MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania
Governor's Office

Subject: Commonwealth of Pennsylvania Mobile Devices Security Policy	***Number:*** 240.12
Date: December 29, 2008	***By Direction of:*** Naomi Wyatt Naomi Wyatt, Secretary of Administration

Contact Agency: PA Office of Administration, Bureau of Enterprise Architecture, (717) 772-8062

This directive establishes policy for the use and security of mobile devices in the Commonwealth.

1. **PURPOSE.** To establish employee and agency obligations when using mobile devices to access Commonwealth IT resources.

2. **SCOPE.** All authorized users in all agencies under the Governor's jurisdiction who have access to Commonwealth mobile devices as set in *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy.*

3. **OBJECTIVE.** To mitigate the risks of improper use and/or handling of mobile devices that can result in the loss or compromise of Commonwealth information or subject Commonwealth information systems to malicious software, programs or code.

4. **DEFINITIONS.**

   a. **Mobile device.** A device easily removable and stores data that can be connected to the Commonwealth network, workstation or other computing device via cable, Universal Serial Bus (USB), Firewire (IEEE 1394), I-LINK, infrared, radio frequency, personal computer memory card international association (PCMCIA), or any other external connection that would allow data to be transferred and removed (ITB-PLT011)**.** Mobile devices include, but are not limited to smart phones, laptops, tablets, zip drives, floppy diskettes, recording and re-writeable compact disks (CD), recordable and re-writeable digital video disks (DVD), USB flash digital media devices (thumb drives), memory sticks/cards, PC card storage devices of all types and external hard drives.

   b. **ISO.** Information Security Office

5. POLICY.

a. No mobile device may store or transmit non-public or sensitive information without protective measures approved by the agency 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 computing devices.

b. Mobile devices are not to be left unattended. Whenever possible, mobile devices are to be secured from access by unauthorized persons, through the use of locking devices, passwords, or other appropriate protection.

c. The improper use of mobile devices may result in disciplinary action ranging from a warning to dismissal from Commonwealth employment, depending on the circumstances of the incident. When warranted, the Commonwealth or its agencies may pursue or refer matters to other authorities for criminal prosecution against persons who violate local, state, or federal laws related to the use of mobile devices.

6. RESPONSIBILITIES.

a. Agencies:

(1) shall establish protective measures to avoid the unauthorized access to, or disclosure of, the information stored and processed by mobile devices (e.g., use of cryptographic techniques).

(2) must ensure that all mobile devices are first scanned for malicious code immediately upon connecting to a Commonwealth network and/or workstation. If antivirus scanning software is not configured to scan all files when accessed, procedures must be implemented to ensure authorized users manually scan media for malicious code before connecting to a Commonwealth network or workstation.

(3) are to provide training to Authorized Users who use mobile devices. This training, which will be developed by the Pennsylvania Office of Administration, will at a minimum be designed to raise awareness of the additional risks associated with these mobile devices and the controls that are to be implemented.

b. Authorized users shall ensure:

(1) information on mobile devices is not compromised;

(2) when using mobile devices in public places, meeting rooms, and other unprotected areas that they are particularly cautious to avoid the risk of unauthorized persons viewing information on the display screen;

(3) devices are not checked into airline luggage systems, with hotel porters, or with other unsupervised handling or storage processes. Mobile devices are to remain in the possession of the authorized users at all times unless other arrangements are required by a governmental authority;

(4) that they immediately report a lost or stolen mobile device containing sensitive information to the agency ISO or designee, in accordance with *ITB-SEC024.*

7. PROCEDURES.

a. ***Guidelines for Deploying Blackberry Devices in Commonwealth Agencies*** - *ITB-PLT003*

b. Guidelines to Prevent Unauthorized Access

(1) *ITB-PLT011 - Mobile Device Policy and Standards*

(2) *ITB-SEC020 - Encryption Standards for Data at Rest*

(3) *ITB-SEC031 - Encryption Standards for* Commonwealth of Pennsylvania Mobile Devices Security Policy *Data in Transit.*

c. Guidelines for to Malicious Software Scan

(1) *ITB-SEC001 - Enterprise Host Security Software Suite Standards and Policy*

d. ***IT Security Incident Reporting Policy –*** *ITB-SEC024*

8. OTHER RELATED POLICY.

(1) *ITB-SEC007 - Minimum Standards for User IDs and Passwords*

(2) *Management Directive 205.34 - Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.