I. Purpose

This Directive establishes guidelines and procedures for Division use of digital cameras.

II. Policy

All Division personnel using digital cameras for photographing evidence will do so in accordance with this directive.

III. Definitions

A. Primary Image: Refers to the first instance in which an image is recorded onto any media that is a separate, identifiable object or objects. Examples include a digital image recorded on a flash card or CD-R.

B. Original Image: An accurate and complete replica of the primary image, irrespective of media.

C. Archive Image: Either the primary or original image stored on media suitable for long-term storage. Examples include Compact Disc – Recordable (CD-R) and Digital Versatile Disc – Recordable (DVD-R).

D. Image Enhancement: Any process intended to improve the visual appearance of an image.

E. Processed Image: Any image enhanced to improve its visual appearance.

F. Digital Zoom: The zoom on digital still cameras which uses software interpolation to increase image detail. Software interpolation is the process of adding of information to an image through software to increase its quality.

G. Optical Zoom: The zoom on digital still cameras which use only true optical glass to magnify images.

H. Digital Imaging Workstation: Desktop computer dedication to digital image management.

IV. Capturing Digital Images - Images will be captured via digital cameras for documentation of crime scenes and any other non-criminal incidents where visual documentation is necessary. The images can be used to supplement testimony in court, aid in investigation and identify evidence.

V. Digital Imaging Equipment

A. Imaging will only be captured with cameras purchased by the Department. If another camera is used, the employee will note that fact in an official report.

B. Due to the unpredictable nature of law enforcement events, digital images from citizens/witnesses/suspects may be necessary for inclusion as evidence. The memory medium will be collected and booked into Department Property.

C. The IRT will note the images associated with this entry into the IRT report.

VI. Storage of Digital Images

A. The current system for storage of digital images is a locked evidence vault box assigned to each detective. ISS will be the depository for all digital images of an evidentiary nature. The ISS Sergeant will designate one detective to manage the digital image program. Two "original images" disk will be created as soon as possible by copying the images directly to serialized CD-R from the digital cameras.

B. In the event the images need to be downloaded for printing, mug shots or photo arrays, the following temporary storage will apply:

1. IRTs and Officers will download images to their assigned, secure "H" drive and note such in a report describing the circumstances and supporting the chain of custody.

2. Detectives and Sergeants will download images into their assigned, secure "H" drives, and advise the IRT supervisor of the process. They will complete a supplemental report documenting the action thus supporting the chain of evidence.

C. Images will be downloaded onto the stand alone imaging computer database in their ORIGINAL, UNALTERED state. Images downloaded onto the computer are now considered the ORIGINAL. Images on the memory card will be stored in the same manner as VI, A.

D. All images will be downloaded whether an image is out of focus or a frame is blank.

E. When downloading images to the secure photo database computer the user will enter information to provided fields and create a file for the images. Required information for file identification will be:

CASE NUMBER:	REQUIRED
EVENT #:	if necessary
TYPE OF CASE:	optional space for notations
DATE:	REQUIRED (date that images were take)
ID#	REQUIRED (ID# of person who downloaded the images)

VII. Distribution of Digital Images

A. Distribution of NON-CERTIFIED copies of digital images for court preparation, case investigation or internal investigations will be done by the following personnel only:
Investigative Services Commander
Investigative Services Sergeant
Detectives

1. Recipients of non-certified copies will be advised that these are non-certified, and the person who captured the image cannot testify as to the authenticity of non-certified copies.

2. Images not labeled as certified will be, by default, considered NON-CERTIFIED.

B. Distribution of CERTIFIED COPIES of digital images will be completed by Detectives ONLY.

1. Certified copies of digital images will be printed or labeled with a notice of certfication/evidence marker.

2. Certified copies may be introduced as evidence in a court of law.

C. Distribution may be accomplished by any of the following means:

1. Production of hard copy prints
2. Electronic Transfer (via e-mail)
3. Computerized digital storage medium

D. Authorization for distribution from citizens, defense attorneys, insurance companies, etc., will be accepted only via a subpoena. Records personnel will review these requests to confirm legitimate connection with the case. If needed, personnel may obtain a detective or supervisor's approval for the release. No images will be released to any news, television or outside press relations representative without prior authorization from the Chief of Police, or designee. At no time, will personnel make copies of photographs contained in a report for reasons other than those related to a pertinent investigation or action.

VIII. Use of Digital Images

A. No alterations of original images will be allowed.

B. Enhancement to images contained in the photo database are to be completed by Forensic Specialist ONLY, and for the following reasons only:

1. Contrast and Brightness
2. Color balance
3. Enlargement
4. Sharpness Enhancement
5. Adding tags and/or marks to highlight and/or identify an item within the image.

C. Enhancements to a copy of an image will be documented in a supplemental Report, completed by the Forensic Specialist.

D. Enhanced copies will be saved and downloaded into the photo database. The Forensic Specialist will use the TYPE OF CASE field in the file name graphic, to note the file contains enhanced copies.

E. An un-enhanced original will be maintained, in addition to any enhanced image.

IX. Security and Access to Digital Images

A. The photo database will be maintained by the IRT supervisor/System Administrator. The only access to configuration set up is by the Systems Administrator.

B. Access for distribution is as described and authorized in Section VI.

C. Access to archives images will be accessed by the System Administrator.

D. Access for viewing by civilians or citizens, will not be allowed, unless authorized reasons exist.

Approved Park Police Document
Signed Original on File

End of Directive