management

The following table summarizes the required use of MDM, MAM, and MEM service offerings from the Office of Administration, Office of Information Technology (OA/OIT) for Commonwealth-issued and personal Mobile Devices. Refer to OPD- SEC035A *Device Management Configurations (authorized CWOPA personnel only, contact RA-ITCentral@pa.gov for requests)* for guidance on baseline configurations required for MDM and MEM.

	Mobile Device Management	Mobile Application Management	Mobile Email Management
Commonwealth-issued Devices	Agencies must leverage OA/OIT service offering or submit a waiver for an alternative.	Agencies must leverage OA/OIT service offering or submit a waiver for an alternative.	Agencies must leverage OA/OIT service offering.
Personal devices / bring your own device (BYOD)	Not Applicable	Users with personal devices may be required to use MAM for some Commonwealth applications to prevent disclosure of Commonwealth Data.	Agencies must leverage OA/OIT service offering or utilize a mobile browser for Outlook Web Access (OWA).

4.2 Mobile Devices

Agencies must submit an ITP waiver with a security management plan for any Active Directory *capable* devices that are not joined to the Commonwealth Active Directory domain and not managed by OA/OIT service offerings.

Promiscuous Mode from a Mobile Device while attached to the Commonwealth network is prohibited.

4.3 Commonwealth-Issued Mobile Devices

All Commonwealth-issued Mobile Devices are required to use OA/OIT service offerings for device management.

Agencies that do not elect to leverage the OA/OIT service offering must have a documented and OA/OIT approved alternative approach to meet the policy requirements in section 5 of this ITP. Any alternative mobile security strategy must receive an approved ITP waiver.

4.3.1 Supported Mobile Devices

OA/OIT will publish and make accessible via the Telecommunication Management Officer (TMO) SharePoint site a current Mobile Device Certification List of Mobile Devices supported by OA/OIT service offerings.

4.3.2 Unsupported Mobile Devices

For mobile devices not listed on the Mobile Device Certification List, agencies shall maintain the responsibility for ensuring these devices conform to the minimum security requirements, perform validation testing, and submit a Mobile Device Certification Form to RA-EnterpriseVoiceServices@pa.gov for review before connecting any unsupported mobile device to the Commonwealth network or accessing Commonwealth IT Resources.

4.3.3 Interconnected Devices and Wearables

Agencies are recommended to conduct risk assessments of each Mobile Device prior to adding to the supported Mobile Device Certification List. Active cloud connectivity, near field communication (NFC), wireless networking (WLAN), and other communication vectors available will need internal risk profiles completed (contact agency or respective ISO for guidance). Each Mobile Device should be reviewed for privacy concerns of data that is transferred and all applicable end-user license agreements (EULAs) should be

reviewed by legal counsel.

4.4 Personal Mobile Devices

OA/OIT MDM service offerings or an agency alternative mobile security solution is not required for personal Mobile Devices (non-Commonwealth-issued devices).

4.5 Mobile Application Management

MAM is used to distribute and manage Mobile Applications. Agencies requiring the use of MAM for Commonwealth-issued Mobile Devices must use the OA/OIT Mobile Management Services service offering.

Users who install Commonwealth applications on personal Mobile Devices may also require the use of MAM to ensure security of Commonwealth Data. Agency ISOs are to make final determinations on appropriate use of personal Mobile Devices and the use of Commonwealth applications.

4.6 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.

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

4.7 Mobile Email Management

Agencies requiring access to CWOPA (Exchange) email from Commonwealth–issued or personal Mobile Devices must use the OA/OIT Messaging (secure containerized email) service.

Agencies requiring access to CWOPA (Exchange) email from personal (BYOD) devices must use the OA/OIT Messaging (secure containerized email) service.

All other messaging applications not defined 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.

5. Mobile Device Provisioning

Figure 1 below details the approval workflow and applies to all organizations issuing Commonwealth-issued Mobile Devices to staff. TMOs are responsible for creating a constant, repeatable, and auditable approval process to ensure recipient staff have the appropriate approval from their operational and financial management leadership.

Each request must be authorized by the appropriate director-level manager in the user's management chain or their designee. All requests for services, new hardware, or replacement hardware must be approved by the appropriate financial manager.

The workflow may be satisfied by workflows leveraging Commonwealth ITSM tools, or custom applications built within environments such as SharePoint. A manual paper process leveraging the form in Management Directive 240.11 *Commonwealth Wireless Communication Policy* may be used as an interim solution. Identification of the approver and hardware/service

recipient must be recorded in this process.

