The Allegheny County Chiefs of Police Association

MODEL

DIGITAL EVIDENCE POLICY

An Allegheny County Criminal Justice Advisory Board Project

In Partnership With

The Allegheny County Police Department
&
The Allegheny County District Attorney's Office

JUNE-2025

This model should serve only as a "**Starting Point**" for those departments who may wish to update their Rules & Regulations Manual in this area. To best serve your department, it should be reviewed and **revised** by you, your Municipality and Insurance Carrier.

ACCPA-ACPD-ACDA
MODEL DIGITAL EVDENCE POLICY

The purpose of this policy is to provide Officers with general guidelines for maintaining the integrity of digital evidence and/or property collected.

Prior to seizing digital evidence or devices and obtaining a search warrant or court order to seize digital evidence or devices; you may want to contact the Allegheny County Police Department Mobile Device Forensic Unit at (412) 473-1380 or the Secret Service Pittsburgh Field Office at (412) 281-7825.

1) EVIDENCE STATUS

At the conclusion of a criminal court trial, the affiant officer will check with the Prosecuting Attorney to determine if all the criteria for a closed case have been met. If so, request a Court Order for the disposal of the evidence (See **PROPERTY & EVIDENCE POLICY**, Section 17 RELEASE OF PROPERTY AND EVIDENCE and Section 18 PROPERTY DISPOSAL).

2) DIGITAL EVIDENCE

Any information stored or transmitted in binary form that is obtained because of an official police investigation, confiscation, or recovery as a result of an official police action (e.g., audio visual recordings and digital images).

a) Officers who encounter a computer or data storage device that he or she believes may contain evidence of a crime should establish probable cause or consent for the seizure of the system or device.

b) Once probable cause has been established, a search warrant or *Consent to Search Form should be completed for the seizure of the data to be examined. If there is a danger that electronic evidence may be destroyed, altered or overwritten, the evidence should be safeguarded and secured pending a search warrant (* Appendix A).

c) An Assistant District Attorney should be consulted to ensure a properly structured and worded search warrant is drafted. **Courts require both specificity and a nexus to the crime.**

d) If circumstances require access to evidence prior to a forensic examination, such as a witnesses' mobile device by consent or warrant, officers will document the date, time and description of evidence viewed or accessed, and will provide that written detail to a digital forensic examiner.

e) Electronic evidence voluntarily provided by bystanders and uninvolved witnesses may be secured as reasonably necessary under the circumstances at the discretion of the officer (in the spirit of accommodating helpful citizens). If a bystander or witness wishes to email or permit the officer to extract the relevant data via a forensic tool, the officer must document the witness' involvement and the collection method to facilitate the witness' authentication of the evidence later. The officer must also secure the address, phone number, and other relevant contact information for the bystander or uninvolved witness.

3) STORAGE DEVICES

If an officer encounters a data storage device (e.g., thumb drive, external hard drive, secure device (SD) card) and has probable cause to believe it contains evidence of a crime, he or she should seize

the device and apply for a search warrant as soon as possible. If officers are unsure if probable cause exists, they should consult with a district attorney before seizing evidence to determine if probable cause exists.

a) All forms of digital media should be handled so as to not damage the data. Some storage media utilize a magnetic medium. The storage device should be kept away from any magnetic fields or high temperatures.

b) The storage devices should be packaged separately from peripherals, cables, or other evidence to facilitate later examination. Do not place evidence tape directly onto any disk, tape, or CD: these items should be placed into appropriate storage containers.

Digital forensic examiners from the Allegheny County Police or Federal Agencies are available to give advice, instruction, and assistance when appropriate.

4) HAND-HELD COMMUNICATION DEVICES

Industry best practices will be followed when collecting handheld communication devices. These handheld communication devices may include but not limited to cellphones, smartphones, personal digital assistance (PDA) and handheld computer (tablet). Within this policy, all these handheld communication devices will be referred to as device(s).

In the 2014 *Riley/Wurie* U.S. Supreme Court decision, 134 S.Ct. 2473, the U.S. Supreme Court clearly held that in order to access any information on a cell phone, police must first obtain a warrant. The rule created by Riley/Wurie is "exceedingly simple: if a member of law enforcement wishes to obtain information from a cell phone, get a warrant".

