pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Mobile Device Security Policy

ITP Number	***Effective Date***
ITP-SEC035	03/13/2014
Category	***Supersedes***
Recommended Policy	ITB-SYM007
Contact	***Scheduled Review***
ra-ITCentral@pa.gov	Annual

This Information Technology Policy establishes policy, responsibilities, and procedures for connecting and using mobile communication devices to access commonwealth IT resources.

1. Purpose

To define accepted practices, responsibilities and procedures for the use of commonwealth-issued and/or personally owned mobile devices that are authorized to connect to the commonwealth network.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the governor's jurisdiction (agencies) or other entities connected to the commonwealth network.

3. Definitions

3.1 Mobile Communication Device (Mobile Devices)

Any mobile phone, smartphone, laptop, or media tablet that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network.

3.2 Smartphone

A mobile communication device with voice, messaging, scheduling, email and Internet capabilities. Smartphones also permit access to application stores, where additional software can be obtained for installation on the mobile device.

3.3 Tablet

An open-face wireless device with touch screen display, primarily used in the consumption of media. These devices may also have messaging, scheduling, email, and Internet capabilities and a camera. Tablets may have open-source OSs (such as Android) or closed OSs under the control of OS vendors and/or device manufacturers (such as Apple and Microsoft). Media tablets may or may not support a mobile application store.

3.4 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.

3.5 Mobile Email Management (MEM)

Mobile Email Management (MEM) controls which mobile devices that can access email, prevents data loss, encrypts sensitive data and enforces compliance policies.

3.6 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.

3.7 Multi-Homed / Split Tunneling

Simultaneously using two different networks or connections, such as USB, wireless, cellular, or Bluetooth, or near-field communications (NFC).

3.8 Promiscuous Mode

A mode for a network controller 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.

3.9 Jailbreaking / 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.

4. Objective

To define accepted practices, responsibilities and procedures for the use of commonwealth-issued and/or personally owned mobile devices that are authorized to connect to the commonwealth network.

5. Policy

5.1 Policy Summary

The following table summarizes the required use of Mobile Device Management, Mobile Application Management and Mobile Email Management service offerings from OA-OIT for commonwealth-issued and personal devices.

	Mobile Device Management	Mobile Application Management	Mobile Email Management
Commonwealth-issued Devices	Agencies must leverage OIT Service Offerings or submit a waiver for an alternative	Agencies must leverage OIT Service Offerings	Agencies must leverage OIT Service Offerings
Personal / BYOD devices	Not Applicable	Not Applicable	Agencies must leverage OIT Service Offerings

5.2 Mobile Devices

For the purpose of this policy, *mobile devices* are devices, such as smartphones and tablets, which are not joined to the commonwealth Active Directory domain and are not capable of being managed by the product standards used for desktop patch management as per ITP-SEC001.

Agencies must submit a 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.

Multi-homing/Promiscuous Mode from a mobile device while attached to the commonwealth network is prohibited.

5.3 Commonwealth-Issued Mobile Devices

All commonwealth-issued mobile devices are required to use OA-OIT enterprise services for device management. Details for these service offerings can be found in the addendum, *Enterprise Mobility Management – Agency Guidance* or from your agency Telecommunication Management Officer (TMO).

Agencies that do not elect to leverage OA-OIT service offerings must have a documented and OIT approved alternative approach to meet the policy requirements in section 6 of this ITP. Any alternative mobile security strategy must be filed as a waiver request per ITP-BUS004 and must be approved by OA-OIT.

5.3.1 Supported Mobile Devices

OA/OIT will publish and make accessible via the IT Central website a current certified device list for devices supported by OA-OIT service offerings.

5.3.2 Unsupported Mobile Devices

For un-tested device types, legacy OS versions, and versions not yet approved for use, 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 OA-COPAMDMDeviceCertification@pa.gov for review before connecting any unsupported mobile device to the commonwealth network.

5.4 Personal Mobile Devices

OA-OIT Mobile Device Management service offerings or an agency alternative mobile security strategy is not required for personal mobile devices (non-commonwealth-issued devices).

5.5 Mobile Application Management

Mobile Application Management (MAM) is used to distribute and manage mobile applications. Agencies requiring the use of MAM for commonwealth-issued devices must use OA-OIT Enterprise Mobile Management Services.

Agencies and the Office of Administration (OA) will approve applications for commonwealth-owned devices.

- OA will approve enterprise applications within the enterprise application repository.
- Agencies will approve agency-specific applications for use within an agency application repository.
- Any agency hosting a commercially developed mobile application within their own application repository accepts all financial, security, and legal risks associated with that decision.
- Agency developed applications hosted on MAM are required to adhere to the $(CA)^2$ standard application vetting processes per ITP-SEC005 - *Commonwealth Application Certification and Accreditation.*

5.6 Mobile Email Management

Agencies requiring access to CWOPA (Exchange) email from commonwealth–issued devices must use either the OA-OIT Enterprise Messaging (secure containerized email) service or Enterprise Mobile Management Services (EMMS).

