



Subject: <b>Patrol Operations - Mobile Data &amp; Audio Visual Devices</b>		
Distribution: <b>All Police Personnel</b>	Effective Date: <b>December 1, 2010</b>	Number of Pages: <b>Page 1 of 4</b>
Revision Date(s): <b>February 24, 2017</b>		

**1. Scope and Purpose**

This policy is directed to all police personnel within the Gulfport Police Department. Its purpose is to provide officers with guidelines for the use of mobile data and audio/visual recording equipment in patrol vehicles, and the management of media devices, to include body worn cameras, by employees of the Gulfport Police Department. All personnel will ensure that these devices are used for legitimate law enforcement purposes only.

**2. Policy**

The purpose of this policy is to provide officers and staff with guidelines for the use of mobile data and audio/visual recording equipment in patrol vehicles, the management of media devices, to include body worn cameras, by employees of the Gulfport Police Department. All personnel will ensure that the devices are used for legitimate law enforcement purposes only.

The Department recognizes that a video recording or image often has a limited field of view and cannot always show the full story or capture an entire scene. Therefore, the use of audio or video recording equipment does not reduce the need or requirement to provide thorough written documentation of an incident. In addition, the technology used in video recording equipment or devices, such as body worn cameras, cannot mimic the physiology of an officer at this time. An officer turning his or her head, focusing his or her vision on a particular object, or experiencing auditory exclusion might observe something not captured in audio or video recordings, or an officer might not observe something that is perhaps captured in an audio or video recording.

**3. Definitions**

- A. "Body Worn Camera" ("BWC") – A camera worn on an individual officer's person while in the performance of their duties that records and stores audio and video.
- B. "Digital Evidence" – MVR SYSTEMS files and data, including photographs, audio recordings and video footage, captured by a MVR SYSTEMS on an individual officer's person while in the performance of their duties and which is stored digitally on the MVR SYSTEMS and is capable of being subsequently transferred or downloaded.
- C. "Mobile Data Terminal" ("MDT") - is a computerized device used in police vehicles to communicate with dispatch.
- D. Mobile Audio/Video Recording (MVR) Systems – A combination of the in-car video system and the BWC camera system.
- E. "Recording Equipment" includes video recording devices, audio recording devices, and body worn cameras.
- F. "MVR System Coordinator" – A supervisor trained to handle MVR responsibilities, including, but not limited to, the MVR SYSTEMS Administrator.
- G. "MVR System Administrator" - Individual or Unit appointed by the Chief of Police within Department who has responsibilities or oversight set out in this General Order.
- H. "Law enforcement activity" – Any activity that is in furtherance of a law enforcement goal. These can include traffic stops, pedestrian stops, calls for service, follow up investigations, interviews, searches, crowd incidents, protests and arrests.

---

**RESTRICTED LAW ENFORCEMENT DATA**

The data contained within this policy is proprietary and will not be duplicated, disclosed, or discussed, without the written permission of the Chief of Police. Data subject to this restriction is contained throughout this policy.

General Orders Manual of the  
Gulfport Police Department

Policy Number	<b>4.7</b>
Page	<b>Page 2 of 4</b>
Date	<b>February 24, 2017</b>

**4. Mobile Data Terminal (MDT)**

**A. Software and passwords**

- 1) Personal software is not to be downloaded or installed on any MDT without approval from the Gulfport Information Technologies Division and written authorization from the Chief of Police.
- 2) Any unauthorized software may be removed from the device at random, and the department will not be liable for the loss of software. Employees may be liable for any damage caused by unauthorized software to the MDT.
- 3) Under no circumstance will external materials or applications be downloaded onto MDTs. To prevent viruses, no material shall be downloaded or installed from the Internet or other external sources such as the Rocket IOT Modem System.
- 4) Employees shall immediately notify their supervisor of any security breach, including compromised personal passwords.

**B. Usage**

- 1) Use of the MDT is restricted to official messages of a job-related nature only. Messages will not be personal in nature, contain derogatory references to other agencies, personnel, policies or contain any text a reasonable person would find offensive. Downloading or transmitting materials that contain obscene or disparaging language or graphics is strictly prohibited.
- 2) Expectation of Privacy. There is no expectation of privacy concerning sending or receiving messages on the MDT system.
  - a. Users will make only official inquiries, which relate to the official business of the department.
  - b. The MDT will not be used for personal or recreational purposes.
- 3) All users will check into service at the beginning of each shift by giving their assigned radio call sign and officer name via the standard MDT sign on the message screen.
  - a. Employees will keep their status updated at all times on the MDTs except in cases of emergency.
  - b. Employees will notify dispatch prior to logging off the MDT except in cases of emergency.
- 4) All users will sign off of the system at the end of their assigned shift or whenever leaving the terminal unattended. The MDT will be locked into its mount; the doors to any vehicle will be locked and secured whenever the MDT is left in the vehicle unattended.
- 5) MDT screens will be in the lowered position when the vehicle is in motion to avoid any unnecessary distractions.

**C. Confidentiality**

- 1) Release of confidential information to the general public that is accessible from the MDT is strictly prohibited. The general public includes family members, friends and civilians participating in the department's ride-along program that are not law enforcement employees.

All officers will take into account their surroundings to prevent any unauthorized view to MDT screens containing confidential information or unauthorized access to the MDT by the public or any non-sworn personnel. MDTs will not be left unattended in public places or residences at any time except in cases of extreme emergency.

