Information Technology Policy

Mobile Device Security Policy

Number ITP-SEC035	**Effective Date** March 13, 2014
Category Security	**Supersedes** ITP-SYM007
Contact RA-ITCentral@pa.gov	**Scheduled Review** February 2025

1. Purpose

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

2. Scope

This ITP 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 ITP as outlined in the Responsibilities section.

3. Policy

Mobile Devices shall not store or transmit sensitive or non-public information without protective measures approved by the agency Information Security Officer (ISO).

Mobile Devices are prohibited from being connected to public Wi-Fi. Physical protection, access controls, cryptographic techniques, backups, virus protection, and the rules associated with connecting Mobile Devices to networks (excluding all public Wi-Fi, which is prohibited under this policy), and guidance on the use of these devices in public places must be followed on all Mobile Devices. These requirements extend to, and cover, removable/mobile media associated with Mobile Devices.

Mobile Devices connecting directly to the Commonwealth network via carrier cellular network integration shall ensure embedded SIM cards, eSIM cards, or compensating controls such as SIM PINs, or locking of the SIM to the serial number of the device are in place to prevent the use of the SIM in an unauthorized device.

Mobile Devices containing Commonwealth Data shall not be left unattended.

Mobile Devices must be secured from access by unauthorized persons, through the use of locking devices, passwords, or other approved protection.

Mobile Devices used for official business shall not be Jailbroken or Rooted. A Commonwealth-issued Mobile Device that is Jailbroken or Rooted is deemed "misuse of IT resources" as defined in *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy* and personnel may face disciplinary actions due to non-compliance.

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

Authorized users of Mobile Devices shall ensure all security updates are applied in accordance with *ITP-SEC041, Commonwealth IT Resources Patching Policy*.

3.1 Required Mobile Device Service Offerings

The following table summarizes the required use of the Mobile Device Management (MDM) and Mobile Application Management (MAM) service offerings from the Office of Administration, Office for Information Technology (OA/IT) for Mobile Devices. Refer to OPD- SEC035A *Mobile Device Management Configurations (authorized CWOPA personnel only, contact RA-ITCentral@pa.gov for requests)* 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 waiver for an alternative.	Agencies must leverage OA/IT service offering or obtain and submit an approved waiver for an alternative.
Privately Owned devices / Bring your own device (BYOD)	Not Applicable	Users with Privately Owned devices shall be required to use MAM for Commonwealth applications to prevent disclosure of Commonwealth Data.

3.2 Commonwealth-Issued Mobile Devices

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

Agencies that do not elect to leverage the OA/IT service offering must have a documented and OA/IT approved alternative approach that includes a security management plan with the approved ITP waiver to meet the policy requirements in Section 4.

3.2.1 Supported Mobile Devices

OA/IT 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/IT service offerings.

3.2.2 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.

3.2.3 Interconnected Devices and Wearables

Agencies shall 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 shall be reviewed for privacy concerns with data that is transferred and/or stored. All applicable end-user license agreements (EULAs) shall be reviewed by legal counsel.

3.3 Privately Owned Mobile Devices

OA/IT MAM service offerings or an approved agency alternative mobile security solution is required for Privately Owned Mobile Devices (non-Commonwealth-issued devices).

Commonwealth applications are prohibited from being installed or utilized on Privately Owned Mobile Devices unless OA/IT service offering for MAM is installed and active on the Mobile Device as outlined in Section 4.1. Agency ISOs shall make final determination on appropriate use of Privately Owned Mobile Devices and the use of Commonwealth applications.

Connection of a Privately Owned Mobile Device to the Commonwealth or an agency network is strictly prohibited.

Authorized users shall fully understand that Privately Owned Mobile Devices utilized to access Commonwealth IT Resources may be seized and/or searched at the Commonwealth's discretion in connection with, but not limited to, a cyber security incident, or breach, e-Discovery, Right-to-Know Law, or non-compliance with Commonwealth policies. Policy guidance on these and other related requirements can be found in *ITP-PLT012, Use of Privately Owned Devices to Access IT Resources*. In addition, under no circumstances shall the Commonwealth be responsible to support or maintain the Authorized User's Privately Owned Mobile Device. Approval to utilize a Privately Owned Mobile Device shall not imply such a responsibility. Additionally, the Authorized User shall not be entitled to, nor receive assistance or reimbursement from the Commonwealth for configuration, installation, maintenance, repair or replacement of the Authorized User's Privately Owned Mobile Device.

NOTE: Authorized Users are permitted to access employee resources, such as

Employee Self Service (ESS), from their Privately Owned Mobile Device to obtain their own personal data, such as, but not limited to, pay statements, tax forms, benefit and leave information.

