JOPLIN POLICE DEPARTMENT	9-11 STANDARD OPERATING GUIDELINE
SUBJECT: Computer Investigations	**REVIEW DATE: Annually - September**
EFFECTIVE DATE: November 15, 2010	**ACTION DATE:**
AMENDS/SUPERSEDES: 9-11 September 30, 2008	**AMEND DATE: November 15, 2010**
ACCREDITATION INDEX: 83.2.5	**APPROVED:**  **Chief of Police**

I. POLICY

It is the policy of the Joplin Police Department to pursue the identification, investigation, and prosecution of persons who use computers in the furtherance of criminal activity. To ensure that this evidence is handled properly, only department employees who are trained in computer forensics shall seize and process computers, recording devices or recording media for the evidence contained therein. The Criminal Investigations Division shall be responsible for maintaining employees trained in computer investigations.

II. PURPOSE

To constitute general guidelines to govern the seizure of computers, recording devices, and recording media and subsequent forensic examinations by department personnel. (83.2.5)

III. DEFINITIONS

A. Computer Forensic Investigator

A sworn or civilian member of the department specifically trained in the techniques of computer data recovery and seizure. Successful completion of department-approved training shall constitute the required training. Other training received shall be evaluated on a case-by-case basis.

B. Computer System

Computer monitor, CPU, hard drive, I/O device, modem, CD-ROM, lap top computer, electronic notebook, smart phone or floppy drive configured to work together as a unit or cabled together externally.

C. Recording Device

CD-ROM, floppy drive, tape drive, zip drive, jazz drive, magneto-optical drive, cell phone, or electronic note book, used to store data that is not currently connected to an operating system.

D. Recording Media

Floppy disk, jazz, zip, or magneto-optical disk. Any tape or other type of media used to store data.

IV. PROCEDURES

A. When an investigator shall be utilized

This policy shall apply in those cases where data residing on computer systems, recording devices, and media are being sought as evidence in an investigation. Computers seized by department

personnel as fruits of crimes, (e.g. burglary, retail theft), shall be treated as normal evidence and processed according to the procedures in evidence and property management, and crime scene procedures. This type of seizure will not normally require the services of the Computer Forensic Investigator.

B. Procedure for seizure (83.2.5)

No department member, except those who have been trained, shall power off, disconnect, power on, or access a computer system, recording device or recording media that is to be seized. Computer systems can and have been found to contain destructive programs which can also alter file access dates that can be critical evidence.

1. When it is determined that a computer is to be seized and processed, the investigating officer at the scene shall note the operating status of the equipment which shall influence seizure proceedings.

    a. Should the computer system be off and its parts disconnected from one another and from a power source, the area shall be photographed, and the equipment may be removed and packaged.

    b. Should a computer system be connected to other unit components and/or a power source, the scene shall be secured from unauthorized access, and the system and surrounding area shall be photographed. No attempt shall be made by untrained personnel to access the system or otherwise power same down. The investigating officer shall contact the appropriate computer forensic investigator. The computer forensic investigator will assist in the seizure of the target system and media.

2. Exigent circumstances may cause immediate seizure of computer equipment by officers on scene. A properly trained employee should be consulted as soon as possible to assist.

3. In an effort to maximize the potential for meaningful data retrieval, the following procedural steps have been established, regarding the physical seizure of computer equipment.

    a. Photograph the general scene, computer monitor (including any on-screen display), and all electrical and computer connections.

    b. Power system down and disconnect from electrical outlets. There are times when it may be necessary to sever power to a suspect's computer, to prevent writing files to the hard drive. This shall be accomplished by disconnecting the power cord from the back of the computer, not from the wall. The Investigating Officer shall consult with the Computer Forensic Investigator or Supervisor prior to taking this action.

    c. Label all connectors prior to disassembly.

    d. Seize all available software and computer discs.

    e. Keep hardware units and connectors together.

    f. Record equipment identification numbers/descriptions.

    g. Transport hardware/software to the police department.

    h. Package software and tag hardware.

i. Computer laptops/towers shall be transported from the scene, by placing them on the back seat floor boards to prevent file corruption. **DO NOT TRANSPORT ANY COMPUTERS IN THE TRUNK OF A VEHICLE.**

j. Complete evidence tag(s) and enter items into evidence. All obscene materials shall be marked "Obscene" prior to being entered into evidence. Obscene refers to material depicting children under the age of 18, being in a state of undress, engaged in erotic poses or sexual activity.

k. Exit photographs shall be taken of the scene, and entered into evidence.

l. Prior to any electronic evidence being examined by computer forensic personnel, the requesting officer is responsible for completing the following:

Complete a Digital Evidence Examination Request Form and forward to the forensic examiner along with the legal justification authorizing the search of the seized media. Examples of proper legal justification are consent to search of electronic media form or search warrant. If a search warrant or written consent to search does not exist, the requesting official may forward an e-mail stating verbal consent was obtained by the authorizing party/property owner.

Outside agencies shall be required to submit a copy of the offense report as well as the above listed forms prior to examination.

4. If a cell phone is to be seized, officers should make attempts to do the following:

a. Locate the charger of the phone

b. Obtain any password that might be in use

c. Power down the phone and remove the battery

d. Package the phone, battery and charger together if possible in Anti-static material

e. Inform a cyber crimes detective of the seizure the day it is seized

5. Whenever possible, the department computer forensic investigator shall process seized systems, devices and media for evidence.

6. Other outside agencies such as the FBI, Treasury Department, etc. with the proper resources and training can be used in the absence of a department trained computer investigator. The trained department investigator may call upon additional assistance from these agencies if needed to assist in a case.

