MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania
Governor's Office

Subject: Commonwealth Wireless Communication Device Policy	***Number:*** 240.11 Amended
Date: April 11, 2012	***By Direction of:*** Kelly Powell Logan, Secretary of Administration

Contact Agency:
Office of Administration, Office for Information Technology, Telephone 717.787.5440

This directive establishes policy, responsibilities, procedures, and guidelines for the procurement, allocation, and use of wireless communication devices by Authorized Users of Information Technology (IT) Resources. Marginal dots are excluded due to major changes.

1. **PURPOSE.** To establish policy, responsibilities, procedures, and guidelines for the procurement, allocation, and use of wireless communication devices by Authorized Users of IT Resources.

2. **SCOPE.** This directive applies to all Authorized Users who utilize or have access to IT Resources via a wireless communication device.

3. **OBJECTIVE.** To assist agencies in achieving maximum productivity and cost-effectiveness when employing wireless communication technology as a business solution and effectively managing the usage of these devices by Authorized Users of IT Resources.

4. **DEFINITION.**

   a. **Authorized Users.** Commonwealth of Pennsylvania employees, contractors, consultants, volunteers or any other user who utilizes or has access to IT Resources.

b. Connection. Includes remote access system (RAS), a tool used to connect remotely to the commonwealth network. Authorized Users may need to connect to the network from home or another remote location, to perform their job functions. Remote access is coordinated by the Office of Administration, Office for Information Technology (OA/OIT), and users must have the Cisco virtual private network (VPN) client on their computer and a valid digital certificate. Connection does not include connecting with Authorized User devices to Office Outlook Web Access.

c. IT Resources. Commonwealth IT Resources include, but are not limited to, the following: the commonwealth's computer systems, together with any electronic resource used for communications, which includes, but is not limited to laptops, individual desktop computers, wired or wireless telephones, cellular phones, pagers, beepers, personal data assistants and handheld devices, and, further, includes use of the internet, electronic mail (email), instant messaging, texting, voice mail, facsimile, copiers, printers or other electronic messaging through commonwealth facilities, equipment or networks (collectively "IT Resources").

d. Telecommunication Management Officer (TMO). A commonwealth employee designated by the agency head to oversee the communications services of the agency and/or worksite.

e. Wireless Communication Devices. A device that transmits and receives data, text, and/or voice with a wireless connection to a network. This definition includes; but is not limited to, such devices as satellite and cellular telephones, pagers, wireless internet services, wireless data devices, wireless laptops, and cellular telephone/two-way radio combination devices. This definition does not include the radio devices that interface with the 800 MHz Statewide Radio System.

5. POLICY.

a. Commonwealth Issued Wireless Communication Devices.

(1) Agency procurement of commonwealth issued wireless communication devices and subscription services shall be in strict adherence with the contractual agreement between the commonwealth and its wireless communication device service providers. No wireless communication device shall be purchased from vendors outside an approved statewide contract, unless a waiver has been granted by OA/OIT. The terms of these agreements have been carefully negotiated and any variances from the standards created in each contract may lead to erosion of value and cause agencies to incur additional and unnecessary costs. Agency comptrollers should not approve expenditures for commonwealth issued wireless communication devices that fall outside the scope of an approved statewide contract, without a waiver from OA's, Deputy Secretary for Information Technology.

(2) Allocation of commonwealth issued wireless communication devices shall be determined as operationally necessary by the agency head and the agency deputy secretary with operational responsibility for the management of wireless communication devices. (For allocation guidelines refer to Enclosure 1, Guidelines for Wireless Communication Device Allocation.)

(3) Agencies are responsible for controlling and managing the use of commonwealth issued wireless communication devices and related services. All usage must comply with all applicable federal laws, state laws, and commonwealth rules and regulations. Any improper use of commonwealth issued wireless communication devices may result in Authorized User disciplinary action up to and including termination, if applicable.

(4) The allocation and use of wireless technology is not an entitlement for an Authorized User. There is no requirement that an Authorized User be issued a commonwealth wireless communication device.

(5) Agencies are required to work with OA/OIT for the issuance of client access licenses and services to connect wireless devices. (Refer to Information Technology Bulletin (ITB) ITB-SYM007, Procedures for Deploying Wireless Communication Devices in Commonwealth Agencies).