It shall only be utilized to conduct personal business and not utilized to conduct Commonwealth business such as, but not limited to, administrative, or job related activities/duties.

3.4 Mobile Application Management

MAM is used to distribute and manage Mobile Applications. Agencies must utilize the OA/IT service offering or obtain and submit an approved waiver for an alternative as outlined in Section 3.1.

3.5 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 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.

- 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. OA/IT shall maintain agency and business area specific application catalogs within the MAM/MDM primary service offering.

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

3.6 Mobile Email Management

Agencies requiring access to CWOPA (Exchange) email from Commonwealth–issued or Privately Owned (BYOD) Mobile Devices must use the OA/IT MAM Messaging (secure containerized email) service.

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.

4. Responsibilities

4.1 Agencies shall:

- Ensure any Commonwealth-issued Mobile Device connected to the Commonwealth network is either fully managed by OA/IT service offering or adheres to an agency mobility security policy that has been approved by OA/IT through the waiver review process per *ITP-BUS004, IT Waiver Review Process*.
- Ensure any Privately Owned Mobile Device utilizing messaging services is managed by OA/IT Mobile Application Management Services.
- Immediately report a lost or stolen Mobile Device or any compromise of data of a Mobile Device per ITP-SEC024, IT Security Incident Reporting Policy.
- Manage the IT, executive, and legal reviews of any third party applications that are being requested for use or deployment by the agency.

4.2 OA/IT shall:

- Manage the MDM and MAM service offerings and base configurations.
- Evaluate requests from multiple agencies for the same third-party mobile application, to determine if it should undergo legal and other applicable reviews and approval at the Enterprise level.

4.3 Third-party vendors, licensors, contractors, or suppliers shall:

- Implement a MDM solution to manage access and protect Mobile Devices in the event they are lost or stolen (if Mobile Device access to Commonwealth resources or data is permitted).

5. 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 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- OPD-SEC035A, *Mobile Device Management Configurations (authorized CWOPA personnel only, contact RA-ITCentral@pa.gov for requests)*
- *ITP-ACC001, Information Technology Digital Accessibility Policy*
- *ITP-BUS004, IT Waiver Review Process*
- *ITP-NET016, Wireless Cellular Data Technology*
- *ITP-PLT012, Use of Privately Owned Devices to Access IT Resources*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC005, Commonwealth Application Certification and Accreditation*

- *ITP-SEC024, IT Security Incident Reporting Policy*
- *ITP-SEC031, Encryption Standards*
- *ITP-SEC040, IT Service Organization Management and Cloud Requirements*
- *ITP-SEC041, Commonwealth IT Resources Patching Policy*

6. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

7. Publication Version Control

It is the Authorized 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 shall be directed to RA-ITCentral@pa.gov.

8. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy 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	N/A
Revision	07/19/2021	Updated Scope Updated policy reference/links Added third party vendors to Scope and Responsibilities section	N/A
Revision	05/23/23	Replaced definitions with links to the glossary where applicable Added third party vendor requirements to Responsibilities section consistent with OPD-SEC000B. Updated/added references. Removed reference and statement for MD 240.11 which was rescinded. Added compensating controls for cellular to Commonwealth network connected devices Updated third party application approvals and app store access Established requirement for MAM for BYOD devices	N/A
Revision	09/07/23	Replaced Personal Device, with Privately Owned device language, to be in line with PLT012. Linked to glossary for Privately Owned Device definition.	N/A

Version	Date	Purpose of Revision	Redline Link
		Removed MEM Column, as MEM functionality is provided by MAM solution. Clarified that Administrative actions in ESS, may not be performed on a Privately Owned Device. Added statement to prohibit connection to public wi-fi Added statement to prohibit connection of Privately Owned Mobile Device to COPA or Agency network. Added disclaimer statement from PLT012 regarding search and seizure of Privately Owned Mobile Devices in connection with cyber security incident, breach, e-Discovery, RTK Law, or non-compliance with COPA policy. Reference added to PLT012. Paragraph one regarding waiver process under previous section 4.2 Mobile devices moved under new section 4.2 Commonwealth issued Mobile Devices. Language regarding the prohibition of Promiscious mode while connected to the commonwealth network was moved under general policy language. Language regarding SIM cards removed, as this is covered in ITP-NET016 (soon to be ITP-TEL001) Reference to ITP-SEC041 and accompanying policy language regarding patching added. Added language around duplicative third-party applications under Mobile Applications.	
Revision	02/20/24	Re-added language removed during last revision on SIM cards.	Revised IT Policy Redline <02/20/2024>