photographic evidence, the entire camera shall be inventoried as Digital Photographic Evidence.

B. Crime Lab Responsibility

- 1. On a routine basis, Crime Lab personnel will sign out Digital Photographic Evidence for processing.
- 2. A CD containing photographs from the SD memory card will be returned to the Property & Evidence Unit as the "original" evidence.
- 3. SD memory cards (or digital cameras) will be formatted by the Crime Lab and will be available for pick up by Precinct/Units for reuse.

C. Digital Camera/SD Card Repair, Replacement and Supplies

- 1. Digital cameras in need of repair shall be brought to the Crime Lab Unit.
- 2. Each precinct Inspector or his/her designee will be responsible for maintaining an adequate supply of SD memory cards for the digital cameras.
- 3. SD memory cards may be obtained from MPD Stores by completing Supply Requisition form (MP-4022), authorized by a Lieutenant or above.

4-218 MOBILE AND VIDEO RECORDING (MVR) POLICY (05/25/04) (9/19/08) (08/28/09) (08/01/11)

(A-D)

I. PURPOSE

The purpose of utilizing mobile video recording (MVR) equipment in Minneapolis Police Department vehicles is to:

- · capture video evidence for criminal, civil and traffic-related court cases.
- · assist officers with recalling facts or other details captured by the equipment that will help them accurately articulate a chain of events when writing reports.
- · allow supervisors to review the contents of the recorded media as a management tool within their chain of command.
- be used as a training tool for officer safety and best practices in the MPD.
- · assist in the assessment of contacts between officers and the public by reviewing procedures and interpersonal actions.

The content of this policy will provide MPD personnel with guidelines and procedures for the use, management, access, retention, handling of evidence, degaussing, storage, and retrieval of recorded media captured by MVR equipment.

II. POLICY

Minneapolis Police Department employees shall be responsible for performing assigned duties in accordance

with the Mobile Video Recording (MVR) System Policy and the MVR Operational Guide. All MPD employees who have access to the MVR systems shall receive training on these systems. Training may include, but not be limited to: department policy, directives, electronic or traditional classroom education. (08/01/11)

All stops and searches captured on the MVR are presumed to be legal and valid unless evidence indicates otherwise. (09/19/08) (08/28/09)

The term "officer" is used generically in this document and does not assume a level of rank, such as Patrol Officer. It includes all applicable sworn and non-sworn personnel. (08/01/11)

III. DEFINITIONS

Activate: Any process which causes the MVR system to record video or audio data. Activation may occur automatically due to a trigger event or be done manually.

"Categorize" an event: Term used to classify an event that has been recorded and for which a predetermined retention period has been set.

Critical Incident: An incident involving any of the following situations occurring in the line of duty:

- · The use of Deadly Force by or against a Minneapolis Police Officer;
- · Death or Great Bodily Harm to an officer;
- · Death or Great Bodily Harm to a person who is in the custody or control of an officer;
- · Any action by an officer that causes or is intended to cause Death or Great Bodily Harm.

Deadly Force: Minn. Stat. §609.066 states that: "Force which the actor uses with the purpose of causing, or which the actor should reasonably know creates a substantial risk of causing death or great bodily harm. The intentional discharge of a firearm other than a firearm loaded with less-lethal munitions and used by a peace officer within the scope of official duties, in the direction of another person, or at a vehicle in which another person is believed to be, constitutes deadly force."

Degaussing: Electronic cleansing by overwriting, erasing, and/or destruction of electronic storage media of analog and digital recording media that returns the media to it original state so it is ready for the imprinting of new images.

Designated Upload Site: Location where MVR recordings stored on media cards are uploaded to server through wireless transmission.

Great Bodily Harm: Bodily injury which creates a high probability of death, or which causes serious permanent disfigurement, or which causes a permanent or protracted loss or impairment of the function of any bodily member or organ, or other serious bodily harm.

Manual Activation: Activation of MVR equipment that is not caused by a trigger event. Officers may activate the MVR equipment at their own initiation or at the direction of a supervisor via the wireless microphone, in-car LCD monitor, or digital video recorder (DVR) box in the vehicle's trunk.

Manual Upload: In the event a digital MVR system is unable to wirelessly upload recordings, the digital memory card may be removed and manually uploaded by Crime Lab Unit personnel.

