# RICHMOND POLICE DEPARTMENT
# GENERAL ORDER

| Subject: **DIGITAL EVIDENCE PROCEDURES** | Chapter 7 | Number 27 | # Pages 4 |
|---|---|---|---|
| References: CALEA: 83.2.5 | Related Orders: 3-12 | Effective Date: 11/30/2023 Revised by: Review Prv. Rev. Date: 04/23/2020 | |
| Chief of Police: Robert D. Edwards | | | |

I. PURPOSE

The purpose of this directive is to facilitate the identification, investigation and prosecution of persons who utilize electronic equipment in the furtherance of criminal activity.

II. ***SUMMARY OF CHANGE***

***This policy is due for review. Procedures for transporting a mobile phone has been updated. All changes will be bold and italicized.***

III. POLICY

It is the policy of the Richmond Police Department that, during criminal investigations, only agency designated employees that are trained in proper digital evidence handling techniques (hereafter referred to as "Digital Evidence Collection Specialists" or "DECS"), or ***who*** are acting under the direction of such persons, shall seize digital evidence. In addition, the analysis of such evidence, whether done on-scene or after seizure may only be performed by those persons designated as Computer Forensic Examiners. [CALEA 83.2.5]

IV. ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this general order. Failure to comply will result in appropriate corrective action. Responsibility rests with the Division Commander to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated.

This directive is for internal use only, and does not enlarge an employee's civil liability in any way. It should not be construed as the creation of a higher standard of safety or case in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this Department, and then only in a non-judicial administrative setting.

V. DEFINITIONS

A. Computer Forensic Examiner – An authorized sworn or civilian member of the Richmond Police Department ***formally*** trained ***and certified*** in the techniques of ***electronic*** data recovery and seizure.

B. Digital Evidence – Computers, cell phones, hard drives, tablets, USB devices, camera, CD/DVD media, removable media (SD cards, memory sticks, etc.), legacy media (floppy disks, tape cartridges, etc.), or other devices designed to hold data in a digital format.

C. Digital Evidence Collection Specialist – An authorized sworn or civilian member of the Richmond Police Department trained in the collection of digital evidence. Attendance at any such training taught by members of the Richmond Police Department's Computer Crimes Unit or an approved outside agency will suffice for this designation.

D. Digital Information Processing Machines – Computers, personal digital assistants (PDAs), MP3 players, digital cameras or other ***electronic*** devices designed to interpret or manipulate information stored in digital format on devices such as those listed under "Digital Evidence" above.

VI. PROCEDURE

This policy shall apply only in those cases where data residing on computer systems, cell phones, tablets, recording devices and/or other storage media are being sought as evidence in an investigation.

A. Seizure: [CALEA 83.2.5]

1. No Department member, except those designated as digital evidence collection specialists, or who are acting under the direction of such employees, shall power-off, disconnect, power-on or access a computer system, cell phone, recording device or other type of storage media that is to be seized.

2. When it is determined that digital evidence is to be seized and processed and neither an examiner nor collection specialist is available, the supervisor shall contact the on-call forensic examiner and request him/her to respond on-scene. Investigators who knowingly have digital evidence as targets in their search warrants will need to either have a collection specialist on hand for the execution of the warrant or will need to contact the on-call member of the Computer Crimes Unit to assist.

3. Any questions regarding equipment seizure (wording of search warrants, etc.) can be addressed by contacting the Computer Crimes Unit during normal business hours or by contacting the Department of Emergency Communications (DEC) during non-business hours. Inquiries to the DEC will be directed to the on-call investigator.

B. Transport:

1. Where applicable, a forensic examiner or digital evidence collection specialist should handle the transport of seized digital evidence.

2. If a computer forensic examiner or evidence collection specialist is unable to physically assist in the transportation of the seized items, the sworn officer or on-scene investigator must adhere to the following:

   a) All items shall be packaged in a manner suitable for safe/secure transport;

   b) All items shall be labeled so they are readily identifiable; and,

   c) At no time shall items be placed [redacted].

3. If the device to be transported is a cell phone, the following procedures must be followed:

   - [redacted]
     - [redacted]
     - [redacted]
     - [redacted]
   - [redacted]

C. Storage:

1. All seized digital evidence should be handled according to the Richmond Police Department's existing evidence handling policies and procedures as defined in General Order 3-12, Handling Property and Evidence.

2. For the purposes of analysis, all seized items shall be transported to the Computer Crimes Unit by Richmond Police Department personnel following the procedures set forth in the section above entitled "Transport" (section "B"). Upon receipt of these items, they will be logged in and maintained by the Computer Crimes Unit until such analysis is complete.

D. Analysis, Reviews and Examinations:

All requests for reviews, examinations and analysis must include a copy of the search warrant or signed consent form and either a Request for Forensic Examination (PD-55) for computers or related media or a Cell Phone Analysis Request (PD-170) for cell phones before a computer forensic examiner can take any action. The time frame for completion will depend on the volume of materials seized in combination with the

reason for seizure. Reasons for seizure will generally fall within one of the following categories:

1. Reviews – The most unobtrusive investigations that generally involve an overall look at the system type, size and operating system. Reviews are often done for the purposes of determining the existence of such things as pornography or Internet access to unauthorized sites. They may also be done to determine ownership on lost and found or stolen property.

2. Examinations – Normally done in an effort to locate a particular file or text statement involving a specific crime or activity which is known or highly suspected to exist on the media device in question.

3. Analysis – Involves a complete and detailed review of the submitted media device. This is the most obtrusive investigation and will generally take the longest period of time to complete.

E. Dissemination:

Upon completion of the analysis, review or examination, the computer forensics examiner will:

1. Make available a report of the findings to the requesting officer or investigator.

2. Maintain a copy of the findings in Computer Crimes Unit.

F. Disposition:

1. Final dispositions or destruction of evidence shall be done in accordance with General Order 3-12, Handling Property and Evidence or, when applicable, at the discretion of the court.

2. Evidence released by the court shall be returned to the owner as soon as practical.

3. Evidence released to the Richmond Police Department's Computer Crimes Unit by order of the court shall be logged and maintained by the Computer Crimes Unit. If, at any point, the property is no longer needed, it shall be disposed of in accordance with General Order 3-12, Handling Property and Evidence.

## VII. FORMS

A. Consent Form

B. PD-55, Request for Forensic Examination

C. PD-170, Cell Phone Analysis Request