Pennsylvania courts have followed suit on the issue as well in multiple cases. **Be mindful that even the slightest manipulation such as the act of powering up a phone is a "search**", navigating through the menus of the phone to obtain it's number is a "search, and monitoring a phone's incoming calls and text messages is a "search" all activating Fourth Amendment protections. A member of law enforcement that wishes to obtain information from a cell phone must get a warrant, *Commonwealth v. Fulton*, 645 Pa 296, (February 21, 2018). Moreover, even when obtaining a warrant, officers must clearly articulate a nexus between the alleged criminal activity and the item or location desired to be searched, see *Commonwealth v. Ani*, 293 A.3d 704 (2023).

For seizure of a device(s) there must be probable cause to believe evidence of the crime is within the device, along with the existence of a signed search warrant or a recognized exception to the search warrant requirement (e.g., consent, circumstances which create a serious bodily injury or death exigency, and immediate destruction of evidence).

If a delay to obtain a search warrant is likely to result in destruction of evidence, the officer must articulate the basis for that belief and may:

a) Seize and secure the device(s) in a way which prevents destruction, if possible.

b) Apply for a search warrant immediately after the seizure.
c) Consult with an Assistant District Attorney immediately before or after the seizure to determine if enough probable cause exists.

When a device(s) is lawfully collected from witnesses, victims, and suspects in order to recover necessary evidence and intelligence information, best practices will be followed to ensure the safe collection of the device(s):

a) Photograph the device(s) and scene.

b) If the device(s) is located “powered off” leave it off.

c) If the device(s) is located “powered on”, keep it on and immediately “shield” the device(s) from the network:

   i) This can be done by placing the device(s) in airplane mode, disconnecting the wireless connection (Wi-Fi), turning off Bluetooth and the removal of a SIM card from the device(s) to keep the device(s) from connecting to the cellular network if possible.

   ii) Devices which cannot be “shielded” from the network by the above method, need to be immediately placed in a “Faraday” bag. The Faraday bag is used to block electromagnetic fields reaching the device, as well as stopping any electromagnetic fields being sent by the device. Any device(s) in a Faraday bag must be provided a power source to ensure the device(s) battery is not depleted. The power source provided to the device(s) cannot come from outside the Faraday bag used, as this will break the Faraday shielding.

   iii) Digital forensic examiners can provide advice and instruction if needed.

   iv) If Airplane Mode is set the phone should not be placed in the Faraday Bag.

   v) If Airplane Mode cannot be set or the SIM card removed place the device(s) and proper labeled evidence envelope into the Faraday Bag and connect the device(s) to a charging cable.

During the collection process, whenever possible the officer should try to obtain the password, passcode, or pattern from the person in possession of the phone. If the device owner is in custody an officer must obtain consent. If consent is denied, passcodes cannot be compelled, even with a court order; however, bio-metric security such as fingerprints, or touch ID can be compelled with a court order. In some cases, if the passcode is not obtained the data cannot be retrieved from the device. Officers should review current PA case law with an Assistant District Attorney before compelling a passcode from a defendant.

If the password, passcode, or pattern for the device has been obtained, it should be verified by the officer and documented.

Proper device collection procedures should be followed or the ability to extract the device data could be lost. Digital forensic examiners will provide advice and instruction when appropriate.

Only Forensic Examiners may conduct extractions of the device(s).

Officers will document all procedures completed, media viewed, or settings changed in the officer’s statement, supplement, examination notes or report.

5) PERSONAL COMPUTER AND LAPTOP SYSTEMS

A desktop computer, laptop, or other data storage device that an officer has probable cause to believe contains evidence of a crime may be seized with a search warrant or warrant exception. Consult with an Assistant District Attorney prior to any seizure.

