GENERAL ORDER

Subject
Mobile Device Security

Topic	Series	Number
SPT	**302**	**10**

Effective Date
February 21, 2007

DISTRICT OF COLUMBIA

I. BACKGROUND

The use of laptop computers and other mobile electronic devices (MEDs) provide flexibility and enhanced communication that allow Metropolitan Police Department (MPD) members to be more productive. Conversely, the use of these devices outside of Metropolitan Police Department offices pose risk to the device, the information it contains and may also present a hazard to other Metropolitan Police Department resources when returned for use at Metropolitan Police Department offices (i.e., by spreading computer viruses obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of the Metropolitan Police Department that may lack the security provided by the Metropolitan Police Department's agency firewall and other perimeter protections. Therefore, additional security measures have been implemented to mitigate increased security risks presented by mobile computing.

II. POLICY

The policy of the Metropolitan Police Department is that reasonable measures will be taken to protect "law enforcement sensitive and/or personal privacy data" stored on mobile electronic devices, consistent with applicable District of Columbia laws and policies.

III. DEFINITIONS

When used in this directive, the following terms shall have the meanings designated:

1. Mobile Electronic Device (MED) – Any portable electronic device with the capability of accessing or storing sensitive data. Examples of such devices include, but are not limited to laptop computers, personal data assistants (PDAs), blackberry devices, pagers, USB flash storage devices, smartphones, digital cameras, and external hard drives.

2. Member – Civilian and sworn personnel employed by the Metropolitan Police Department. This term also includes all contract personnel actively associated with MPD.

3. Sensitive Data – MPD personnel records, files (i.e., data such as employee names or social security numbers) and data used for law enforcement or law enforcement related financial activities. This data is confidential in nature, may be qualified by the term “For Official Use Only” and should not be released to the public.

4. Portable Storage Device (PSD) – Any portable electronic device with the capability of accessing or storing sensitive data. Examples of such devices include, but are not limited to: laptop computers, personal data assistants (PDAs), blackberry devices, pagers, USB flash storage devices, digital cameras, and external hard drives.

IV. REGULATIONS

A. Sensitive data owned by MPD shall not be stored on any MED that is not managed by the MPD.

B. All MEDs used to store sensitive data shall utilize password protection and data encryption.

C. Members shall not share passwords with any other person.

D. Members shall not permit anyone who is not an MPD member to use or access MPD-owned or leased MED equipment.

E. Members shall not disable or tamper with security controls installed on MPD owned or leased MED equipment.

F. Personnel records and information for a given MPD member shall be maintained and accessed in accordance to GO-PER 201.19 (Employee Personnel Records).

G. Members shall report lost or stolen MED equipment to a supervisory official and then to the Synchronized Operations Command Center (SOCC) within 1 hour of loss, in addition to procedures outlined in GO-PER-110.11 (Uniforms and Equipment).

V. PROCEDURAL GUIDELINES

A. All MPD members provided with MPD-owned or leased MED equipment shall ensure the physical security of the equipment at all times.

1. MED equipment shall not be left unattended in public spaces.

2. Members shall secure and store MEDs and PSDs as outlined in GO-PER 110.11.

3. When using MED equipment during travel, member(s) shall make all reasonable efforts to secure the equipment, and shall ensure

equipment contents are not displayed or accessible when unattended in hotels or meeting rooms.

B. Notification of lost or stolen MED or PSA equipment

1. If an item is lost outside of the District of Columbia, member(s) shall complete an offense/incident report in that jurisdiction within one hour of occurrence. Members shall follow the procedures in Section IV., G and complete PD Form 43, (Report of Damage To or Loss of District Government Property) as outlined in GO-PER 110.11. The member must ensure that a description of any sensitive data known to be stored on the device is included in the Statement of Facts section of the PD Form 43.

2. In the event that the individual responsible for completing the PD Form 43 is incapacitated or otherwise unavailable to complete the form, a supervisory official shall complete the form and make the required notifications.

3. SOCC members shall:

   a. If the device is a laptop or a portable storage media device, contact the MPD Office of the Chief Information Officer (OCIO) member on-call and provide the offense/incident report information.

   b. If the device is managed by the Telephone Support Unit (smart phone, pager, etc.) notify the Telephone Support Unit and provide the offense/incident report information.

4. Personnel assigned to the Office of the Chief Information Officer (OCIO) shall:

   a. Verify that the individual making the report was actually issued the subject device.

   b. Upon successful verification of the member or supervisor, OCIO will take actions to disable the subject device access to MPD networks and activate device tracking procedures.

5. The Telephone Support Unit shall verify that the individual making the report was actually issued the subject device, and take actions to disable the subject device access to MPD networks.

C. When an MPD owned or leased MED is lost and the member responsible for completing the PD Form 43 is incapacitated (i.e., illness or injury) or otherwise unavailable to complete the form, a supervisory official shall make the notification to the SOCC and follow procedures outlined in GO-PER 110.11.

D. The Chief Information Officer, (CIO) shall:

1. Provide authorization for all laptop computer operating system configurations.

2. Ensure that all laptops are configured to prevent additional application installations without prior approval from the OCIO.

3. Ensure that equipment is issued with only the minimum applications required by the member to fulfill their MPD business responsibilities. All laptop communications ports not required for business use by the member shall be disabled. This includes IrDA (infrared) ports and Bluetooth connectivity. The laptop wireless channel (802.11 a,b,g) shall remain enabled, but shall be switched off unless needed.

4. Ensure media storage is encrypted using software compliant with Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules (FIPS 140-2), Level 1. This requirement specifically includes all data written to the computer's internal hard drive, DVD RW or CD RW drive, and any external storage device attached to the computer, (e.g. USB flash drive, external hard drive, etc.).

5. Ensure equipment includes antivirus, anti-spyware, and personal firewall software managed by the OCIO.

6. Ensure equipment includes device tracking software managed by the OCIO.

7. Ensure that all laptops and other mobile computing devices are inventoried to include, at a minimum, the following information:

   a. The name, manufacturer, serial number, and date of issuance of the subject device.

   b. The name, unit, phone number, and email address of the equipment recipient.

   c. The tracking data must be continuously available to on-call personnel for purposes of loss/theft verification and response.

VI. CROSS REFERENCES

1. GO-SPT 110.11 (Uniforms and Equipment)

2. GO-PER 201.19 (Employee Personnel Records)

//SIGNED//
Cathy L. Lanier
Acting Chief of Police

CLL:SOA:DAH:DEP:pe:phc:pas