

Memorandum

**TO: ALL DEPARTMENT
PERSONNEL**

FROM: Edgardo Garcia
Chief of Police

**SUBJECT: DUTY MANUAL REVISIONS:
SEE SUBJECT BELOW**

DATE: July 27, 2020

Memo# 2020-032

SUBJECT

L 4420 DIGITAL EVIDENCE DEFINITIONS
L 4421 DIGITAL EVIDENCE – ACCEPTABLE FILE TYPES
L 4422 DIGITAL EVIDENCE CAPTURE
L 4423 DIGITAL EVIDENCE STORAGE

BACKGROUND

The Department is migrating to Evidence.com to store all digital evidence. The use of Digital CrimeScene (DCS) to upload digital evidence will cease. With the exception for CSOs, which will continue to use DCS until further notice. A review of Duty Manual sections L 4420 – L 4423 regarding digital evidence, revealed that it requires revision in order to incorporate new technology acquired.

ANALYSIS

The Duty Manual has been revised to reflect the following changes to Department policy regarding digital evidence. Additions are shown in italics and underlined. Deletions are shown in “strike through” form.

L 4420 DIGITAL EVIDENCE DEFINITIONS *Revised 08/03/20*

The following terms will be used in describing digital evidence:

- Original Digital Evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure, e.g. 1) An original audio file recorded to a memory storage device ~~compact flash memory module~~ or 2) A seized computer system with a hard drive containing its original information or 3) any image, video, audio or document digitally captured using the Department issued smartphone and uploaded to the digital Database or 4) any third-party vendor digital information acquired using their digital format/program (i.e. cell phone recovery programs).

- Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item, e.g. an exact duplicate of the original data but now stored on a separate piece of media or uploaded to the digital database via the Department issued smartphone or computer.
- Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item, e.g. an audio / image / video file that has been changed into a different file format but reproduces the same audio / image / video when played or displayed. This copy is to be properly documented as a converted file of the original digital evidence source.
- Image / Audio Enhancement: Any process intended to improve the visual appearance of any image or video or the sound quality of an audio file and properly documented as an enhancement of the original digital evidence source.

L 4421

DIGITAL EVIDENCE - ACCEPTABLE FILE TYPES

Revised 08/03/20

It is necessary to store digital evidence that can be used effectively by other law enforcement agencies and the District Attorney's Office. To do so, the following file types are used to store all digital evidence.

- STILL PICTURES
 - JPEG/JPG – (Joint Photographic Experts Group), pronounced 'jay-peg'. A compressed file format supported by Web browsers. The compressed file results in reduced image quality. This is the still photograph file type to be used under normal circumstances for general photographs such as people, general scene overviews, etc. (Naming scheme: filename.jpg)
 - ~~TIFF – (Tagged Image File Format) is a good format for saving all the details. This file format should not be compressed. It is used for scenes where greater detail of evidence is necessary. Example: shoe prints, detailed photos of a crime scene. (Naming scheme: filename.tif)~~
- AUDIO FILES
 - ~~WAV files are Microsoft Wave format handled by Windows Media Player. (Naming scheme: filename.wav)~~
 - MP3 files are audio files that are the most widely used file to run audio. (Naming scheme: filename.MP3)
- VIDEO FILES
 - MPEG (Moving Picture Experts Group) has a high output quality. It was developed as an international standard for use on CD-ROMs and other media that require quality digital video. (Naming scheme: filename.mpg)
 - AVI is a Microsoft Windows-oriented video format and is the preferred format for video files. (Naming scheme: filename.avi)

L 4422

DIGITAL EVIDENCE CAPTURE

(Revised 08/03/20)

Department issued smartphones using the vendor capture application, dDigital video recorders, including Department-issued body-worn cameras, still cameras, and audio recorders ~~may~~ should be used, when appropriate, to capture evidence. Some digital evidence may be captured onto ~~tape~~ external memory devices or DVDs. Such evidence (e.g. digital video) will be considered to be both the primary and original evidence, as defined in Section L 4420. These ~~tapes~~ external memory devices or DVDs will be handled in the same manner as other physical evidence.

Other digital equipment captures information onto “flash” memory. Flash memory may be stored on the digital device or it may be stored on a removable memory card. The evidence on the flash memory is considered the Original Digital Evidence as defined in DM Section L 4420. All digital evidence uploaded into ~~Dataworks™~~ the digital storage database is considered Original Digital Evidence.

~~Central Supply will issue each officer two photo cards that are used to capture digital photographs in the field. When an officer intends to use a digital camera in the field, it is the responsibility of that officer to insert the photo card into the camera and ensure that the card does not contain photographs from prior investigations. When an officer places a photo card into the camera, the format function must be performed to erase any existing photos before use.~~

Digital equipment that is personally owned by an officer, ~~excluding personally owned body-worn cameras, may~~ should not be used except in cases where Department issued equipment is not functioning or available, to collect evidence as long as it meets the minimum specifications set forth for evidence collection and where the evidence can be archived using the digital media computers provided by the Department.

