Investigation and Prosecution

600.1 PURPOSE AND SCOPE

The purpose of this policy is to set guidelines and requirements pertaining to the handling and dispositions of criminal investigations.

600.2 POLICY

It is the policy of the Elkton Police Department to investigate crimes thoroughly and with due diligence, and to evaluate and prepare criminal cases for appropriate clearance or submission to a prosecutor.

600.3 INITIAL INVESTIGATION

600.3.1 OFFICER RESPONSIBILITIES

An officer responsible for an initial investigation shall complete no less than the following:

(a) Make a preliminary determination of whether a crime has been committed by completing, at a minimum:

1. An initial statement from any witnesses or complainants.
2. A cursory examination for evidence.

(b) If information indicates a crime has occurred, the officer shall:

1. Preserve the scene and any evidence as required to complete the initial and follow-up investigation.
2. Determine if additional investigative resources (e.g., investigators or scene processing) are necessary and request assistance as required.
3. If assistance is warranted, or if the incident is not routine, notify a supervisor or the Duty Officer.
4. Make reasonable attempts to locate, identify and interview all available victims, complainants, witnesses and suspects.
5. Collect any evidence.
6. Take any appropriate law enforcement action.
7. Complete and submit the appropriate reports and documentation.

(c) If the preliminary determination is that no crime occurred, determine what other action may be necessary and what other resources may be available, and advise the informant or complainant of this information.

600.4 CUSTODIAL INTERROGATION REQUIREMENTS

Suspects who are in custody and subjected to an interrogation shall be given the *Miranda* warning, unless an exception applies. Interview or interrogation of a juvenile shall be in accordance with the Temporary Custody of Juveniles Policy.

600.4.1 AUDIO/VIDEO RECORDINGS

An officer conducting a custodial interrogation of an individual who is suspected of having committed any violent felony offense, including murder, rape, sexual offense in the first degree or sexual offense in the second degree, shall make reasonable efforts to create an audiovisual recording in its entirety. Regardless of where the interrogation occurs, every reasonable effort should be made to secure functional recording equipment to accomplish such recordings (Md. Code CP § 2-402).

Consideration should also be given to recording a custodial interrogation, or any investigative interview, for any other offense when it is reasonable to believe it would be appropriate and beneficial to the investigation and is otherwise allowed by law.

No recording of a custodial interrogation should be destroyed or altered without written authorization from the prosecuting attorney and the Criminal Investigation Unit supervisor. Copies of recorded interrogations or interviews may be made in the same or a different format as the original recording, provided the copies are true, accurate and complete and are made only for authorized and legitimate law enforcement purposes. An audio or audiovisual recording made by a law enforcement unit of a custodial interrogation of a criminal suspect is exempt from the Maryland Wiretapping and Electronic Surveillance Act (Md. Code CP § 2-403).

Recordings should not take the place of a thorough report and investigative interviews. Written statements from suspects should continue to be obtained when applicable.

600.5 DISCONTINUATION OF INVESTIGATIONS

The investigation of a criminal case or efforts to seek prosecution should only be discontinued if one of the following applies:

(a) All reasonable investigative efforts have been exhausted, no reasonable belief that the person who committed the crime can be identified and the incident has been documented appropriately.

(b) The perpetrator of a misdemeanor has been identified and a warning is the most appropriate disposition.

1. In these cases, the investigator shall document that the person was warned and why prosecution was not sought.
2. Warnings shall not be given for felony offenses or other offenses identified in this policy or by law that require an arrest or submission of a case to a prosecutor.

(c) The case has been submitted to the appropriate prosecutor but no charges have been filed. Further investigation is not reasonable nor has the prosecutor requested further investigation.

(d) The case has been submitted to the appropriate prosecutor; charges have been filed; further investigation is not reasonable, warranted or requested; and there is no need to take the suspect into custody.

(e) Suspects have been arrested, there are no other suspects, and further investigation is either not warranted or requested.

(f) Investigation has proved that a crime was not committed (see the Sexual Assault Investigations Policy for special considerations in these cases).

The Domestic Violence, Child Abuse, Sexual Assault Investigations and Adult Abuse policies may also require an arrest or submittal of a case to a prosecutor.

600.5.1 REOPENING OF A DEATH INVESTIGATION

The Special Operations Bureau Commander shall review and reopen or reinvestigate, as appropriate, any death for which the Department is notified by the medical examiner that the cause or manner of death was amended or corrected to be undetermined or homicide. These cases must not be closed for at least 20 years (Md. Code PS § 3-531).

600.6 COMPUTERS AND DIGITAL EVIDENCE

It is the policy of the Elkton Police Department to preserve, collect, and examine any computer related or digital evidence linked to criminal activity. The Digital Forensics Unit has been established to provide specially trained digital forensic examiners to assist members of the Elkton Police Department. The digital forensic examiners are trained in the collection and examination of various types of magnetic and electronic media found within computer systems, cellular telephones, digital cameras, and other electronic storage media. The digital forensic examiners are able to provide sworn and non-sworn personnel with technical advice for the preparation of search warrants, the seizure of computers, digital storage media, and the recovery and examination of relevant evidence.

600.6.1 DEFINITIONS

Digital Evidence - evidence contained within any form of magnetic or electronic media. Digital evidence is found in, but not limited to: hard drives, USB drives, compact disks (CD), digital versatile disks (DVD), floppy disks, Zip disks, Jaz disks, flash memory cards, magnetic tape, Secure Digital cards (SD), digital cameras, Subscriber Identity Module cards (SIM), cellular telephones, Personal Data Assistants (PDA), computers, hand held computers (tablets), and any other memory developed for the storage of electronic data or information.

600.6.2 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. During

the certification process, a newly assigned digital forensic examiner may conduct examinations under the supervision of a certified examiner.

The Elkton Police Department digital forensic examiner, will be licensed to use all software utilized in the Digital Forensics Lab. This does not include software contained on or extracted from the target device/media and used to examine that same target device/media/data.

600.7 INVESTIGATIVE USE OF SOCIAL MEDIA AND INTERNET SOURCES

Use of social media and any other Internet source to access information for the purpose of criminal investigation shall comply with applicable laws and policies regarding privacy, civil rights and civil liberties. Information gathered via the Internet should only be accessed by members while on-duty and for purposes related to the mission of this department.

Information obtained via the Internet should not be archived or stored in any manner other than department-established record-keeping systems (see the Records Maintenance and Release and the Criminal Organizations policies).

600.7.1 ACCESS RESTRICTIONS

Information that can be accessed from any department computer, without the need of an account, password, email address, alias or other identifier (unrestricted websites), may be accessed and used for legitimate investigative purposes without supervisory approval.

Accessing information from any Internet source that requires the use or creation of an account, password, email address, alias or other identifier, or the use of non-government IP addresses, requires supervisor approval prior to access. The supervisor will review the justification for accessing the information and consult with legal counsel as necessary to identify any policy or legal restrictions. Any such access and the supervisor approval shall be documented in the related investigative report.

Accessing information that requires the use of a third party's account or online identifier requires supervisor approval and the consent of the third party. The consent must be voluntary and shall be documented in the related investigative report.

Information gathered from any Internet source should be evaluated for its validity, authenticity, accuracy and reliability. Corroborative evidence should be sought and documented in the related investigative report.

Any information collected in furtherance of an investigation through an Internet source should be documented in the related report. Documentation should include the source of information and the dates and times that the information was gathered.

600.7.2 INTERCEPTING ELECTRONIC COMMUNICATION

Intercepting social media communications in real time may be subject to federal and state wiretap laws. Officers should seek legal counsel before any such interception.