Mobile Video Recorder (MVR): Audio/video recording equipment designed for fixed installation in patrol vehicles that includes at a minimum, a camera, microphone, recorder and LCD monitor. Can be a VHS or digital system.

- · VHS: An electronic system for recording video and audio information on videocassettes.
- Digital: Digitized (text, graphics, audio, and video).

MVR Equipment Check: An audio/video test to ensure that the MVR equipment is in working order. This check shall include a test of the video and microphone recording components and a date and time check of the in-car LCD monitor.

MVR Operational Guide: Training manual/guide which outlines the protocol for operating the MVR system/equipment.

Pre-Event Recording: Video stored by the MVR system prior to activation. This is a configurable feature for the digital MVR system and is preset to record video prior to activation. The pre-event recording is included as part of the incident and is viewable during playback.

Record Mode: Any time MVR equipment is recording audio/video as indicated on the LCD monitor, wireless microphone and/or DVR.

Recorded Media: Audio-video signals recorded on any of several storage devices, including but not limited to, analog tape (VHS) or other portable digital storage devices (e.g. CD, DVD, hard drive, flash drive).

Significant Incident:Includes, but are not limited to, any of the following situations occurring in the line of duty:

- · Critical incident;
- · Domestic abuse incident interview;
- · Felony crime;
- · Pursuit;
- · Squad accident;
- · Any incident in which the officer or sworn supervisor believes the recording to be of evidentiary and/or administrative value;
- · The identity of someone in the video needs to be protected;
- · Man-made or natural disaster or act of terrorism;
- · Any event that an officer or supervisor believes should be brought to the immediate attention of police command staff;
- · Any time that a citizen makes allegations of police misconduct or discrimination during the incident.

Trigger Event: An event that causes the MVR system to begin a video and audio recording. Trigger events include the activation of emergency lights or vehicle collision sensor.

Wireless Upload: When the police vehicle is within range of the designated upload site, MVR (digital) recordings are automatically transferred over a wireless connection to a storage server.

IV. PROCEDURES / RULES / REGULATIONS

A. Conditions of Use (Digital and VHS Systems) (05/25/04) (09/19/08) (08/01/11)

- 1. MVR equipment installed in any MPD vehicle is the responsibility of the officer(s) assigned to that vehicle and shall be operated in accordance with MPD training, MPD policy and procedures, and the manufacturer's recommendations. (08/01/11)
- 2. When the activation indicator is illuminated, officers should be aware that activities are being recorded. (09/19/08) (08/28/09) (08/01/11)
- 3. Before placing any MVR-equipped vehicle in service, officers shall conduct an MVR Equipment Check

to ensure that the equipment is working properly. (05/25/04) (09/19/08) (08/01/11)

- a. MVR Equipment Checks conducted on the digital MVR system shall be categorized "90 Day Retention". (08/01/11)
- b. The officer's immediate supervisor shall immediately be notified of any missing or malfunctioning MVR equipment. (07/11/07) (08/01/11)
- 4. The driver shall wear the wireless microphone, verify that it is turned on and shall be responsible for ensuring that it is working properly throughout the shift. (07/11/07) (08/01/11)
- 5. Record Mode can be activated in the following ways: (08/01/11)
 - a. Automatically, when a trigger event occurs; (08/01/11)
 - b. Manually, by an officer via the wireless microphone, LCD monitor console, or digital video recorder (DVR) box in the vehicle's trunk. (08/01/11)
- 6. MVR equipment shall be in Record Mode: (08/01/11)
 - For every stop/contact where a motor vehicle is involved and shall record the stop/contact in its entirety. (04/11/07) (08/01/11)
 - · For domestic abuse incident interviews conducted inside or in close proximity to an MVR equipped vehicle. (08/01/11)
 - Any time a person is transported in a squad, regardless of the destination. This does not apply when an authorized ride-along is the only other person in the squad. When practical, officers shall begin recording when the person is placed in the squad, regardless if transportation begins immediately following activation. (06/09/15)
- 7. MVR equipment may be manually deactivated during non-enforcement activities, such as protecting accident scenes, traffic posts, and/or assisting motorists. (08/01/11)
- 8. MVR equipment shall not be manually deactivated for an arrest, DUI, Use of Force, traffic stop or a "Significant Incident" as defined in this policy. (08/01/11)
- 9. Any sworn supervisor can direct an officer to activate or deactivate MVR equipment.
- 10. Officers shall notify their immediate supervisor of any recorded event believed to be of value administrative review or training purposes. (08/01/11)
- 11. Officers shall inform those who ask, that video/audio recording equipment is in use. (04/11/07)
- 12. Nothing herein shall preclude MPD personnel from reviewing or using recorded data for the purposes of investigation or prosecution of crimes, or preparation of reports. Recorded data may only be used for training purposes with the approval of the Deputy Chief of Professional Standards. (09/19/08) (08/28/09) (05/24/13)
- 13. An MPD employee who is captured on or referenced in any recorded media, may review such data and use the data for any purpose relating to his/her employment, provided such use complies with the Minnesota Government Data Practices Act, MPD policy and other laws. (09/19/08) (08/28/09) (08/01/11)
- 14. All MVR recordings are the property of the MPD and original MVR recordings shall remain in the sole custody of the MPD, unless used in court as evidence, provided to an expert for analysis, or required to

