Digital Forensics Investigations

42.8.1.1 PURPOSE AND SCOPE

This policy establishes procedures for the seizure, storage and analysis of computers, mobile communication devices, digital video recorders and other electronic devices that are capable of storing digital information. All evidence seized or processed pursuant to this policy shall be done in compliance with clearly established search and seizure provisions.

42.8.1.2 DEFINITIONS

Digital Forensics Lab (DF Lab): The SPD Digital Forensics Lab (referred throughout this policy as "Lab") refers to the secure location where specialized equipment is used for investigative examination of digital media.

Forensic Examiner: The Forensic Examiner is any SPD member who has been specially trained to provide investigative examination of digital media.

Digital Media: For the purposes of this policy, digital media refers to any computer, mobile phone, camera, flash drive or other digital device which may contain evidence relevant to a criminal case.

Digital Evidence: Recovered files and/or forensic data obtained from digital media that are relevant to any criminal case

Investigating officer: For the purposes of this policy, the term Investigating officer refers to the primary officer assigned to the case in which digital media is seized for investigative examination. It could also refer to any officer assisting with the case.

42.8.1.3 POLICY

It is the policy of the Springfield Police Department (SPD) to preserve, collect and examine any computer-related or digital evidence linked to criminal activity. The Digital Forensics Lab has been established to provide specially trained digital forensic examiners to assist the assigned officers and detectives.

48.8.1.4 RESPONSIBILITIES

a) Investigating officers are responsible for ensuring they properly safeguard the collection of evidence stored in electronic form and that they follow the procedures in this policy for submitting digital media for investigative examination.

b) Forensic examiners are responsible for providing technical assistance and guidance for members of SPD in the proper safeguarding and collection of evidence stored in electronic form; the examination of digital media in any case where evidence or information pertinent to an investigation may be stored on a computer, smartphone or other electronic or digital device; and assisting outside agencies in investigating crimes requiring digital forensic services.

c) In processing digital evidence, the Forensic Examiner will follow standard protocols as taught in his/her training to ensure digital evidence integrity. The examiner will make all efforts to ensure the use of industry best practices and standards with the goal of preventing or limiting the alteration of data on evidence media and maintain the integrity of the evidence files by following proper electronic evidence recovery and storage procedures. Upon conclusion of the examination the examiner should provide a report to the investigating officer.

42.8.1.5 SECURITY AND INVENTORY CONTROL WITHIN THE LAB

a) The Digital Forensics Lab is inside the secured access area of the Springfield Police Department and housed in a locked room separated from the rest of the Investigative Unit. The Digital Forensics Lab also includes a secure storage area accessible by Lab personnel.

b) To protect against unauthorized access and maintain the chain of custody, the room shall be secured at all times. Only a Forensic Examiner shall have unescorted access to the Lab. Any other personnel entering the Lab must be accompanied by a Forensic Examiner unless authorized by the Chief of Police.

c) Forensic industry best practices suggest that any computer system that is used to store digital evidence will not normally have an active internet connection or connection to the SPD network while the system stores evidence files.

d) Evidence files on forensic workstations and contained on the network storage will be stored in such a way as to protect the integrity of the evidence files and that the evidence files can be verified that they have not been altered.

e) Digital evidence files should be copied to a redundant archival storage within the Lab as soon as practical.

42.8.1.6 SUBMITTING DIGITAL MEDIA FOR EXAMINATION

a) When requested, a Forensic Examiner will assist with the proper drafting and execution of search warrants or consensual searches for digital media to ensure that the evidence is properly seized.

b) Any computers, cellular phones, other digital media or device seized shall be entered into evidence in the Property Control Unit. Any computers, cellular phones, other digital media or device submitted by an outside agency will be handed directly to a Forensic Examiner. All standard procedures and best practices regarding evidence handling apply.

c) To request investigative examination of digital devices, the investigating officer or detective will complete the Digital Media Examination Request form (Attachment A: V:\Forms\Digital Forensics Request Form 021424 FINAL.pdf) and submit it to the Forensic Examiner via the

Detective Sergeant or his/her designee. The Detective Sergeant or his/her designee will forward all approved requests to the DF Lab.

d) Evidence files generated within the Digital Forensics Lab will be provided back to the investigating officer or detective as well as being stored on redundant storage within the Lab.

e) Upon completion of forensic examination, SPD evidence items should be returned to SPD Property Control for secure storage.

42.8.1.7 CONTRABAND EVIDENCE

a) A Forensic Examiner will not copy, distribute, or release from the care, custody and control of the Springfield Police Department any digital evidence containing contraband evidence (e.g., child sexual abuse material (CSAM) and child sexual exploitation material (CSEM)), unless such copy, distribution or release occurs to another law enforcement agency or the National Center for Missing and Exploited Children (NCMEC). Such copy, distribution, or release to another law enforcement agency or NCMEC will be documented in a report.

b) Upon request, such contraband digital evidence will be made reasonably available for inspection by authorized persons (e.g., prosecuting attorneys, defense attorneys, defense forensic examiners) in a controlled environment at the Springfield Police Department. Defense forensic examiners doing on-site analysis of evidence shall do so in a controlled environment and be required to sign a Statement of Understanding form agreeing that they shall not duplicate or remove contraband evidence files from the control of the Springfield Police Department.

42.8.1.8 OUTSIDE AGENCY ASSIST

a) A Forensic Examiner may assist other agencies in the processing or examination of seized digital devices or evidence if authorized by the Detective Sergeant (or his/her designee).

b) Digital devices or evidence seized by the other agency will be transferred to a Springfield Police Forensic Examiner. The requesting agency will complete a Springfield Police Digital Media Examination Request form when submitting digital media for processing.

c) The Forensic Examiner will process the seized digital devices or evidence following the procedures in this policy.

d) Once the requested activity is complete, the Forensic Examiner will release the evidence back to the initiating agency. Copies of created evidence files and reports may be provided to the outside agency and will be maintained on redundant storage in the Lab.

42.8.1.9 QUALIFICATIONS/TRAINING

To qualify as a Forensic Examiner, an SPD member must successfully complete one or more Springfield Police Department approved digital forensics training programs.