(6) The use of commonwealth issued wireless communication devices is intended for commonwealth business purposes. Please refer to *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy* on appropriate use of commonwealth IT Resources.

(7) A commonwealth issued wireless communication device is only to be used by the Authorized User to whom it is issued. Access to commonwealth IT Resources via non-commonwealth issued wireless communication devices is limited to Authorized Users.

(8) Authorized Users of a commonwealth issued wireless communications device are subject to compliance with the *Right to Know Law, 65 P.S.SS67.101-67.3104* as outlined within *Management Directive 205.36, Right-to-Know Law Compliance*.

(9) Authorized Users of a commonwealth issued wireless communications device are subject to any eDiscovery requests.

(10) Authorized Users with commonwealth issued wireless communication devices are not to alter the terms of the commonwealth wireless agreement in any way without consultation with TMO. Individual plan or feature changes must be made by the TMO.

(11) Authorized Users of commonwealth issued wireless communication devices should not place their cellular telephone numbers on their business cards unless the agency has entered into an appropriate agreement with the carrier to receive volume cost discounts. Authorized Users should work with their agency TMO prior to providing this information publicly.

(12) With the exception of renewals of existing service plans and devices, no Authorized User is permitted to exchange, upgrade, or substitute his/her commonwealth issued wireless communication device without approval of the agency deputy secretary.

(13) Each agency issuing wireless communication technology is to employ an allocation process based upon Enclosure 1, Guidelines for Wireless Communication Device Allocation. Every Authorized User with a commonwealth issued wireless communication device must sign Enclosure 2, Wireless Communication Device Justification and Acknowledgement, stating the Authorized User is aware of and understands this wireless communication policy and his/her wireless communication plan. The agency deputy secretary or equivalent must also sign Enclosure 2, Wireless Communication Device Justification and Acknowledgement, in which the agency deputy secretary or equivalent acknowledges that the wireless communication device was issued to the Authorized User based upon one or more of the guidelines set forth in Enclosure 1, Guidelines for Wireless Communication Device Allocation. A copy of this documentation will be maintained in the employee's Official Personnel Folder as prescribed in *Management Directive 505.18, Maintenance, Access, or Release of Employee Information* or with the agency TMO office for non-commonwealth employees.

(14) Agency TMOs are responsible to monitor the appropriateness of the use of commonwealth issued wireless communication devices and the costs related to that usage.

b. Non-Commonwealth Issued Devices.

(1) Connection of non-commonwealth issued wireless communication devices to commonwealth IT Resources is voluntary for any Authorized User and shall be determined as operationally necessary by the agency head and the agency deputy secretary with operational responsibility for the management of wireless communication devices. (For allocation guidelines refer to Enclosure 1, Guidelines for Wireless Communication Device Allocation.)

(2) The approval of connection of a non-commonwealth issued wireless communication device to the commonwealth IT Resources is not an entitlement for an Authorized User.

(3) There will be no reimbursement to Authorized Users for use of a personal wireless device related to commonwealth business.

(4) Agencies are responsible for controlling and managing the use of wireless communication devices and related services regardless of whether the device being used is commonwealth issued or non-commonwealth issued.

(5) All business related usage on an Authorized User's device must comply with all applicable federal laws, state laws, and commonwealth rules and regulations. Any improper business use (as defined in *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*) of non-commonwealth issued devices may result in disciplinary action up to and including termination.

(6) Authorized Users who use non-commonwealth issued wireless communication devices to connect to commonwealth IT Resources are subject to compliance with the *Right to Know Law, 65 P.S.SS67.101-67.3104* as outlined within *Management Directive 205.36, Right-to-Know Law Compliance*.

(7) Authorized Users who use non-commonwealth issued wireless devices to connect to commonwealth IT Resources may be subject to eDiscovery.

(8) Agencies are required to work with the OA/OIT for the issuance of client access licenses and services to connect non-commonwealth issued wireless devices to IT Resources. (Refer to ITB-SEC035, Mobile Devices Security Policy.)

