


<b>POLICY 105.0</b>	<b>DIGITAL EVIDENCE PROCEDURES</b>	
	NEW: <b>06/11</b>	RELATED POLICIES: <b>105.2, 105.3, 110.1, EVIDENCE UNIT SOP</b>
	CFA STANDARDS: <b>18.06, 18.08, 35.02, 35.03, 35.05, 36.01, 36.02, 36.03, 36.04, 36.07, 36.08, 36.09</b>	REVIEWED:

**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 digital cameras and 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 intended for use in court presentations or other legitimate police functions. The Foray Authenticated Digital Asset Management System (ADAMS) 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.

**C. EXEMPTIONS**

Digital evidence collected and stored using other approved Department methods (i.e. in-car video recorders, Criminal Investigations Division interview room DVD recorders, 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. Department personnel will utilize FLPD Photo Identifier Card to document the date, time, location, case number and the photographer’s name and CCN number. This document will be the first photograph captured to identify the case the image(s) relate to. The Photo Identifier Card has a four-inch scale that can be utilized to put evidentiary items into perspective when captured in a photograph. Scales should be positioned on the same plane as the evidence they are associated with.
3. Digital video and audio recordings of statements made by victims, witnesses, and perpetrators shall be submitted as digital evidence.

4. Department personnel shall submit digital evidence via a Department Digital Upload Terminal. 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 the Digital Upload Terminal. Instructions for the submission of digital evidence will be made available at each Digital Upload Terminal.
5. Unless exigent circumstances exist, only Department issued digital equipment (cameras, video cameras and digital recorders) will be utilized to document evidence.
6. Any collected digital evidence shall be submitted prior to the end of the employee's shift unless authorized by a supervisor.
7. If digital evidence cannot be uploaded using a Digital Upload Terminal, the evidence must be immediately submitted to the Photo Lab. If Photo Lab personnel are unavailable, the evidence must be sealed in an envelope and deposited in the secured Photo Lab drop box.
8. Digital evidence will not be deleted or reformatted before it has been submitted to the Digital Upload Terminal. All evidentiary images will be uploaded into the system, regardless of whether the photo was taken unintentionally or is of poor quality.
9. Digital evidence will not be opened, viewed, downloaded or uploaded in any other device prior to their submission to a Digital Upload Terminal. The proper submission of digital evidence into the Digital Upload Terminal provides for a proper evidentiary chain of custody and authenticates the digital file for later use in court.
10. 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.
11. Department personnel will document the information pertinent to the identification, collection, processing, preservation and dissemination of the digital evidence in the appropriate police report.
12. The unauthorized reproduction, sharing and/or dissemination of digital evidence for personal use is prohibited.
13. No personal photographs or files will be stored on any Department issued camera or recorder utilized for the collection of evidence.

**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.

**F. REPRODUCTION, PRINTING AND COPIES FOR COURT PURPOSES**

Once uploaded, all digital evidence is maintained on a secure server using ADAMS. 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 photographic prints and copies for court may be requested through the Department Photo Lab.

**G. RECORDS**

The Foray Technologies ADAMS software ensures the integrity of digital media by creating an irrevocable audit trail of all digital evidence entered into the system. The Foray system ensures that the original image has been preserved and unaltered with a hashing function and digital signature. The system maintains a chain of custody and generates 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. Computers, upload terminals and servers related to the Foray ADAMS 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.