---

**RESTRICTED LAW ENFORCEMENT DATA**

The data contained within this policy is proprietary and will not be duplicated, disclosed, or discussed, without the written permission of the Chief of Police. Data subject to this restriction is contained throughout this policy.

General Orders Manual of the  
Gulfport Police Department

Policy Number	<b>4.7</b>
Page	<b>Page 3 of 4</b>
Date	<b>February 24, 2017</b>

- 2) Confidential information will include, but is not limited to:
  - a. Criminal history information;
  - b. Intelligence files;
  - c. Software designed to conduct department business and software setups; and
  - d. Department files or databases.
- 3) Employees shall immediately notify a supervisor of any breach in confidentiality as it applies to the above criteria.

**5. Mobile Audio/Video Recording (MVR) Systems**

**A. Usage**

Officer safety and public safety take precedence over recording events. Officers shall follow existing officer safety policies when conducting enforcement stops. Officer safety and the safety of the public shall be the primary considerations when contacting citizens or conducting vehicle stops, not the ability to record an event.

All audio/video captured during the scope of an officer's duties are the property of the Gulfport Police Department and are subject to departmental policies and applicable laws regarding viewing, release, retention, and destruction.

The MVR System and all media captured, recorded or otherwise produced by either authorized or issued MVR SYSTEMS equipment are the sole property of the Gulfport Police Department and are subject to departmental policies and applicable laws.

Officers shall not intentionally edit, alter, erase, duplicate, copy, or otherwise distribute in any manner, any MVR system recordings without the written authorization and approval from the Chief of Police or his designee.

Requests for deletion of portions of the recordings (e.g. in the event of personal recording) must be submitted in writing and approved by the Chief of Police or his designee. All requests for deletion and final decisions shall be kept on file in the Professional Standards Bureau.

**B. Officer Responsibilities**

- 1) Prior to the end of each shift officers will ensure:
  - a. Video evidence is properly categorized with the case number for retention on the server. (Accidental, Miscellaneous, Misdemeanor, Felony, etc.)
  - b. That the camera is synced and docked for downloading video.
  - c. Indicate in their reports the existence of any body worn camera video.
  - d. Officers will inform their supervisor of any video that has significant evidentiary value or that may be utilized for training purposes.

**C. Supervisory Responsibilities**

- 1) Supervisors shall ensure that officers assigned a body worn camera utilize them in accordance with policy and procedure.
- 2) Supervisors will review MVR System video's periodically to ensure compliance.

---

**RESTRICTED LAW ENFORCEMENT DATA**

The data contained within this policy is proprietary and will not be duplicated, disclosed, or discussed, without the written permission of the Chief of Police. Data subject to this restriction is contained throughout this policy.

- 3) Supervisors will ensure all videos are uploaded to corresponding digital files and tagged for retention.
- 4) Supervisors may have the ability to resolve citizen complaints by reviewing video captured by an officer's body worn camera. In those circumstances where a complaint is resolved with no further action needed, the supervisor shall document their review.
- 5) Supervisors, where reviewing video should look for training opportunities to enhance officer performance. In addition, any video believed to benefit recruit and/or in-service training should be forwarded through the chain of command to the police academy.
- 6) Minor infractions of policy or procedure will be handled as a training issue and supervisors should use the opportunity to counsel with employees to ensure no future violations occur.

#### D. When and How to Use the MVR System

- 1) Officers will activate their MVR System to record all contacts that are conducted within the scope of an official law enforcement capacity.
- 2) Officers are not required to obtain consent from a private person when in a public place or in a location where there is no reasonable expectation of privacy. It is at the discretion of the officer to determine if they want to announce a recording is occurring.
- 3) While in public areas, officers are not required to advise a subject that they are recording their interaction unless the subject specifically asks if they are being recorded. At which point the officer will inform the subject that they are being recorded.
- 4) When officers are lawfully present in a private residence in an official capacity (warrant, consent, or exigent circumstances), there is no reasonable expectation of privacy. Therefore, officers are not required to give notice they are recording.
- 5) However, if asked, officers shall advise citizens they are being recorded. Officers are not required to initiate or cease recording an event, situation or circumstance solely at the demand of a citizen.
- 6) Prior to deactivating the MVR SYSTEMS, officers will make a recorded announcement as to the reason the device is being deactivated such as:
  - a. "Contact completed"
  - b. "Accident concluded"
  - c. "Instructed by supervisor (name) to end recording"
  - d. "Officer or supervisor discussion in the field"
- 7) If the MVR SYSTEMS fails to activate, the officer will document the failure in an incident report. The officer will also notify their supervisor of the equipment failure.
- 8) If an officer fails to activate the MVR SYSTEMS or the MVR System fails to record the entire contact, the officer will document the reasons in an incident report.

#### E. Remote Activation

Remote activation of MVR SYSTEMSs may only be allowed under the following circumstances:

- a. To view a critical incident as it is occurring; or
- b. For investigative purposes by the Professional Standards Bureau as directed by the Chief of Police

---

#### **RESTRICTED LAW ENFORCEMENT DATA**

The data contained within this policy is proprietary and will not be duplicated, disclosed, or discussed, without the written permission of the Chief of Police. Data subject to this restriction is contained throughout this policy.