be provided to another by lawful order. (08/28/09) (8/01/11)

- 15. An MVR-equipped vehicle can be used for off-duty employment with supervisor pre-approval. MVR-equipped vehicles and use of MVR equipment are subject to all requirements as outlined for on-duty use. (08/28/09)
- 16. Only MPD-issued videotapes, memory cards and microphones shall be used in MVR equipment. MPD Stores is responsible for distributing blank MVR media to the precincts and units. (08/28/09) (08/01/11)
- 17. Disabling MVR equipment and/or altering, duplicating or destroying MVR recordings is prohibited, except for authorized personnel. (08/01/11)
- 18. When reference is made to an MVR recorded event in a police report or supplement, the P# of the squad which captured the event shall be noted in the report. (05/24/13)

B. MVR System - Supervisor Responsibility (05/24/04) (09/19/08) (08/01/11)

- 1. Supervisors shall ensure that officers follow established procedures for the use and maintenance of MVR equipment, videotapes, and the completion of MVR documentation.
- 2. Supervisors shall periodically view recorded media to ensure proper procedures are being followed. (08/01/11)
- 3. Supervisors may review the contents of the MVR systems, as a management tool within their chain of command. (08/28/09) (08/01/11)

C. MVR Digital System (08/01/11)

- 1. Every recorded event shall be appropriately categorized in order to ensure proper data retention guidelines are followed.
- 2. Recorded events will be categorized using the following categories. Only one category can be chosen for each recorded event.
 - · 90 day retention;
 - · Citation;
 - · Arrest or DUI;
 - · Use of Force;
 - Significant Incident
- 3. MVR digital recorded events categorized as Arrest, Use of Force or Significant Incident shall be uploaded at designated upload sites by the officers assigned to the squad, prior to the end of their shift whenever possible.
- 4. When the display shows less than 4 gigabytes of available space, officers shall proceed to a designated upload site to upload recordings.
- 5. In the event a memory card which contains recording(s) needs to be removed from the DVR, only Crime Lab personnel are authorized to remove the memory card.
- 6. Only Crime Lab Unit personnel are authorized to remove a memory card from DVR equipment.

D. VHS System (05/25/04) (09/19/08) (08/01/11)

1. Only shift supervisors are authorized to possess a key to the MVR trunk vault. (08/01/11)

- 2. Only shift supervisors are authorized to load or unload videotape into the MVR. (08/01/11)
- 3. When the 30-minute warning light appears on the MVR overhead console display, officers shall notify their immediate supervisor and arrange to have the MVR videotape inventoried and replaced. (08/01/11)
- 4. If the original MVR recording is of evidentiary value, it shall be inventoried in the Property & Evidence Unit prior to the end of the officer's shift which encompasses the recorded event. A recording that is of evidentiary value includes the following: (08/28/09) (08/01/11)
 - a. Significant Incident;
 - b. Arrest;
 - c. DUI;
 - d. Use of force
- 5. MVR (VHS) recordings of non-evidentiary value will be stored at the precinct/unit where issued for a period of 1 year and then may be degaussed and re-used. (08/28/09) (08/01/11)
- 6. Exercise caution to ensure that repeated viewing of an original VHS recording is kept to a minimum. Repeated viewing may result in the quality of the recording to become degraded. (08/01/11)
- 7. In the event of a Critical Incident, Crime Lab personnel shall collect MVR VHS recorded media from all squads at the scene. (04/03/09) (08/28/09) (08/01/11)
 - a. In order to preserve the quality and integrity of the videotape, the recording shall not be reviewed in the squad car prior to collection. (04/03/09) (08/28/09) (08/01/11)
 - b. A duplicate copy of the VHS recorded media will be made as soon as possible by Crime Lab personnel. (04/03/09) (08/28/09) (08/01/11)
 - c. At the request of the Involved and/or Witness Officers, the Lead Investigator for the Critical Incident shall provide them an opportunity to view a copy of the MVR recorded media prior to giving a statement and completing a report. (04/03/09) (08/28/09) (08/01/11)

