Public Safety Video Surveillance System

332.1 PURPOSE AND SCOPE

This policy provides guidance for the placement and monitoring of agency public safety video surveillance, as well as the storage and release of the captured images.

This policy only applies to overt, marked public safety video surveillance systems operated by the Agency. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Agency.

332.2 POLICY

The Milwaukee County Sheriff's Office operates a public safety video surveillance system to complement its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance public safety and security in public areas. Cameras may be placed in strategic locations throughout the County to detect and deter crime, to help safeguard against potential threats to the public, to help manage emergency response situations during natural and man-made disasters and to assist County officials in providing services to the community.

Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

332.3 OPERATIONAL GUIDELINES

Only agency-approved video surveillance equipment shall be utilized. Members authorized to monitor video surveillance equipment should only monitor public areas and public activities where no reasonable expectation of privacy exists. The Sheriff or the authorized designee shall approve all proposed locations for the use of video surveillance technology and should consult with and be guided by legal counsel as necessary in making such determinations.

332.3.1 PLACEMENT AND MONITORING

Camera placement will be guided by the underlying purpose or strategy associated with the overall video surveillance plan. As appropriate, the Sheriff or authorized designee should confer with other affected County divisions and designated community groups when evaluating camera placement. Environmental factors, including lighting, location of buildings, presence of vegetation or other obstructions, should also be evaluated when determining placement.

Recorded video may be used for a variety of purposes, including criminal investigations and monitoring of activity around high-value or high-threat areas. The public safety video surveillance system may be useful for the following purposes:

(a) To prevent, deter and identify criminal activity.

(b) To target identified areas of gang and narcotics complaints or activity.

(c) To respond to critical incidents.

(d) To assist in identifying, apprehending and prosecuting offenders.

Exhibit 30

(e) To document deputy and offender conduct during interactions to safeguard the rights of the public and deputies.

(f) To augment resources in a cost-effective manner.

(g) To monitor pedestrian and vehicle traffic activity.

Video from each camera should be recorded in a manner consistent with the underlying purpose of the particular camera. Video should be transmitted to the Law Enforcement Analytics Division (LEAD). When activity warranting further investigation is reported or detected at any camera location, the available information should be provided to responding deputies in a timely manner. LEAD personnel are authorized to adjust the cameras to more effectively view a particular area for any legitimate public safety purpose.

The Sheriff or the authorized designee may authorize video feeds from the public safety video surveillance system to be forwarded to a specified location for monitoring by other than Sheriff's personnel, such as allied government agencies, road or traffic crews, or fire or emergency operations personnel.

Unauthorized recording, viewing, reproduction, dissemination or retention is prohibited.

332.3.2 INTEGRATION WITH OTHER TECHNOLOGY

The Agency may elect to integrate its public safety video surveillance system with other technology to enhance available information. Systems such as gunshot detection, incident mapping, crime analysis, license plate recognition, facial recognition and other video-based analytical systems may be considered based upon availability and the nature of agency strategy.

The Agency should evaluate the availability and propriety of networking or otherwise collaborating with appropriate private sector entities and should evaluate whether the use of certain camera systems, such as pan-tilt-zoom systems and video enhancement or other analytical technology, requires additional safeguards.

332.4 VIDEO SUPERVISION

Supervisors should monitor video surveillance access and usage to ensure members are within agency policy and applicable laws. Supervisors should ensure such use and access is appropriately documented.

332.4.1 PROHIBITED ACTIVITY

Public safety video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Public safety video surveillance equipment shall not be used in an unequal or discriminatory manner and shall not target individuals or groups based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

Video surveillance equipment shall not be used to harass, intimidate, or discriminate against any individual or group.

332.5 STORAGE AND RETENTION OF MEDIA

All downloaded media shall be stored in the designated cloud platform with access restricted to authorized persons. A recording needed as evidence shall be properly tagged and retained in accordance with the applicable records retention schedule. Refer to the Portable Audio/Video Records Procedure for additional guidance.

332.5.1 EVIDENTIARY INTEGRITY

Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

332.6 RELEASE OF VIDEO

All recorded video gathered by the public safety video surveillance equipment are for the official use of the Milwaukee County Sheriff's Office.

Recorded videos are classified as public records (Wis. Stat. § 19.32(2)). Requests for recorded video from the public or the media shall be processed in the same manner as requests for agency public records.