C. <u>Responsibilities of the computer forensic investigator</u>

The computer forensic investigator shall make all efforts to accomplish the following during the examination of the seized system and media.

1. Ensure the original media and data are maintained in their original unaltered state.

2. Ensure no unauthorized writes are made to the media by viruses, booby trap defense schemes, the operating system, write back applications or by other inadvertent means.

3. Recover, unlock and access deleted files, hidden data, password protection files and encrypted files.

4. Examine unallocated and slack space for relevant data.

5. Information, which may be obtained by a search of computer equipment, will be secured and documented as evidence according to the situation. Other data will be held with the computer until released by proper authorization.

6. When not being examined, ensure the integrity of potential evidence by either returning the seized system and media to the property room, or by securing the system and media in a locked storage unit approved by the chief of police.

7. Provide a report of findings to the case investigator as soon as possible.

8. While conducting forensic evaluations, or undercover investigations, the Computer Forensic Investigator shall ensure all precautions are taken, to secure all obscene materials and prevent it from being viewed by non-authorized personnel.

    a. The Computer Forensic Investigator's Office door will remain closed during these operations.

    b. A sign shall be affixed to the entrance to the office, instructing persons to knock on the door, prior to entering the office. The Investigator shall secure all obscene materials as soon as practically possible, prior to permitting access to the office.

D. Legal Consultation

In those instances where a question exists as to the legal justification regarding the seizure of computer components, or documentation derived therefrom, consultation should be made with the County Prosecuting Attorney's Office prior to any seizure being initiated.

E. Training

All investigators shall be trained in the proper methods to seize and properly package a computer system.

F. Authorized Access

The Joplin Police Department Cyber Laboratory shall be considered a secured area with authorized access only. No unauthorized personnel shall be permitted within the secure area without an escort. This location is considered an evidence storage facility. All personnel with the exception of the computer forensic examiner, cyber detective, special investigations supervisor and investigations bureau lieutenant, shall be recorded on an access log to include the date and time of entry and the date and time of exit from the laboratory. This log shall be maintained upon the entrance of the laboratory.

V. COMPLIANCE

Violations of this policy, or portions thereof, may result in disciplinary action as described in the City of Joplin's Personnel Rules or the Joplin Police Department's Rules and Regulations and General Orders.

Members of the Joplin Police Department, while assigned to or assisting other agencies shall comply with this policy.

VI. APPLICATION

This document constitutes department policy, is for internal use only, and does not enlarge an employee's civil or criminal liability in any way. It shall not be construed as the creation of a higher legal standard of safety or care in an evidentiary sense, with respect to third party claims insofar as the employee's legal duty as imposed by law. Violations of this policy, if proven, can only form a basis of a complaint by this department, and then only in a non-judicial administrative setting.

Southwestern Missouri Cyber Crime Task Force

Digital Evidence Examination Request Form

Submitting Agency: _____ Case Number: _____ Date: _____

Submitted By: _____ ID Number: _____

Contact Phone #s: Office #_____, Cell #_____, Fax #_____

Suspect's Name: _____ Race: _____ Sex: _____ DOB: _____

Victim's Name: _____Race: _____ Sex: _____ DOB: _____

Type of Crime:
_____

Brief synopsis of Investigation:
_____
_____
_____
_____

Item#	Description (make, model, type, capacity and/or serial number	Date Seized	Seized By

1. Describe in detail the evidence you expect to recover from the storage media or computer system submitted for forensic processing. List any special considerations:

_____
_____
_____

2. Do you have pictures or images of the suspect(s) and/or victim(s)? YES / NO If so attach them to this form.

3. Is a copy of your search warrant/consent form attached? YES / NO If not, why?

_____

4. Are you aware of any passwords, login's, email addresses or file encryption used? YES/NO If so, list them:

_____
_____
_____

5. If the suspect, witness, or other persons were interviewed, did they provide any useful information that will assist in the examination of the computer system or device submitted? YES / NO If so, please list or provide documentation.

_____
_____
_____
_____
_____
_____
_____
_____

6. Do these submitted devices need to be fingerprinted? YES / NO

7. Do these submitted devices need to be swabbed for DNA? YES / NO

8. Has this evidence been previously viewed and/or accessed by anyone? YES / NO

9. Does any of the evidence contain privileged information? YES / NO

JOPLIN POLICE

303 E. 3rd Street * Joplin, MO 64801-2274 * 417-623-3131 * Fax 417-625-4733

CONSENT TO SEARCH COMPUTER(S)/CELL PHONES

I, _____, have been asked by Detective(s)/Officer(s) of the Joplin Police Department, to permit a complete search by the Joplin Police Department, or its designees, of any and all computers, any electronic and/or optical data storage and/or retrieval system or medium, and any related computer peripherals, described below:

_____
_____

CPU Make, Model & Serial Number (if available)

_____
_____

Storage or Retrieval Media, Computer Peripherals

_____
_____
_____
_____

and located at_____, which I own, possess, control, and/or have access to, for any evidence of a crime or other violation of the law. The required passwords, logins, and/or specific directions for computer entry are as follows:

_____

_____

I have been advised of my right to refuse to consent to this search, and I give permission for this search, freely and voluntarily, and not as the result of threats or promises of any kind.

I authorize Detective(s)/Officer(s) with the Joplin Police Department, or their designee, to take any evidence discovered during this search, together with the medium in/on which it is stored, and any associated data, hardware, software and computer peripherals.

_____ _____

Date Signature

_____ _____

Date Signature of Witness

_____

Printed Full Name of Witness

_____

Location