
	<b>GAITHERSBURG POLICE DEPARTMENT</b>			
	<b>GENERAL ORDER 1107.1</b> <b>Seizing Computers and Equipment</b>			
	<b>GENERAL ORDER</b>	<b>1107.1</b>		<b>Related CALEA Standards:</b>  <b>83.2.1, 83.2.5, 83.3.2</b>
	<b>Effective Date</b>	<b>03/19/2015</b>		
<b>Authorized by:</b>	<b>Mark P. Sroka</b> CHIEF OF POLICE	SIGNATURE	DATE	

**I. DEPARTMENT POLICY**

The purpose of this directive is to establish basic guidelines and procedures for officers who encounter situations involving the need to seize computer equipment for evidentiary reasons or other official purposes.

The proliferation of computer usage and the constantly changing world of technology not only enhances the quality of life for law abiding citizens, but also provides an instrument for potential criminal conduct.

Since computers come in many forms, officers must be mindful of the information stored by computers and the data processing capabilities of them.

**II. PRECAUTIONS**

**A. Shut Down**

1. When dealing with computer systems, officers must be mindful of proper handling sequences and procedures as the system could be programmed to automatically erase data if improperly shut down or turned off. Therefore, officers should follow the procedures listed in section III of this directive and contact qualified personnel.

**B. Activation**

1. When turning on or *booting* a system, the possibility exists that a computer system may have been pre-programmed to erase or destroy data if certain start-up procedures are not followed. Therefore, officers will follow the procedures listed in section III of this directive.

**C. Availability of Technical Assistance**

1. During business hours, Investigators from the Montgomery County Police Computer Crimes Unit are available to assist officers with questions regarding computer crimes, seizure techniques, etc.

2. After hours, MCP Computer Crimes investigators can be reached through the Public Safety Communications Center or at the number listed for them in the General Orders Phone Number WIP.xlsx.
3. Investigators from the Maryland State Police Computer Crimes Unit are available to assist officers. After hours, they can be reached through the Public Safety Communications Center or at the number listed for them in the General Orders Phone Number WIP.xlsx.
4. Depending upon the type of case and advance notice they receive (preferably at least one week prior to the raid), MSP investigators will accompany officers on Search and Seizure Warrant execution, and can assist with case preparation, packaging, and labeling of evidence, etc.

### **III. PROCEDURES**

#### **A. Planned Seizures**

1. Officers planning an operation that could result in the seizure of computer related evidence will obtain the services of personnel who have had formal computer seizure training (i.e., MCP or MSP Computer Crimes investigators).
2. When personnel with formal training are not available to assist at the scene, officers planning the seizure should contact the Computer Crimes Unit by phone for technical guidance prior to the seizure.
3. If computer crimes investigators are unavailable altogether, officers seeking guidance should contact the State's Attorney's Office.

#### **B. Search Warrants**

1. For the purpose of applying for, obtaining, and executing a Search Warrant for computers and related devices, all are treated the same as any other piece of evidence.
2. To seize and search a computer database, the search warrant must specify the items to be seized and searched.
3. All computer hardware and software should be included, keeping

in mind the entire system is necessary to replicate the suspect's use of it and to enable forensic examination of the system.

4. Officers are cautioned to consult with a member of the MCP or MSP Computer Crimes Units, or the State's Attorney's Office, in the event the computer or electronic storage media to be seized may involve legitimate business records or intellectual property.

**C. Stand-Alone Computer (Non-Networked)**

1. For computer equipment which appears to be turned off:
  - Move people away from the computer and contact Computer Crimes Units.
2. For computer equipment which appears to be turned on:
  - Move people away from the computer and power supply.
  - Do not touch the keyboard or mouse.
  - Record what is on the screen by photograph or other means.
  - Contact Computer Crimes Units.

**D. Networked or Business Computers**

1. Officers will consult with Computer Crimes Investigators, or other personnel with formal training and expertise when dealing with networked or business computers, a computer network, mainframe or mainframe terminal.
2. Officers should not pull the plug as this could damage the system and/or disrupt legitimate business.

**E. Packaging/Labeling Evidence**

1. Each item seized must be properly marked, labeled and/or packaged.
2. Large items such as monitors, keyboards and system units (CPU) (normally containing the hard drive) may be tagged or labeled rather than bagged (although completely covering or wrapping the CPU is preferable).

3. Small items such as removable media must be bagged/boxed, tagged and sealed.
4. Each individual item inside the bag or box must be marked sufficiently to connect the item to that bag or box, i.e. (CR Number, owner or suspect name, etc).
5. Bags used for electronic evidence items are to be paper or static-free plastic bags.
6. All evidence will be handled in accordance with 1100 series general orders, lab protocols and with advice from computer crimes trained personnel.

**F. Protecting Evidence**

1. During transportation and storage of computers and related electronic devices, officers must avoid external magnetic sources ( i.e., placing near the speaker of police radios in a vehicle), extreme temperatures and other possible contaminants.
2. Do not use fingerprint powder on optical discs or other computer media, as the presence of fingerprint powder may render forensic data examination impossible.
3. If other physical forensic evidence is present on these items, consult with Computer Crimes Unit investigators.

**G. Other Procedures**

1. Officers may submit seized computer equipment for laboratory examination if all laboratory procedures are followed.
  - *If submitting to the Maryland State Police, officers should first contact the MSP Computer Crimes Unit to ensure proper packaging and form completion to document chain of custody and to tell lab personnel the reasons the equipment is being submitted.*
  - *If submitting to the Montgomery County Police, officers should first contact the MCP Computer Crimes Unit to ensure appropriate handling.*
2. Officers seizing (or anticipating the seizure of) computer systems should contact the State's Attorney's Office prior to seizing any work product or documentary materials from a suspect if it is

reasonably believed the materials are intended for public dissemination or publication.