E. VHS System - Supervisor Responsibility (05/25/04) (09/19/08) (08/01/11)

- 1. Patrol supervisors are responsible for the installation, removal and storage of VHS videotapes. (08/01/11)
- 2. Precinct/Unit commanders or their designees are responsible for the usage, labeling, storage, degaussing, and recycling of VHS recordings intended for patrol use. (08/28/09) (08/01/11)
- 3. Unless otherwise noted, MVR VHS videotapes stored at precincts shall be retained for one year and then may be degaussed and/or reused. (08/28/09) (08/01/11)
- 4. Videotapes that have been degaussed three times shall be destroyed. (05/07/07) (07/11/07) (08/28/09) (08/01/11)
- 5. Supervisors shall maintain a logbook to ensure inventory control of videotapes.
- 6. Each precinct/unit shall track the installation/removal of MVR videotapes via the Precinct/Unit MVR Videotape Log (MP-8898). (08/01/11)

F. Property Inventorying MVR (VHS) Videotapes (05/25/04) (09/19/08) (08/01/11)

- 1. Mobile Video Recording (MVR) videotapes shall be property inventoried when the MVRequipment was in use in the following situations: (08/01/11)
 - a. Significant Incident;
 - b. Arrest;
 - c. DUI; and
 - d. Use of force
- 2. If the squad is involved in or responds to a Critical Incident:
 - a. Crime Lab Unit personnel will remove and property inventory MVR videotapes from all squads at the scene. (08/01/11)
 - b. MVR videotapes property inventoried for reasons related to a Critical Incident shall only be permanently released or destroyed by the Property and Evidence Unit at the direction of the Commander of the Internal Affairs Unit. (07/11/07) (04/03/09)
- 3. In cases where evidence is recorded, it shall be noted on the videotape and in the CAPRS report.

G. MVR Equipment Coordinator (08/01/11)

- 1. Each patrol precinct/unit will have a designated MVR Equipment Coordinator.
- 2. The MVR Equipment Coordinator will:
 - a. Ensure that all MVR equipment in vehicles is operational and accounted for;
 - b. Follow up when equipment and microphones are reported missing or in need of repair;
 - c. Conduct and/or coordinate training for personnel regarding MVR operations, MVR desktop software, and policy/procedure updates;
 - d. Liaison between the precinct/unit, the Business Technology Unit (BTU) and the Radio Shop;
 - e. Ensure videotapes from the MVR (VHS) system are maintained appropriately and requests for video duplication are handled in a timely manner.

H. MVR Equipment Maintenance, Repair and Replacement (05/25/04) (09/19/08) (08/01/11)

- 1. The Radio Shop is the liaison with the MVR vendor and will conduct all repair and replacement of MVR equipment, except wireless microphones. (08/01/11)
- 2. Officers are responsible for immediately notifying their supervisor of any missing or malfunctioning MVR equipment, including microphones. (08/01/11)
- 3. The supervisor is responsible for rectifying the problem by having the squad taken to the Radio Shop for repair as soon as it is practical. (08/01/11)
- 4. If a supervisor is notified of a missing microphone he/she shall make attempts to locate it. If it cannot

be located, this shall be reported to the precinct/unit MVR Coordinator who will again make attempts to locate it. (08/01/11)

5. If the microphone cannot be located the precinct/unit MVR Coordinator shall make a CAPRS report "Lost Property" and forward the report with a request for a replacement through his/her chain of command to the Business Technology Unit. (08/01/11)