Requests for recorded images from other law enforcement agencies shall be referred to LEAD for release in accordance with a specific and legitimate law enforcement purpose.

Recorded video that is the subject of a court order or subpoena shall be processed in accordance with the established agency subpoena process.

332.7 TRAINING

All agency members authorized to operate or access public video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, interaction with agency operations and a review regarding relevant policies and procedures, including this policy. Training should also address state and federal law related to the use of video surveillance equipment and privacy.

Mobile Audio Video

419.1 PURPOSE AND SCOPE

The Milwaukee County Sheriff's Office has equipped marked patrol cars with Mobile Audio Video (MAV) recording systems to provide records of events and assist deputies in the performance of their duties. This policy provides guidance on the use of these systems.

419.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - Any process that causes the MAV system to transmit or store video or audio data in an active mode.

In-car camera system and Mobile Audio Video (MAV) system - Synonymous terms which refer to any system that captures audio and video signals, that is capable of installation in a vehicle, and that includes at minimum, a camera, microphone, recorder and monitor.

Recorded media - Audio-video signals recorded or digitally stored on a storage device or portable media.

419.2 POLICY

It is the policy of the Milwaukee County Sheriff's Office to use mobile audio and video technology to more effectively fulfill the agency's mission and to ensure these systems are used securely and efficiently.

419.3 DEPUTY RESPONSIBILITIES

Deputies assigned to a squad with MAVs will utilize the equipment to record audio and video in the field. At the end of the shift, each deputy will follow the established procedures for providing to the Agency any recordings or used media and any other related equipment.

At the start of each shift, deputies should test the MAV system's operation in accordance with manufacturer specifications and agency operating procedures and training.

System documentation is accomplished by the deputy recording his/her name and the current date and time at the start each shift. The deputy should playback the recording to ensure system function. If the system is malfunctioning, the deputy shall take the vehicle out of service unless a supervisor requests the vehicle remain in service.

419.4 ACTIVATION OF THE MAV

The MAV system is designed to turn on in a variety of ways. The system remains on until it is turned off manually. The audio recorder shall be utilized anytime the video recorder is activated.

419.4.1 REQUIRED ACTIVATION OF THE MAV

This policy is not intended to describe every possible situation in which the MAV system may be used, although there are many situations where its use is appropriate. A deputy may activate the system any time the deputy believes it would be appropriate or valuable to document an incident.

In some circumstances it is not possible to capture images of the incident due to conditions or the location of the camera. However, the audio portion can be valuable evidence and is subject to the same activation requirements as the MAV. The MAV system should be activated in any of the following situations:

(a) All field contacts involving actual or potential criminal conduct within video or audio range:
    1. Traffic stops (to include, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops)
    2. Emergency vehicle operation
    3. Vehicle pursuits
    4. Suspicious vehicles
    5. Arrests
    6. Vehicle searches
    7. Physical or verbal confrontations or use of force
    8. Pedestrian checks
    9. OWI investigations including field sobriety tests
    10. Consensual encounters
    11. Crimes in progress
    12. Responding to an in-progress call

(b) All self-initiated activity in which a deputy would normally notify Milwaukee County 911 Communications Division

(c) Any call for service involving a crime where the recorder may aid in the apprehension and/or prosecution of a suspect:
    1. Domestic abuse calls
    2. Disturbance of peace calls
    3. Offenses involving violence or weapons

(d) Any other contact that becomes adversarial after the initial contact, in a situation that would not otherwise require recording.

(e) Any transportion of a subject

(f) Any other circumstance where the deputy believes that a recording of an incident would be appropriate.

419.4.2 CESSATION OF RECORDING

Once activated, the MAV system should remain on until the incident has concluded. For purposes of this section, conclusion of an incident has occurred when all arrests have been made, arrestees have been transported and all witnesses and victims have been interviewed. Recording may be stopped during significant periods of inactivity such as traffic control away from an incident or other breaks from direct participation in the incident. If a recording is intentionally stopped, the member should make a verbal notation as to why prior to stopping the recording.

419.4.3 WHEN ACTIVATION IS NOT REQUIRED

Activation of the MAV system is not required when exchanging information with other deputies or during breaks, lunch periods, when not in service or actively on patrol.

