POLICE DEPARTMENT
HANOVER PARK, ILLINOIS

DIRECTIVE: 448-I

REFERENCE STANDARDS: 83.2.5

SUBJECT: Seizure of Computer Equipment and Electronic Evidence

POLICY: It is the policy of the Hanover Park Police Department to pursue the identification, investigation, and prosecution of persons who use computers and/or other electronic equipment capable of storing data in a electronic format in the furtherance of criminal activity, and to ensure that this evidence is handled properly. This policy shall apply in those cases where data residing on computer systems, recording devices, and other media are being sought as evidence in an investigation. Computers and other devices seized by department personnel shall be treated as evidence and processed according to the procedures outlined in Directive 401-I, Collection and Preservation of Evidence. (83.2.5)

DEFINITIONS:

COMPUTER SYSTEM - computer monitor, CPU, hard drive, I/O device, modem, CD-ROM, or floppy drive configured to work together as a unit or cabled together externally.

RECORDING DEVICE - CD-ROM, floppy drive, tape drive, zip drive, jazz drive, and magneto-optical drive used to store data that is not currently connected to an operating system. Other electronic storage devices include wireless and cordless telephones, answering machines, caller ID devices, electronic paging devices, facsimile machines, smart cars and magnetic stripe cards, ID card printers and other printers, scanners, copiers, compact disk duplicators and labelers, digital cameras/video/audio, electronic games devices, global positioning systems, personal data assistants and hand held computers, security systems, vehicle computer devices, and others.

RECORDING MEDIA - floppy disk, jazz, zip, or magneto-optical disk, hard drives, memory cards and sticks, and others. Any tape, or other type of media or electronic equipment, capable of storing data.

I. RESPONSIBILITIES OF THE INVESTIGATING OFFICER

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

1. Whenever practical, computer and electronic equipment should be recovered by an officer who has been trained in digital evidence collection techniques.

2. For personal computers, the officer should:
   a. Disconnect the computer from the power source, usually by unplugging from the back of the computer even if the computer was left on.
   b. Tape all ports and openings on the computer with evidence tape.

3. For laptop computers, the officer should:
   a. Disconnect the laptop computer from the power source, even if the computer was left on. If the computer was powered via a power cord, unplug from the outlet. If the laptop does not shut down when the power cord is removed, locate and remove the battery pack.
   b. Tape all ports and openings on the laptop computer with evidence tape.

4. For servers and network computers, officers will secure the scene and not let anyone other than a trained computer evidence technician touch or access the equipment. Officer will then request assistance from an outside agency specifically trained in computer recovery techniques. These agencies could include, but are not limited to, the FBI, the U.S. Secret Service, and other specially trained persons in the recovery of servers and network computers.

5. Complete a written case report detailing the specifics of the case, procedures followed, and other findings. A copy of this report shall be forwarded to the Investigations Bureau as soon as practical after the incident.

B. PROCEDURE FOR SEIZURE

1. When it is determined that a computer or electronic equipment is to be seized and processed, department personnel shall prepare the computer or other digital evidence for processing by disconnecting the equipment from its power source, and taping the ports and openings as outlined in sections I.A.2, 3, and 4 above. The seized items shall be treated as evidence and processed according to the procedures outlined in Dirctive 401-I, Collection and Preservation of Evidence. A properly trained investigator should be consulted as soon as possible to assist.

2. During a criminal investigation, examination of the contents of a computer, or other recording device/media, by the investigating officer, constitutes a search. This search can only be conducted with the consent of a properly authorized individual, or by the issuance of a search warrant. It should be noted that consent to search can be withdrawn at any time, and is especially difficult to ensure if the examination process is conducted at a later date and at another location. Unless exigent circumstances exist, officers shall not examine the contents, or access any file, on any computer or data storage device, that is subject to the criminal investigation.

3. A search warrant allows for the search, seizure and examination of electronic evidence as predefined under the warrant. This method is most preferred, and consistently is met with the least resistance at the scene, and in the court system.

4. Using evidence obtained from a computer or electronic equipment in a legal proceeding requires:
    a. Probable cause for the issuance of a warrant or an exception to the warrant requirement.
    b. Acceptable and appropriate evidence collection techniques to avoid altering or destroying evidence.
    c. Forensic examination of the system completed by trained personnel in a timely manner with expert testimony available at trial. This requirement will normally be filled by the evidence custodian or investigator sending the computer evidence to a crime lab that examines computer evidence.

II. OTHER ELECTRONIC EVIDENCE

A. Best Practices for Seizing Electronic Evidence, (Appendix A)

1. Officers will familiarize themselves with the publication, Best Practices for Seizing Electronic Evidence, (Appendix A). This publication will guide officers in recognizing potential evidence, preparing for the search and/or seizure, consent searches, search warrants, and specific actions that should be taken to ensure the integrity of the evidence and the device seized.