I. Requests for Duplication of MVR Recordings (05/25/04) (09/19/08) (08/01/11)

- 1. Requests by MPD personnel for duplication of MVR video for purposes of official MPD business shall be directed to the Crime Lab Video Forensics section via submission of the Crime Lab Video Request for Services form (MP-9069).
- 2. Requests by MPD personnel for duplication of MVR video for non work-related purposes (e.g. teaching, personal reasons) shall be submitted to the Records Information Unit and are subject to the Minnesota Government Data Practices Act and City of Minneapolis data charges.
- Requests made by the public for MVR video will be processed by the Records Information Unit (RIU), in conjunction with Precinct Supervisors, the Crime Lab Video Forensics Section and the Public Information Office.
 - a. Records Information Unit responsibilities:
 - i. Determine nature of the request;
 - ii. Ensure video is not part of an active criminal or internal investigation;
 - iii. Submit Crime Lab Video Request for Services form (MP-9069) to the CLU requesting duplication of video;
 - iv. Receive recorded media intended for release;
 - v. Ensure the Public Information Office reviews video prior to release to make certain that only public information is released;
 - vi. Notify requestor video is ready;
 - vii. Collect fees and release video.
 - b. Precinct Supervisor responsibilities when an MVR VHS videotape recording is required for duplication:
 - i. Receive request from Records Information Unit;
 - ii. Locate and property inventory videotape;
 - · If no CCN exists, one shall be generated and a CAPRS report completed using the code MISC.
 - iii. Notify RIU via e-mail if the videotape is already inventoried under another CCN, if it no longer exists, or cannot be located.
 - c. Crime Lab Video Forensics Section responsibilities:

- i. Receive requests via Crime Lab Video Request for Services form (MP-9069).
- ii. Process requests according to Crime Lab Division SOP's.
- d. Public Information Office responsibilities:
 - i. Coordinate with Records Information Unit to manage requests.
 - ii. Review all videos to be released.

4-219 PROCUREMENT OF COMPUTER HARDWARE, SOFTWARE AND COMPUTER-RELATED SERVICES (12/21/01) (08/01/11) (09/19/08) (05/23/12)

(A-D)

The purpose of this policy is to ensure compliance with city Business Information & Technology Services (ITS) (BIS) hardware and software standards. (09/19/08)

The purchase or procurement of all computer hardware, software or computer-related services such as programming or consulting shall be facilitated through the supervisor of the MPD's Business Technology Unit (BTU). Any precinct, unit or division wishing to obtain or implement hardware, software or services shall submit a written request detailing specific needs and requirements, (including the Space ID and Asset Tag Number) to the BTU supervisor of the Business Technology Unit. The supervisor of the Business Technology Unit will evaluate the request and forward it to BIS ITS as appropriate. It is the responsibility of the requesting precinct, unit or division to make all necessary budgetary arrangements. (09/19/08)

All computer and related equipment (printer, scanner and accessories) procured by the MPD is managed by BIS ITS and may be subject to redeployment within the MPD based upon departmental needs. Computer equipment obtained through grant programs shall be maintained according to the grant guidelines.

Any computer equipment, software or service that is obtained outside of this procedure will not be supported by BIS ITS. All ongoing support, maintenance, repairs and upgrades shall be the responsibility of the purchasing precinct, unit or division. In addition, hardware/software that is obtained or purchased without the approval of BIS ITS may be removed from the network to prevent corruption or any adverse effect on the MPD or City network(s). (09/19/08)

Any employee found to have installed illegal or unauthorized copies of computer software may be subject to disciplinary action.

4-220 COMPUTER USE AND ELECTRONIC COMMUNICATION (12/21/01) (09/19/08) (08/01/11) (05/23/12)

(A-D)

All use of the City's computer system shall comply with the City of Minneapolis Electronic Communications Policy.

Users are responsible for maintaining security of any computer to which they have logged on. When users leave the computer, they shall log off the system.

Domain passwords are selected by individual users and are not to be shared. Users should protect their password against unauthorized use. Passwords can be stolen, guessed or inadvertently made available, therefore BIS will prompt users when to change their password. Users are required to change their passwords every 30 days and will have to supply a new password in order to log on. (09/19/08)