No member of this agency may surreptitiously record a conversation of any other member of this agency except with a court order or when lawfully authorized by the Sheriff or the authorized designee for the purpose of conducting a criminal or administrative investigation.

419.4.4 SUPERVISOR RESPONSIBILITIES

Supervisors should determine if vehicles with non-functioning MAV systems should be placed into service. If these vehicles are placed into service, the appropriate documentation should be made, including a CAD entry

When an incident arises that requires the immediate retrieval of the recorded media (e.g., serious crime scenes, peace officer-involved shootings, agency-involved crashes), a supervisor shall ensure that recorded media is uploaded as soon as practicable.

Supervisors may activate the MAV system remotely to monitor a developing situation, such as a chase, civil disturbance or an event that may threaten public safety, officer safety or both, when the purpose is to obtain tactical information to assist in managing the event. Supervisors shall not remotely activate the MAV system for the purpose of surveillance regarding the conversations or actions of a deputy.

419.5 REVIEW OF MAV RECORDINGS

All recording media, recorded images and audio recordings are the property of the Agency, unless otherwise specified by an existing memorandum of understanding. Dissemination outside of the agency is strictly prohibited, except to the extent permitted or required by law.

Recordings may be reviewed in any of the following situations:

(a) For use when preparing reports or statements

(b) By a supervisor investigating a specific act of deputy conduct

(c) By a supervisor to assess deputy performance

(d) To assess proper functioning of MAV systems

(e) By agency investigators who are participating in an official investigation, such as a personnel complaint, administrative inquiry or a criminal investigation

(f) By agency personnel who request to review recordings

(g) By a deputy who is captured on or referenced in the video or audio data and reviews and uses such data for any purpose relating to his/her employment

(h) By court personnel through proper process or with permission of the Sheriff or the authorized designee

(i) By the media or public through proper process or with permission of the Sheriff or the authorized designee

(j) To assess possible training value

(k) An audio/video recording may have value for training purposes. If the Training Academy or other supervisor intends on using the recording for training, the supervisor or authorized designee shall receive the permission of any involved current member prior to training use.

In no event shall any recording be used or shown for the purpose of ridiculing or embarrassing any employee or citizen.

419.6 DOCUMENTING MAV USE

If a deputy is assigned to a vehicle with MAV equipment and becomes aware of a malfunction of the MAV or an incident is not recorded by MAV equipment, it shall be noted in the related incident report or CAD.

419.7 RETENTION OF RECORDINGS

All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 122 days.

419.7.1 IDENTIFICATION AND PRESERVATION OF RECORDINGS

To assist with identifying and preserving data and recordings, members should review their recordings and ensure the recordings are tagged appropriately.

419.8 SYSTEM OPERATIONAL STANDARDS

(a) MAV system vehicle installations should be based on officer safety requirements and vehicle and device manufacturer recommendations.

(b) The MAV system should be configured to minimally record for 30 seconds, prior to an event.

(c) The MAV system may not be configured to record audio data occurring prior to activation.

(d) Deputies using digital transmitters that are synchronized to their individual MAV shall activate both audio and video recordings when responding in a support capacity. This is to obtain additional perspectives of the incident scene.

(e) Deputies shall not erase, alter, reuse, modify or tamper with MAV recordings.

419.9 TRAINING

All members who are authorized to use the MAV system shall successfully complete an approved course of instruction prior to its use.

Portable Audio/Video Recorders

243.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of this agency while in the performance of their duties. Portable audio/video recording devices include all recording systems, whether body-worn, hand-held, or integrated into portable equipment (Wis. Stat. § 165.87).

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Milwaukee County Sheriff's Office facility, authorized undercover operations, wiretaps, or eavesdropping (concealed listening devices).

243.2 POLICY

The Milwaukee County Sheriff's Office may provide members with access to portable recorders, either audio or video or both, for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Agency by accurately capturing contacts between members of the Agency and the inmate population and critical incidents including uses of force in accordance with the law.

243.3 MEMBER PRIVACY EXPECTATIONS

All recordings made by members on any agency-issued device at any time, and any recording made while acting in an official capacity of this agency regardless of ownership of the device it was made on, shall remain the property of the Agency. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

243.4 MEMBER RESPONSIBILITIES

Prior to going into service, each member assigned a portable audio/video recorder will be responsible for making sure it is in good working order. If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner or otherwise notify persons that they are being recorded, whenever reasonably practicable.

