Information Technology Policy

Wireless Cellular Data Technology

ITP Number ITP-NET016	**Effective Date** March 16, 2007
Category Network	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** June 2018

1. Purpose

This Information Technology Policy (ITP) covers wireless cellular data technology for the Commonwealth of Pennsylvania.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Definitions

Integrated Cloud Storage: A cloud-based storage integrated at the mobile device operating system level.

Mobile Communication Device (Mobile Devices): Any mobile phone, smartphone, or media tablet that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network.

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.

Mobile Device Service Plan: Any service agreement established with a cellular service provider to grant mobile device access to cellular networks for the transmission of voice and data traffic.

4. Policy

The use of cellular technology is governed by the Management Directive 240.11 *Commonwealth Wireless Communication Policy* and Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

Commonwealth agencies are to adhere to the Commonwealth Wireless Cellular Contract for the procurement of cellular services and equipment. Cellular data rates are variable based on location and vendor. It is recommended that agencies determine service requirements, availability of service, and data rates from the vendor before ordering the service. Mobile device service plans and equipment are procured through the Enterprise Services Management System (ESMS). Agencies are to regularly review their mobile plan details with their cellular service provider(s) to ensure the most cost effective plans are in place. At a minimum, annual reviews will be conducted with the agency provider(s).

All commonwealth mobile devices that are capable of mobile device management (MDM) must be enrolled in accordance with ITP-SEC035 *IT Mobile Device Security Policy*. End user devices using cellular connectivity may not connect directly to the commonwealth network except in cases where an approved COPPAR waiver for this ITP is in place.

Agencies are to ensure backup and storage of commonwealth mobile device data is in accordance with all policies, specifically ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*, ITP-SEC020 *Encryption Standards for Data at Rest*, and ITP-SEC031 *Encryption Standards for Data in Transit*. The use of integrated mobile device storage must follow the ITPs as it relates to commonwealth data protection.

Agencies are to manage lost or stolen devices in accordance with ITP-SEC024 *IT Security Incident Reporting Policy*.

5. Responsibilities

Office of Administration, Office for Information Technology (OA/OIT) is responsible for the management of the wireless contract and is the service owner for the commonwealth's mobile device management (MDM) system.

Commonwealth Agencies are responsible for the procurement of wireless service plans and devices and compliance with all Management Directives and ITPs.

6. Related ITPs/Other References

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*
- ITP-SEC000 *Information Security Policy*
- ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC020 *Encryption Standards for Data at Rest*
- ITP-SEC024 *IT Security Incident Reporting Policy*
- ITP-SEC031 *Encryption Standards for Data in Transit*
- ITP-SEC035 *IT Mobile Device Security Policy*

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

8. 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.

9. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

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

Version	Date	Purpose of Revision
Original	03/16/2007	Base Document
Revision	03/03/2011	Added ESMS reference for agencies to use for ordering cellular services
Revision	06/15/2017	ITP reformat Removed Background section Added Definitions Expanded Policy section Added References