The following guidelines are directed toward both laptop and stand-alone desktop computer systems (not to include networked computers):

a) If the computer is **ON,** it **SHOULD NOT BE TOUCHED**. If information is displayed on the monitor, the monitor should be photographed. Do not push any other key/buttons or click any desk icons. Digital photographs should be taken of the items displayed on the system's monitor and connected devices. Unplug the computer as is and collect the power cable.

b) If the computer is **OFF, DO NOT** turn it on.

c) Devices to be electronically processed should be packaged with the power cable separately from other evidence.

d) Digital forensic examiners from the Allegheny County Police and State Police are available to provide advice and instruction when appropriate.

The following guidelines should be used when dealing with Routers:

e) If there is a router/modem in the household, DO NOT UNPLUG IT. If you unplug the router the evidence will be lost.

f) Take pictures of the device, as it may contain information accessing the device. (Passwords and BSSID information and network names).

g) Examination of the router must be done by a digital forensic examiner on site.

h) Digital forensic examiners from the Allegheny County Police and State Police are available to provide advice and instruction when appropriate.

6) RELATED DOCUMENTATION

During the seizure of computer-related evidence, the officer may attempt to find and photograph (before collection) all related documentation and materials on or in the area of the system. Items to be seized include software, manuals, printouts, check stock, Post-It Notes, notebooks, day planners, and any other items associated with the equipment. These items are frequently related to the criminal activity and may contain additional evidence and passwords to files or programs.

7) NETWORKED SYSTEMS AND SERVERS

Properly trained officers should be the only personnel authorized to seize corporate network and server-based systems.

a) With limited exceptions, servers shall be **powered down properly** to avoid any system damage or loss of information. Damage to the system may disrupt legitimate business and create potential liability. When practical, the digital forensic examiner will coordinate with on-site personnel familiar with the server in order to determine the most appropriate course of action. In cases requiring a deviation from a normal server shutdown, the digital forensic examiner will specify the reasons within the examination report.

b) A legitimate business' computer system should only be seized when necessary and then only with the appropriate warrant or warrant exception.

c) Digital forensic examiners will strive to minimize the impact of the computer examination on the legitimate operation of a business. This can often be accomplished through execution of a search warrant or lawful warrantless examination during the hours of the least computer usage.

d) The examination should be only as intrusive as is necessary and proper for the investigation (e.g., if the suspect only had access to his computer workstation and specific network drives, the entire company's computer network should not be seized).

e) If an entire system must be seized from an entity with legitimate business operation, it should be returned as soon as practical and appropriate.

8) SEARCH WARRANTS

Officers writing digital evidence search warrants must ensure that there is a Nexus between the electronic data and criminal activity or evidence. Merely relying on the connection that a crime occurred and the purported actor was in possession of an electronic device is insufficient.

a) If an officer who is otherwise lawfully on the premises develops probable cause to believe that a computer or other data storage device contains evidence of a crime, the device may be seized pursuant to a separate search warrant or warrant exception (Consult with an Assistant District Attorney). If the computer or data storage device is located in an area in which an individual has a reasonable expectation of privacy, a search warrant or voluntary consent will be required to enter and seize said evidence. A forensic examination of the evidence requires a search warrant where the device(s) are known, or which may require a separate search warrant post-seizure.

b) An Assistant District Attorney should be consulted during the preparation of any search warrant intended to seize digital evidence or devices that will be forensically examined.

c) In any case where an arrest warrant needs approval from an Assistant District Attorney an Assistant District Attorney should be consulted to review all search warrants prior to obtaining a judge's signature.

9) INTERNET SERVICE PROVIDERS

Valuable information can be obtained through any of the Internet Service Providers (ISP). Officers who intend to submit a search warrant to an ISP should consult with an Assistant District Attorney (as applicable).

A search warrant will allow the investigator to obtain detailed subscriber, account, and billing information, transactional information, and any stored user files as well as emails and Internet history.

a) Depending on the ISP and the court order required, the court order may need to be issued by a court having geographic jurisdiction for the ISP.

b) ISP data and items may be time sensitive, so preservation and prompt application are required.

c) For specifics on obtaining information from an ISP, contact the ISP's law enforcement liaison.

10) EXAMINATION PROCEDURES

All examinations will be conducted in accordance with accepted digital forensics best practices. All examinations, except those conducted under Section 1, will be conducted by, or under the supervision of, a properly trained Digital Forensic Examiner.

