


POLICY 105.0	DIGITAL EVIDENCE PROCEDURES	
	REVISED: 06/11, 12/20, 05/24	RELATED POLICIES: 105.2, 105.3, 110.1, EVIDENCE UNIT SOP
	CFA STANDARDS:	REVIEWED: AS NEEDED THIS VERSION EFFECTIVE DATE: MAY 28, 2024

A. PURPOSE

The purpose of this policy is to establish guidelines pertaining to the collection and handling of digital evidence by Department personnel.

B. POLICY

Employees utilizing Body Worn Cameras, mobile devices, digital cameras and/or recorders to document crime scenes, traffic investigations and/or criminal investigations /administrative investigations shall adhere to the operational objectives and protocols outlined in this policy to ensure the integrity of evidence. Digital evidence consists of images and recordings that are required to be maintained for use in court presentations, administrative investigations, or other legitimate police functions. Evidence.com will serve as the Department’s system for storing, organizing, documenting and preserving digital files in a manner acceptable to the courts for later use in criminal proceedings. CSI also uses Foray for certain evidence and photo lab.

C. EXEMPTIONS

Digital evidence collected and stored using other approved Department methods (i.e. MESH cameras, etc.) shall not be subject to the below guidelines.

D. GUIDELINES

1. Digital photographs of victims, perpetrators, crime scenes, instruments of a crime, or any item of value for prosecution of a crime shall be submitted as digital evidence.
2. Digital video and audio recordings of statements made by victims, witnesses, and perpetrators shall be submitted as digital evidence.
3. Department personnel shall submit digital evidence via a Department Digital Upload Terminal and/or through Evidence.com. Department personnel will not be issued or utilize Department digital equipment until having successfully completed training specific to the use of the digital equipment and Evidence.com.
4. Unless exigent circumstances exist, only Department issued digital equipment (mobile devices, Body Worn Cameras, cameras, video cameras and digital recorders) will be utilized to document evidence.

5. Any collected digital evidence shall be submitted/uploaded prior to the end of the employee's shift unless authorized by a supervisor.
6. If digital evidence cannot be uploaded using Evidence.com. Digital Evidence will be notified by email (digitalevidence@flpd.gov).
7. Digital evidence will not be deleted or reformatted before it has been submitted to Evidence.com. All evidentiary images will be uploaded into the system, regardless of whether the photo was taken unintentionally or is of poor quality.
8. Digital evidence will not be downloaded or uploaded onto any other device prior to its submission to Evidence.com. The proper submission of digital evidence into Evidence.com provides for a proper evidentiary chain of custody and authenticates the digital file for later use in court.
9. Only Department Crime Scene Unit and Photo Lab Personnel are permitted to process digital images. Processing will be performed on a working copy with an audit trail, maintained in the Foray Authenticated Digital Management System. The original image will be preserved so it can be compared to the processed image.
10. Department personnel will document the information pertinent to the identification, collection, processing, preservation and dissemination of the digital evidence in the appropriate police report.
11. The unauthorized reproduction, sharing and/or dissemination of digital evidence for personal use is prohibited.
12. No personal photographs or files will be stored on any Department issued mobile device, camera or recorder.

E. VIEWING OF DIGITAL EVIDENCE

Digital evidence that has been submitted and entered into the Department Digital Upload Terminal can be accessed via the Foray Digital Viewer. The Foray Digital Viewer is a web-based application available to Department personnel with administrative approval. The production of photographic prints for law enforcement purposes and court presentation may be requested from the Photo Lab as needed. Digital evidence that has been uploaded into Evidence.com can be accessed through www.evidence.com using designated credentials.

F. REPRODUCTION, PRINTING AND COPIES FOR COURT PURPOSES

Once uploaded, all digital evidence is maintained on a secure server using ADAMSWEB. Each file is saved and tracked in the system to ensure it remains unaltered. When provided for court discovery or use in a court proceeding, it is essential that all digital images and recordings be copied from the system, not from other sources. Digital photographs needed for court will be copied from Foray and uploaded to Evidence.com and may be requested through the Digital Evidence Unit.

G. RECORDS

Axon Evidence.com software ensures the integrity of digital media by creating an irrevocable audit trail of all digital evidence entered into the system. The Foray system used by CSI and the photo lab ensures that the original image has been preserved and unaltered with a hashing function and digital signature. Both systems maintain a chain of custody and generate reports related to the steps used to process a working copy of the original digital media (including lists of personnel who have viewed the digital evidence).

1. Evidence.com, as well as computers, upload terminals, and servers related to the Foray ADAMSWEB software are stored in a secured environment. The system is protected by locked doors and a fire suppression system. The system is password and firewall protected. User permissions are granted based on Department personnel assignments.
2. To prevent the loss of digital files in the event of a disaster, digital evidence is duplicated on separate servers and stored in an alternate, secure location.