Approved: *Chief Marcia Harnden*	Subject: **612. Computers and Digital Evidence**	
Effective: November 28, 2017	CALEA Standards: 83.2.5	Page: 1

612.1: PURPOSE AND SCOPE

This policy establishes procedures for the seizure and storage of computers, personal communications devices (PCDs) digital cameras, digital recorders and other electronic devices that are capable of storing digital information; and for the preservation and storage of digital evidence.

612.2: POLICY

It is the policy of the Albany Police Department that all evidence seized and/or processed pursuant to this policy shall be done so in compliance with clearly established Fourth Amendment and search and seizure provisions and best practices.

612.3: SEIZING COMPUTERS AND RELATED EVIDENCE

a. When seizing computers and accessories, members should be aware of the potential to destroy information through careless or improper handling and should utilize the most knowledgeable available resources.

b. The following steps should be taken to preserve computer-related evidence:

   1) Photograph each item, front and back, specifically including cable connections to other items;

   2) Look for a source for Internet connection (wireless router, modem, cable connection, phone line connection);

   3) Be mindful of the presence of physical evidence on and around the hardware relevant to the particular investigation such as fingerprints, biological or trace evidence, and/or documents;

   4) Do not power the computer on if it is turned off;

   5) If the computer is on, do not shut it down normally and do not click on anything or attempt to examine any files.

      A. Photograph the screen, if possible, and note any programs or windows which appear to be open and running;

B. Disconnect the power cable from the back of the computer (For laptops, disconnect any power cable and remove the battery, if possible.);

6) Label each item with a case number and evidence item number;

7) Handle and transport the computer and storage media (e.g., tape, discs, memory cards, flash memory, external drives) with care so that potential evidence is not lost;

8) Book all computer items into Property and Evidence. Do not store computers where normal room temperature and humidity is not maintained;

9) The following should be documented in related reports:

A. The specific location of the computer or device and whether it was in operation;

B. Who was using the computer or device at the time;

C. Who claimed ownership of the computer or device;

D. If it can be determined, how the device was being used.

10) In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all storage devices (hard drives, tape drives and disk drives) should be seized along with all media. Accessories (printers, monitors, mouse, scanner, keyboard, cables, software and manuals) should not be seized unless as a precursor to forfeiture.

612.3.1: BUSINESS OR NETWORK COMPUTERS

In cases where business or network computers must be seized as evidence, members should contact a Certified Forensic Examiner for instructions or a response to the scene in order to ensure that the business or network computer is handled properly and perform an on-site forensic examination or obtain an image of the hard drive, if appropriate.

a. Members not specifically trained in processing computers as evidence should not attempt to perform a forensic examination or obtain an image of the hard drive themselves.

b. Assistance may be obtained from the Detective Unit, the Northwest Regional Computer Forensics Lab, Oregon State Police, or certified examiner from an outside agency.

612.3.2: FORENSIC EXAMINATION OF DIGITAL EVIDENCE

a. If a forensic examination for digital information contained within a computerized device, personal communications device, or media storage device is required, the following shall be forwarded to the Detective Division:

1) A completed and approved copy of Digital Evidence Forensics: Form A32;

2) A copy of the document providing the basis of legal authority to conduct a search of the computerized device (i.e. consent to search form or copy of the search warrant, etc.)

b. The Detective Unit Supervisor will be responsible for the final approval and assignment of the forensic examination.

612.4: SEIZURE OF DIGITAL STORAGE MEDIA

Digital storage media, to include hard discs, floppy discs, CDs, DVDs, tapes, memory cards, or flash memory devices should be seized and stored in a manner that will protect them from damage.

a. If the media has a write-protection tab or switch, it should be activated.

b. Do not review, access or open digital files prior to submission. If the information is needed for immediate investigation, request Property and Evidence to copy the contents to an appropriate form of storage media.

c. Keep all media away from magnetic devices, electric motors, radio transmitters or other sources of magnetic fields, which may damage or erase data.

d. Do not leave storage media where they would be subject to excessive heat such as in a parked vehicle on a hot day.

e. Use plastic cases designed to protect the media, or other protective packaging, to prevent damage.

612.5: SEIZURE OF PERSONAL COMMUNCATION DEVICES

Personal communication devices such as cell phones, tablet computers or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device including messages, stored data and/or images.

a. Officers should generally not attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Unsent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages.

b. Officers should attempt to solicit information from device users to determine the phone number, pass codes, pattern locks or PINs whenever possible.

c. If exigent circumstances dictate that the device must be left on for immediate processing, the device should be isolated from its network while maintaining power.

1) This can be accomplished by placing the device in “Airplane Mode”, and disabling the wireless Internet (Wi-Fi) and Bluetooth connections.

d. If the cell phone is unable to be processed immediately, turn off the phone, remove the battery if

practical, if not, do not turn it back on.

e. When seizing the devices, also seize the charging units and keep them plugged in to the chargers until they can be examined. If the batteries go dead data may be lost.

f. Include in the report the authority under which the device was accessed or manipulated and the steps which were taken to protect the device.

612.6: DIGITAL EVIDENCE

The following procedures shall be followed to ensure the integrity and admissibility of digital evidence such as photographs, audio recordings and video recordings obtained by members of this Department. Direction regarding the handling of footage from Portable Audio/Video Devices, Mobile Audio Video may be found in the Digital Media Recording: Policy 633.

612.6.1: COLLECTION OF DIGITAL EVIDENCE

Once evidence is recorded it shall not be erased, deleted or altered in any way prior to submission. All photographs taken will be preserved regardless of quality, composition or relevance. Video and audio files will not be altered in any way.

612.6.2: SUBMISSION AND TRANSFER OF DIGITAL EVIDENCE

The following are required procedures for the submission of digital media used by cameras or other recorders:

a. The recording media (phone, recorder, flash drive, or any other media) shall be brought to the department as soon as possible for submission into the department storage system;

b. Digital evidence should not be opened or reviewed prior to downloading and storage;

c. The recording media should be connected to a computer and the files accessed directly from the computer directory or downloaded to a folder on the host computer for copying to the department storage system;

d. Once it is verified that the digital evidence is properly transferred to the department storage system, the officer will normally erase the evidence off the recording media (phone, recorder, flash drive, or other device) for re-use or disposal;

e. If the recording media itself is evidence, the evidence shall not be erased and the media along with its digital evidence shall also be entered into the property and evidence module and placed into an evidence locker.

612.6.3: PRESERVATION OF DIGITAL EVIDENCE

a. Property and Evidence Technicians and Police Clerks are authorized to copy original digital media that

is held as evidence.

b. Digital images that are enhanced to provide a better-quality photograph for identification and investigative purposes must only be made from a copy of the original media.

c. If any enhancement is done to the copy of the original, it shall be noted in the corresponding incident or supplemental report.

612.7: FORENSIC WORKING FILES

a. Department members who have been trained to forensically examine digital information and assigned to do so may make a working copy of digital information or digital evidence.

b. The following procedures are to be followed regarding the working copies:

1) Files shall be clearly identified by a case number.

2) Files will be secured in a locked office and normally saved on a secured Network-Attached Storage (NAS) device.

3) Working copy files will be audited annually. Working copies no longer needed for investigative purposes and adjudicated will be deleted.

4) The Investigations Lieutenant, or his/her designee, will complete an audit memo and forward to the Chief of Police through the Chain of Command.