# PALM BEACH GARDENS POLICE DEPARTMENT

## SEIZURE OF COMPUTER EQUIPMENT

## POLICY AND PROCEDURE 4.3.9.6

| Effective Date : | Accreditation Standards: | Review Date: |
|---|---|---|
| 11/15/11 | CALEA 83.2.5<br>CFA 35.05 | 07/01/2014 |

**CONTENT**



**PURPOSE**: To provide information and guidelines regarding the seizure of computer equipment.

**SCOPE**: This policy and procedure applies to all members.

**REVIEW RESPONSIBILITY**: Investigations Bureau Major

**POLICY**: It is the policy of this Department to ensure that potential evidence contained on or stored in computer based media is preserved and recovered in a manner consistent with the constraints of the United States Constitution, the Florida Constitution, and the rules of evidence.

**1. PROCEDURE**

a. Preparing for the Search and Seizure
   i. Using evidence obtained from a computer in a legal proceeding requires a search warrant or an exception to the search warrant requirement. A search warrant for the computer, associated equipment, and software should be obtained whenever possible. The Federal Guidelines for Searching and Seizing Computers, located in the detective division, can be used as a guide for the preparation of warrants and computer searches and addresses many legal and other issues regarding computer evidence.
   ii. Prior to searching the site, gather as much information as possible. Attempt to ascertain the user's level of knowledge and the environment in which the computer and equipment are located.
   iii. Whenever possible, in the case of a personal computer, a person trained in the seizure of computer evidence shall be involved in the seizure. In cases involving networked or business computers, a computer specialist or person trained in seizure of computer equipment must be consulted. Improper seizure of networked or business computers can result in damage to the system or the disruption of legitimate business.
   iv. On occasion, there may be a need to examine a computer on-site, e.g., when a person gives consent to a search without a warrant but will not allow the computer to be removed from the location. In such cases, a person trained in the examination of computer evidence shall conduct the examination on-site. If such examination reveals evidence of a crime, the computer may then be seized for safekeeping and a warrant obtained for further examination.

b. Conducting the Search and Seizure
   i. The first priority shall be officer safety.
   ii. Immediately restrict access to any computers and peripherals. Order all persons present at the location to move away from any computers or related equipment. Watch for anyone attempting to access computers or equipment.
   iii. Isolate any computers or related equipment from telephone lines and Ethernet cables because data on the computer can be accessed remotely. In most cases, this isolation can be accomplished by unplugging the phone line and Ethernet cables from the back of the computer.

iv. Preserve area for potential fingerprints and other evidence as appropriate.

c. Securing the Computer as Evidence
   i. If the computer is off, do not turn it on. Proceed to Step iii.
   ii. If the computer is turned on, **do not** turn it off. Photograph the screen, and then disconnect all power sources. If a person at the scene has accessed the computer and it appears to be destroying data, immediately disconnect all power sources. Do not attempt to open or view any files on the computer.
   iii. When disconnecting the power source, unplug the power cord at the back of the computer, then from the wall. If unplugged only from the wall and the computer has a battery back-up power source, the computer may continue to run.
   iv. Place evidence tape over each drive slot.
   v. Photograph and diagram all existing cables and connections.
   vi. Label all connectors and cable ends to allow re-assembly as needed.
   vii. Disconnect all connectors and cables.
   viii. Prior to transporting the computer and related equipment, package as fragile cargo.
   ix. Keep the computer and related equipment away from magnets and any equipment that generates a magnetic field.

d. Processing the computer evidence
   i. Only persons trained in the forensic examination of computers shall conduct examinations or other tests on a seized computer, related equipment or software.
   ii. The Department has personnel trained in the forensic examination of computers. Information Technology (IT) should be contacted to make arrangements for the examination of computer evidence. In the event IT cannot accomplish the examination, the Palm Beach County Sheriff's Office (PBSO) or Florida Department of Law Enforcement or the Federal Bureau of Investigation may be contacted.
   iii. Any time a computer, software or related equipment is turned over to another agency, normal evidence procedures used for such transfers shall be followed in accordance with Policy and Procedure 4.3.9.3.

e. Returning Seized Computers, Software and Related Equipment
   i. Anytime a computer, software or related equipment is cleared for return to the owner, such return shall be made as soon as possible. Any items that are not evidence, contraband, or property subject to seizure shall be returned to the owner.

f. Other devices containing data in electronic format
   i. Officers should be aware of other devices which may contain evidentiary data in electronic format. These devices may include portable USB drives (external, thumb drives, etc), digital cameras and recorders, cellular phones, etc.
   ii. In addition to the procedures described above that apply to these other types of devices; officers should follow the procedures in this section.
   iii. Any seizure of these devices must be in accordance with law, i.e., based on probable cause, warrant, consent, etc.
   iv. The power state of the device (on or off) should not be changed during the seizure unless the circumstances require doing so, e.g., unplugging an external hard drive.
   v. When available, the device's external power supply and any related cables/wires should be submitted along with the device.
   vi. The device shall be appropriately packaged to protect the device.
   vii. If the device is a cellular phone, it should be placed in an RF blocking bag, if available, to prevent remote wiping of the phone's memory. A "paint can" evidence container may also be used, but the device should be padded to prevent movement inside the can and possible damage.
   viii. The seizing officer should also be alert for any information at the scene, e.g., scraps of paper, containing passwords for the device.
   ix. The seizing officer shall contact Crime Scene to advise of any examinations requested and provide information as needed to facilitate the examination. Crime Scene will assist in arranging the examination by a qualified person.

x. The examination of any data contained on the device shall only be performed by a person who has received training in the proper extraction of data and data forensics. The extraction of data should only be done pursuant to a search warrant (preferred) or written consent. The seizing officer or assigned investigator, if any, shall be responsible for obtaining the warrant or written consent.

xi. These requirements do not preclude an officer from reviewing records on a phone such as a phone log or text messages when the officer has a reason for doing so, has received proper consent from the owner or person in lawful control of the device and there is no expectation that a forensic analysis will be necessary on the device.

2. **DEFINITIONS**:

**Computer** -Any internally programmed, automatic device that performs data processing.

**Computer Software** -A set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

**Computer Evidence** -Images, audio, text and other data as well as hardware.

---

**INDEX AS:**

- SEIZURE OF COMPUTER EQUIPMENT

**RESPONSIBILITY INDEX**

- INVESTIGATIONS BUREAU MAJOR
- SERGEANTS
- OFFICERS
- DETECTIVES

DRAFTED: SDD\WB / 11-15-11 FILED: 4.3.9.6.pdf

---

**APPROVED:**

11/15/2011

**Stephen J. Stepp** **Date**
**Chief of Police**