11) DIGITAL FORENSIC EXAMINERS

Each digital forensic examiner will be trained and/or certified in the seizure of computers and digital evidence, digital forensic examinations, and in the use of the primary examination software. The examiner, will be licensed to use all the software utilized in the Digital Forensic Lab. This does not include software contained on or extracted from the target device and used to examine that same target device or data.

12) EVIDENCE STORAGE

Industry best practices and Evidence Chain of Custody Room procedures will be followed.

a) Once the forensic images have been acquired and all the systems information is annotated, if there is no longer a need for the system, it should be returned to, or properly submitted to, the Property and Evidence Section. Before evidence is returned to a suspect or defendant an Assistant District Attorney should be consulted.

b) Items stored will be kept separate from other items to ensure the integrity of each case and its evidence.

c) After the examination is completed, a copy of the image will be provided to the submitting officer. The data will be maintained in accordance with your departments evidence policy. The Allegheny County Police Mobile Device Forensic Unit will maintain data for one year after the examination date.

MODEL #1
POLICE DEPARTMENT
VOLUNTARY CONSENT TO SEARCH
COMPUTERS, COMPUTER ACCESSORIES, DATA STORAGE DEVICES AND MEDIA

(READ & PRINT YOUR NAME) I, _____, have been made aware of my constitutional rights regarding the privacy of data stored on computers, computer accessories, data storage devices, media, internet accounts, and cell phones. I understand my constitutional right to be free from searches without a search warrant and my right to refuse consent to such searches. I also acknowledge that I have the right to revoke my consent to a search at any time.

I understand that conducting such a search may be time consuming, may require a lengthy documentation process, and may require the temporary utilization of software and/or hardware.

CHECK ITEM(S) TO BE SEARCHED

☐**CONSENT TO SEARCH COMPUTERS AND INTERNET ACCOUNTS**

(READ & PRINT YOUR NAME) I,_____, hereby authorize Police or other law enforcement agencies they deem necessary to access, search, seize, print, copy, or otherwise save in any form, data and any information stored, transmitted, or existing on computers, or internet accounts listed on the second page of this form which is contraband, or may be used as evidence in criminal proceedings.

☐**CONSENT TO SEARCH CELLULAR TELEPHONES, SERVICES AND DATA**

(READ & PRINT YOUR NAME) I,_____, hereby authorize Police to conduct a complete search of the cell phone(s) described on the second page of this form and any information stored or transmitted or data contained therein/thereon. Police are authorized by me to take any information, media or data which is contraband, or may be used as evidence in criminal proceedings.

I am not unduly under the influence of drugs and/or alcohol._____**(INITIAL)**

I am giving this written permission voluntarily and without threats, pressures, coercion or promises of any kind being made to me._____**(INITIAL)**

PRINT NAME:_____

LOCATION:_____

SIGNATURE:_____ **DATE:** _____

OFFICER: _____ **DATE:** _____

OFFICER: _____ **DATE:** _____

DESCRIPTION OF ARTICLES TO BE SEARCHED p.2

DESCRIPTION: **PASSWORD:** **INITIALS:**

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

11. _____

12. _____

13. _____

14. _____

15. _____

16. _____

17. _____

18. _____

19. _____

20. _____

MODEL #2
POLICE DEPARTMENT

VOLUNTARY CONSENT TO SEARCH

(READ & PRINT YOUR NAME) I, _____,
having been informed of my constitutional rights not to have a search made of myself, the premises, property, or motor vehicle mentioned below without a search warrant and, my right to refuse to consent to such search, and that I may revoke my consent to search at any time, hereby authorize Police to conduct a complete search of my person, premises, property or motor vehicle described as _____

_____

_____

_____

These Police Officers are authorized by me to take any letters, papers, materials or other property, which is contraband or may be used as evidence in criminal proceedings.

I am not unduly under the influence of drugs and/or alcohol._____ **(INITIAL)**

I am giving this written permission voluntarily and without threats, pressures, coercion or promises of any kind being made to me._____ **(INITIAL)**

Print Name_____

Signature_____

Location _____

Date & Time_____

Police Officer_____

Police Officer_____