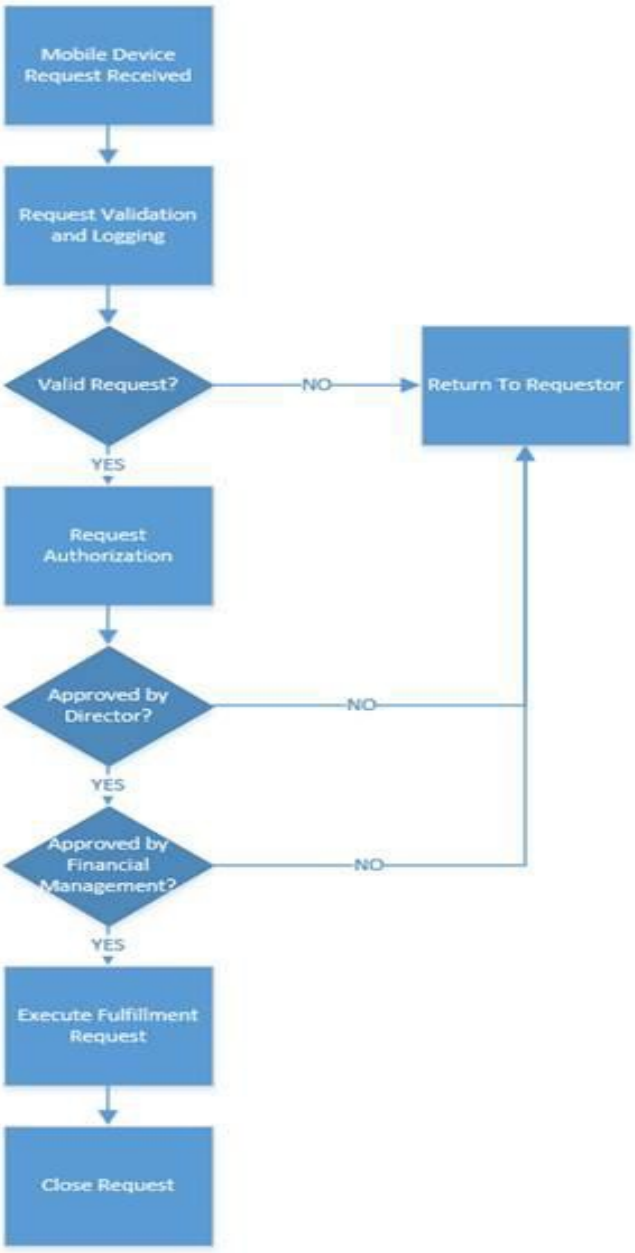

Figure 1. Mobile Device Authorization Process

6. Responsibilities

6.1 Agencies:

- Ensure any Commonwealth-issued Mobile Device connected to the Commonwealth network is either fully managed by OA/OIT service offerings or adheres to an agency mobility security policy that has been approved by OA/OIT through the waiver review process per ITP-BUS004 *IT Waiver Review Process*.
- Ensure any personal Mobile Device connected to the Commonwealth network utilizing messaging services is managed by OA/OIT Enterprise Mobile Messaging (secure containerized email) Services.

- Immediately report a lost or stolen Mobile Device or any compromise of data of a Mobile Device per ITP-SEC024 *Information Technology Security Incident Reporting Policy*.

6.2 Office of Administration, Office for Information Technology (OA/OIT):

- Manages the MDM, MAM, and MEM service offerings and base configurations.

6.3 Third-party vendors, licensors, contractors, or suppliers:

- When providing services to the Commonwealth must comply with the requirements outlined in this ITP and OPD-SEC000B *Security Policy Requirements for Third Party Vendors*.

7. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- Management Directive 240.11 *Commonwealth Wireless Communication Policy*
- OPD-SEC000B *Security Requirements for Third Party Vendors*
- OPD-SEC035A *Device Management Configurations (authorized CWOPA personnel only, contact RA-ITCentral@pa.gov for requests)*
- ITP-ACC001 *Information Technology Digital Accessibility Policy*
- ITP-BUS011 *Commonwealth Cloud Computing Services Requirements*
- ITP-BUS004 *IT Waiver Review Process*
- ITP-NET016 *Wireless Cellular Data Technology*
- ITP-SEC000 *Information Security Policy*
- ITP-SEC001 *Enterprise Host Security Software Suite Policy*
- ITP-SEC005 *Commonwealth Application Certification and Accreditation*
- ITP-SEC024 *IT Security Incident Reporting Policy*
- ITP-SEC031 *Encryption Standards*

8. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which

appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

10. Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	03/13/2014	Base Document	N/A
Revision	04/6/2020	• Removed references to Enterprise Mobility Management Agency Guidance • Removed Objectives section • Migrated Device Management Configurations to OPD-SEC035A • Added Mobile Applications language in Policy section • Edited language throughout for clarity • Added Exemption section	Revised IT Policy Redline <04/6/2020>
Revision	07/19/2021	• Updated Scope • Updated policy reference/links • Added third party vendors to Scope and Responsibilities section	Revised IT Policy Redline <07/19/2021>