(9) An Authorized User seeking to utilize a non-commonwealth issued wireless communication device to access commonwealth IT Resources must sign Enclosure 4 - Authorized User Acknowledgement for Non-Commonwealth Issued Wireless Communication Device, certifying:

(a) adherence to established commonwealth policy;

(b) compliance with terms of their respective subscription plans; and,

(c) agreement to utilize a non-commonwealth issued wireless communication device to access commonwealth IT Resources, in lieu of a commonwealth issued wireless communication device.

(10) A copy of this documentation will be maintained in the employee's Official Personnel Folder as prescribed in *Management Directive 505.18, Maintenance, Access, or Release of Employee Information* or with the agency TMO office for non-commonwealth employees.

c. Wireless Device Security.

(1) When using wireless communication devices, security can be compromised. Authorized Users are to use caution and good judgment when communicating sensitive information via wireless devices. In the event that any wireless communication device that connects to commonwealth IT Resources or stores commonwealth data is compromised, lost, or stolen, it is the responsibility of the Authorized User to immediately report the incident to his/her supervisor so that procedures defined in *ITB-SEC024, Information Technology Security Incident Reporting Policy* can be followed and compliance with *Management Directive 240.12, Commonwealth of Pennsylvania Mobile Devices Security Policy* will be maintained.

(2) Authorized Users shall inform their agency TMO when they change or end service of commonwealth issued and non-commonwealth issued wireless communication devices that connect to commonwealth IT Resources.

(3) Authorized Users are to be aware of the dangers associated with driving while using wireless communication devices, which can distract a driver's attention from the primary job of responsible driving. Authorized Users are required to obey all local, state, and federal laws related to the use of wireless communication devices while driving. Employees are strongly encouraged to avoid using wireless devices while driving, particularly while driving a commonwealth vehicle.

6. RESPONSIBLITIES.

a. Agency Deputy Secretaries or Designees, with the operational responsibility for the management of wireless communication devices, are authorized to allocate wireless communication devices as deemed operationally necessary and monitor usage and costs associated with each device for their subordinate bureau directors.

b. Agency Bureau Directors or Equivalent, with the operational responsibility for the management of wireless communication devices, are authorized to allocate wireless communication resources as deemed operationally necessary and monitor usage and costs associated with each device for their subordinate employees.

c. Office of Administration, Office for Information Technology, shall establish, maintain and administer an enterprise solution to support the connection of wireless communication devices to commonwealth email, data, and other required applications; and, in addition, provide guidance and procedures for mitigating security risks associated with wireless communication devices.

d. Telecommunication Management Officer, shall work with OA/OIT and the Authorized User to configure the connection of wireless communication devices to commonwealth email, data, and other required applications in compliance with all related ITBs.

7. REFERENCE(s).

a. *Management Directive 240.12, Commonwealth of Pennsylvania Mobile Devices Security Policy*.

b. *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

c. *Management Directive 205.36, Right-to-Know Law Compliance*.

d. *ITB-SEC024, Information Technology Security Incident Reporting Policy*.

This directive replaces, in its entirety, *Management Directive 240.11* dated October 8, 2004.

Enclosure 1 - Guidelines for Wireless Communication Device Allocation
Enclosure 2 - Wireless Communication Device Justification and Acknowledgement
Enclosure 3 – Authorized User Acknowledgement for Commonwealth Issued Wireless Communication Device
Enclosure 4 - Authorized User Acknowledgement for Non-Commonwealth Issued Wireless Communication Device

GUIDELINES FOR WIRELESS COMMUNICATION DEVICE ALLOCATION

Agencies are to closely manage allocation of wireless communication devices to Authorized Users and scrutinize the subscription plans, usage and costs associated with each device.

Each agency head and agency deputy secretary or equivalent with the operational responsibility for the management of wireless communication devices is authorized to allocate wireless communication resources as deemed operationally necessary.

Authorized Users should meet one or more of the following guidelines in order for a wireless communication device to be assigned:

- The duties of the position are such that immediate emergency response is critical to successfully carrying out the job (e.g., police officer, fire or emergency responder, etc.).

- The duties of the position require response and decision-making to life threatening or other public safety issues and situations.