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

Details for these service offerings can be found in the addendum, *Enterprise Mobility Management – Agency Guidance* or from your agency Telecommunication Management Officer (TMO).

Additionally, OA-OIT provides Outlook Web Access (OWA). OWA provides

access to email from Internet browsers, including Internet browsers on mobile devices.

All other messaging applications not defined in this policy are prohibited; including but not limited to web mail scrapers, non-commonwealth issued VDI clients, or any other messaging applications that access commonwealth resources.

6. Configuration

6.1 Mobile Device Management (MDM) – Baseline Configuration

The following minimum security policies apply to all commonwealth-issued mobile devices permitted for use on the commonwealth network. Agencies may, at their discretion, implement more stringent policies as required.

MDM Configuration	
Policy Requirements	Minimum Requirement
Device password: **minimum 6 characters** required	**Enforced** by OIT Service Offering
Device wipe after 10 failed attempts	
Enterprise Data wipe for Jailbroken/Rooted devices	
Device Encryption	
Device 15 Minute inactivity timeout	
Device Passwords will expire after sixty days, requiring the creation of a new password	
May not reuse any of the last ten previously used passwords	
Backup of data to any device will be encrypted	
SD cards or other portable media that contain sensitive data must be encrypted (per ITP-SEC020 Encryption Standards for Data at Rest)	
Sync to vendor cloud based backup disabled	
Minimum Operating System version controlled per Mobile Device Certification List	
Mobile Antivirus for Non-iOS Devices	
Remote wipe for lost/stolen mobile devices	Action required by Agency Administrator (required per ITP-SEC024)

6.2 Mobile Email Management (MEM) - Baseline Configuration

The following minimum secure messaging policies apply to all commonwealth-issued mobile devices permitted for use on the commonwealth network.

MEM Configuration for Commonwealth-Issued Mobile Devices	
Policy Requirements	**Minimum Requirement**
Minimum Operating System version controlled per Mobile Device Certification List	On certified device list
Non-Standard attachments blocked	Enforced by MEM
Mobile Antivirus for Non-iOS Devices	
Device password: **minimum 6 characters** required	
Data copy from device applications into commonwealth secure email application	Allowed
Data copy from commonwealth secure email application into device applications	
Storage card encryption	
Remote wipe of commonwealth secure email	
Ability to edit attachments received in email and send documents as attachments created in device applications through the commonwealth secure email application	

The following minimum secure messaging policies apply to all personal mobile devices permitted for use on the commonwealth network.

MEM Configuration for Personal Mobile Devices	
Policy Requirements	**Minimum Requirement**
Minimum Operating System version for device	Minimum OS level supported by MEM
Secure email container password: **minimum 6 characters** required	Enforced by MEM
Mobile Antivirus for Non-iOS Devices	
Non-Standard attachments blocked	
Secure email container locked after idle for more than 15 minutes	
Data wipe upon Jailbreak/Rooted device detection	
Data copy into secure email container	
Data copy from secure email container	Prohibited
Ability to edit attachments received in email and send documents created in device applications through email as attachments	
Importing/exporting attachments between secure email container and third-party applications	

7. Responsibilities

7.1 Agencies Shall:

- Ensure any commonwealth-issued mobile device connected to the commonwealth network is either fully managed by OA-OIT services or adheres to an agency mobility security policy that has been approved by OIT through the waiver review process per ITP-BUS004.
- Ensure any personal mobile device connected to the commonwealth network utilizing messaging services is managed by OA-OIT Mobile Messaging (secure containerized email) Services and is in compliance

with MD 240.11 - Commonwealth Wireless Communication Policy.

- Immediately report a lost or stolen wireless communication device or any compromise of data of a wireless communication device per ITP-SEC024 - Information Technology Security Incident Reporting Policy.

8. Related ITPs/Other References

- ITP-SEC001 – Enterprise Host Security Software Suite Policy
- ITP-SEC005 - Commonwealth Application Certification and Accreditation
- ITP-SEC020 – Encryption Standards for Data at Rest
- ITP-SEC024 – IT Security Incident Reporting Policy
- ITP-BUS004 – IT Waiver Review Process
- MD 240.11 – Commonwealth Wireless Communication Policy
- MD 205.34 –Information Technology Acceptable Use Policy
- Enterprise Mobile Device Email Rules of Engagement
- Enterprise Mobility Management – Agency Guidance

9. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

10. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original		Base Document