MONROE COUNTY SHERIFF'S OFFICE

General Order

CHAPTER: 034-C		TITLE: Computer Search and Seizure
EFFECTIVE DATE: August 19, 2009	**NO. PAGES:** 3	**REVIEWED/REVISED:** April 9, 2019
REFERENCE: CALEA 83.2.5		**RESCINDS:**
Sheriff of Monroe County		

I. PURPOSE: The purpose of this General Order is to establish a procedure to ensure the proper search and seizure of computer evidence.

II. SCOPE: Includes the search and seizure of computer equipment both in operating and non-operating models and all disks, drives, and peripheral equipment.

III. DEFINITIONS:

A. **Computer system:** computer monitor, central processing unit (CPU), hard drive, I/O (in/out) device, modem, CD-ROM or floppy drive configured to work together as a unit or cabled together externally.

B. **MCSO forensic computer examiner:** Office personnel who have received specific training on the proper techniques to examine and recover evidence from computers and storage devices.

C. **Peripherals:** Auxiliary devices, such as a printer, modem or storage system, that work in conjunction with a computer.

D. **Recording device:** CD-ROM, digital video disc, floppy disc, tape, zip, jazz, magneto-optical, or hard drive used to store data that is not currently connected to an operating system.

E. **Recording media:** Any disk, tape, cartridge or other type of media used to store data electronically (i.e. floppy disk, jazz cartridge, zip disk, jump drive, or magneto-optical disk).

IV. PROCEDURE: Searches and seizures of computer hardware and software shall be done in accordance with State and Federal Guidelines for searching and seizing computers.

A. Secure the scene

1. Deputy safety is of utmost importance
2. The area and equipment should be treated as a crime scene and preserved for potential fingerprints and/or DNA evidence
3. Immediately restrict access to the computer by any person
4. Isolate from phone lines (data on the computer(s) can be accessed remotely)
5. Remove wireless (Wi-Fi or Bluetooth) capabilities

6. Secure the computer as evidence and record serial numbers of each item

B. Computer operation status: Deputies shall not attempt to log on to the computer, operate the computer in any manner in an effort to use any software or explore files that may be contained on the media storage devices, retrieve e-mails, instant messages, etc.

1. If the computer is “ON” follow these steps for stand-alone computer (non-networked) systems.

    a. Consult with MCSO forensic computer examiner as needed to secure the computer system

    b. If you determine that the computer is running encryption software or Vista Operating System, contact MCSO forensic computer examiner before proceeding

    c. Do not turn off

    d. Do not enter any input from the keyboard or mouse

    e. Photograph the video screen display, computer system, surroundings and connections

    f. Label all cable connections and associated ports

    g. Disconnect the power source from the computer, not the wall outlet

    h. Disassemble the computer system and seize all cables and peripherals

    i. Package all seized property

    j. Do not place the computer equipment or related devices in a vehicle trunk during transport

    k. Do not use radios that produce strong magnetic fields around computers or while transporting them

2. If the computer is “OFF” follow these steps for stand-alone computer (non-networked) systems:

    a. Disconnect any telephone or modem connection

    b. Photograph the computer system, its surroundings and connections

    c. Label all cable connections and associated ports

    d. Disconnect the power source from the computer, not from the wall outlet

    e. Disassemble the computer systems and seize all cables and peripherals

    f. Package all seized property

    g. Do not place the computer equipment or related devices in a vehicle trunk during transport

    h. Do not use radios that produce strong magnetic fields around computers or while transporting them

C. Networks, business operations or online providers: Do not attempt to disconnect or recover any networked computer system or related device prior to consulting with the MCSO forensic computer examiner. Seize all investigation relevant related computer systems, recording devices,

recording media, tapes, papers, documents, manuals and notes in and around your crime scene (as indicated in search warrant or consent search).

D. Evidence Handling Procedures: All seized computer equipment evidence shall be reported, handled, and stored in accordance with Office procedures (General Orders, Chapter 54). Due to the nature of computer and electronic devices forensic analysis, the MCSO forensic computer examiners are authorized to maintain a temporary storage area for such equipment. The temporary storage area is only authorized for evidence submitted for computer/electronic examination and/or analysis and shall be secured to the level of all evidentiary property. A Deputy transferring computer equipment as evidence for review, examination or analysis will:

1. Complete a property receipt

2. Provide a copy of the search warrant, acknowledgment of consent or other documentation which authorizes the evaluation of the evidence to the MCSO forensic examiner

3. Upon completion of the computer/electronic device forensic analysis, the evidence shall be returned to the property division for evidentiary storage