- The duties associated with the position make it necessary that the incumbent be accessible to communicate with agency senior management at any time.

- The duties of the position require a significant amount of travel during regular work hours, making the wireless device a productivity enhancement tool.

- The duties of the position may lead to potentially dangerous scenarios and situations and there is no acceptable and reliable alternative communication system.

Please refer to the cost guidelines published by OA/OIT to assist in the selection of the appropriate device for the Authorized User.

NOTE: The agency head, agency deputy secretary or equivalent with operational responsibility for the management of wireless communication devices will have the final approval of any wireless communications devices and may grant exceptions from the above criteria on a case-by-case basis. These unusual exceptions must be approved through appropriate agency documentation, as are all other allocated wireless communication devices.

WIRELESS COMMUNICATION DEVICE JUSTIFICATION AND ACKNOWLEDGEMENT

As Deputy Secretary (or equivalent) for

_____

I am authorizing

____the issuance of a commonwealth issued wireless communication device; or

____the connection to commonwealth IT Resources via a non-commonwealth issued wireless communication device for one or more of the following reason(s):

- The duties of the position are such that immediate emergency response is critical to successfully carrying out the job (e.g., police officer, fire or emergency responder, etc.).
- The duties of the position require response and decision-making to life threatening or other public safety issues and situations.
- The duties associated with the position make it necessary that the incumbent be accessible to communicate with senior management at any time.
- The duties of the position require a significant amount of travel during regular work hours, making the wireless device a productivity enhancement tool.
- The duties of the position may lead to potentially dangerous scenarios and situations and there is no acceptable and reliable alternative communication system.

_____ for _____
(Type of Device) (Authorized User)

Approval of this allocation indicates that this action is financially feasible within the agency budget.

Signature: _____ Date:_____

AUTHORIZED USER ACKNOWLEDGEMENT for COMMONWEALTH ISSUED WIRELESS COMMUNICATION DEVICE

I, the undersigned, an Authorized User of _____, of the Commonwealth of Pennsylvania, hereby acknowledge that I have received, read and understand the Wireless Communications Device Policy (*Management Directive 240.11*) and the applicable subscription plan. I agree that I am bound by the terms of the policy and the subscription plan and that I will adhere to the policy and comply with the terms of the subscription plan. I understand that my failure or refusal to comply with the policy and/or subscription plan may result in the loss of the privilege of the use of a commonwealth issued wireless communication device, and that I may be subject to discipline related to the acceptable use of IT Resources in accordance with *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

Name: _____
(Print)

Signature: _____ Date:_____

AUTHORIZED USER ACKNOWLEDGEMENT FOR NON-COMMONWEALTH ISSUED WIRELESS COMMUNICATION DEVICE

I, the undersigned, an Authorized User of _____, of the Commonwealth of Pennsylvania, hereby acknowledge that I have received, read and understand the Wireless Communications Device Policy (*Management Directive 240.11*) and the applicable subscription plan. I agree that I am bound by the terms of the policy and the subscription plan and that I will adhere to the policy and comply with the terms of the subscription plan.

I understand that although the commonwealth could provide a wireless communications device for me, I have declined such offer and have instead opted of my own volition to utilize my own non-commonwealth issued wireless communication device to connect to commonwealth IT Resources, and further, agree to the following:

- I will work with my TMO to ensure the proper configuration, obtain an agency purchased license to support the use of my device and keep current with the software license that allows me to connect to commonwealth IT Resources.

- I am solely responsible for backing up my personal content and non-commonwealth applications on my device.

- I am solely responsible for the cost of my personal device and voice/data plans, even if that cost increases due to use of the device for commonwealth business purposes.

- If my device has been lost, stolen or otherwise determined to compromise the security of commonwealth IT Resources, it may be wiped. If this occurs, or it is wiped by mistake, I will not pursue any litigation against the commonwealth.

- The use of my personal device's connection to commonwealth IT Resources may be subject to monitoring for compliance with *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

I understand that my failure or refusal to comply with the policy may result in the loss of the privilege of the use of commonwealth IT Resources and I may be subject to discipline related to the acceptable use of IT Resources in accordance with *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

Name: _____
(Print)

Signature: _____ Date:_____