- All digital audio files must be able to be converted to a WAV MP3 file
- Digital still pictures must be in JPG format. ~~or TIF~~ ~~Officer, excluding personally owned body-worn cameras, may be used to collect evidence as lo format~~
- ~~The following minimum resolutions are adhered to for still photos:~~
 - ~~Facial pictures: 1 mega pixel = 1280 X 960 dots per inch (dpi)~~
 - ~~Overall crime scene photos and pictures where some detail is needed. E.g. shoe prints: 3 mega pixel = 2048 X 1536 dpi or greater~~
 - ~~Detailed crime scenes such as officer involved shootings or homicides: 6.1 mega pixel~~
- Digital video must be able to be saved in AVI or MPG MP4 format. ~~The AVI format is preferred.~~

Vendor-provided cloud storage will be used to store body-worn camera data and all other digitally captured evidence.

L 4423 DIGITAL EVIDENCE STORAGE

Revised 08/03/20

1. AUDIO

- BUREAU OF FIELD OPERATIONS:

An officer who has recorded any audio using a Department issued smartphone will upload the audio file in accordance with established procedures.

~~An officer who has recorded an interview with a digital voice recorder will place the recorder in a docking cradle or use USB access located at any of the available Department computers. When the recorder is properly connected to the computer and the Dataworks™ icon is opened, a screen will automatically appear that will direct the officer through the appropriate steps for booking the recording as evidence.~~

- BUREAU OF INVESTIGATIONS:

An officer who has recorded any audio using Department issued smartphone will upload the audio file in accordance with established procedures.

Each Unit assigned within the Bureau of Investigations may have access to different methods or applications to record audio. Those digital files should be uploaded as evidence through the vendor application to the department's digital database unless designated by the unit to be stored elsewhere.

~~Each Unit assigned within the Bureau of Investigations will have access to their own media folder containing all voice recordings captured and booked pertinent to the Unit's mission. If an investigator wants to burn a copy of a digital voice recording from the media folder onto a CD for the case file or for court purposes, they will create a copy for the requesting party.~~

- Voice recordings captured in the field will be booked as evidence using the Department issued smartphone or in the manner described above using the vendor applications on the Department issued smartphone or computers ~~via the docking cradles or USB access.~~

- OTHER BUREAUS:

All other Bureau members will adhere to the above listed procedures for capture and storage of digital audio evidence.

2. DIGITAL PHOTOGRAPHS AND VIDEO (SMARTPHONES)

- BUREAU OF FIELD OPERATIONS:

Digital photographs and video collected on Department issued smartphones ~~photo cards~~ will be uploaded to the Department's digital storage database. ~~booked into Central Supply at the end of shift in the following manner:~~

- An officer who has recorded digital photographs via a Department issued ~~or personal camera and Department photo card~~ will ~~download and store the captured files~~ smartphone will upload the captured files prior to the conclusion of their shift.
- ~~Officers will use the USB access located at any of the available Department computers that contains the Dataworks™ Crime Scene Capture program. When the camera is properly connected to the computer and the Dataworks™ icon is opened, a screen will automatically appear that will~~

~~direct the officer through the appropriate steps for booking the digital photographs as evidence.~~

- Officers will use the installed software on the Department issued smartphones to upload the captured digital files into the Department's digital storage database for evidence.
- Officers using their own smartphone, external memory device or digital cameras are responsible for uploading the captured digital files into the Department's digital storage database for evidence downloading their images into Dataworks™ via the Crime Scene Capture program, or they may download the images to a CD for submission to the Photo Lab for entry into Dataworks™.
- BUREAU OF INVESTIGATIONS:
Revised 5/10/13
Each Unit assigned within the Bureau of Investigations will have access to their own media folder containing all digital photographs captured and booked pertinent to the Unit's mission for review. If an investigator wants to burn a copy of digital photographs from the media folder onto a CD for the case file or for court purposes, they will request a copy be made at the Photo Lab. Upon filing a case, Investigators should remove digital evidence from their media folder.
- Digital photographs captured in the field are booked in the same manner described in section L 4422 Digital Evidence Capture above.
- Efforts should be made to limit the number of photographs attached to a General Offense Report (Form 200-2-AFR) in Versadex. Images over 10 MB will not be attached.
- OTHER BUREAUS:
All other Bureau members will adhere to the above listed procedures for capture and storage of digital photograph evidence.

DIGITAL EVIDENCE RETENTION POLICY

All digital evidence will be subject to the retention policy set forth in The City of San Jose Retention Schedule. The current software program will automatically purge digital evidence stored within its database per The City's retention schedule. Digital evidence may be stored past the retention schedule through the current software program.

ORDER

The above stated changes to the Duty Manual are effective Monday August 3, 2020.



EDGARDO GARCIA
Chief of Police

EG:PC:RD:MB