The use of a portable audio/video recorder may not appropriate in certain assignment.(e.g. change-over).The use of a portable audio/video recorder may not be necessary in certain non-inmate contact assignments.(e.g. pre-book, jail records, AFIS)

When using a pool portable recorder, the assigned member shall record his/her name and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded.

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording. Members should include the reason for deactivation.

243.5 ACTIVATION OF THE AUDIO/VIDEO RECORDER

This policy is not intended to describe every possible situation in which the portable recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder at the beginning of their assignment and any time the member believes it would be appropriate or valuable to record an incident.

The portable recorder should be activated in any of the following situations:

(a) During all assignments with inmate contact except during changeover

(b) During all emergency situations

(c) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate detention interest in recording. Recording should resume when privacy is no longer at issue. A portable audio/video recorder should not be used in situations including but not limited to:

- A strip search or a body cavity search.
- During any change-over of clothing process (e.g. suicide gown, discipline change-over, clothing exchange)
- During any attorney-client privileged meeting
- During any court proceeding
- During the member's break-time, in a member restroom, or member locker room
- Inside the supervisors office

At no time is a member expected to jeopardize his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

243.5.1 CESSATION OF RECORDING

Once activated, the portable recorder should remain on until the end of the shift. Recordings may be stopped during significant periods of report writing if being completed in the roll call room. If a recording is intentionally stopped, the member should make a verbal notation as to why prior to stopping the recording.

243.5.2 SURREPTITIOUS USE OF THE PORTABLE RECORDER
Wisconsin law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Wis. Stat. § 968.31(2)(b)).
Members shall not surreptitiously record another agency member without a court order unless lawfully authorized by the Sheriff or the authorized designee.

243.5.3 EXPLOSIVE DEVICE
Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

243.6 PROHIBITED USE OF PORTABLE RECORDERS

Members are prohibited from using agency-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity.

Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with agency-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate agency business purposes. All such recordings shall be retained at the Agency.

Members are prohibited from using personally owned recording devices to record audio or video while on-duty without the express consent of the supervisor. Any member who uses a personally owned recorder for agency-related activities shall comply with the provisions of this policy, including retention and release requirements, and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

243.7 IDENTIFICATION AND PRESERVATION OF RECORDINGS

To assist with identifying and preserving data and recordings, Jail Lieutenants should review the daily recordings and ensure the recordings are tagged appropriately.

243.8 REVIEW OF RECORDED MEDIA FILES

A member will not allow a citizen or inmate to review a recording.

When preparing written reports, members should review their recordings as a resource (see the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct, or reports of meritorious conduct, or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

(a) Upon approval by a supervisor, by any member of the Agency who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation.

(b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

(c) By media personnel with permission of the Sheriff or the authorized designee.

(d) In compliance with a public records request, if permitted, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy). Recordings that unreasonably violate a person's privacy or sense of dignity should not be publicly released unless disclosure is required by law or order of the court (Wis. Stat. § 165.87(3)).

243.8.1 USE OF AUDIO/VIDEO RECORDINGS FOR TRAINING

An audio/video recording may have value for training purposes. If the Training Academy or other supervisor intends on using the recording for training, the supervisor or authorized designee shall receive permission of any involved current member prior to training use.

243.9 COORDINATOR

The Sheriff or the authorized designee should designate a coordinator responsible for (Wis. Stat. § 165.87):

(a) Ensuring members are trained in use of the equipment prior to deployment.

(b) Establishing procedures for the security, storage, and maintenance of data and recordings.

(c) Establishing procedures for accessing data and recordings.

(d) Establishing procedures for logging or auditing access.

(e) Establishing procedures for transferring, downloading, tagging, or marking events.

(f) Coordinating with the Training Director to provide training on this policy to:

1. Members who are authorized to use portable audio/video recorders.
2. Members of the Agency who use, maintain, store, or are responsible for the release of records and recordings.

(g) Periodically reviewing the Agency's practices relating to the use, maintenance, and storage of body cameras and data to confirm compliance with this policy.

243.10 RETENTION OF RECORDINGS

All recordings shall be retained for a period consistent with the requirements of the established records retention schedule but in no event for a period less than 120 days (Wis. Stat. § 165.87).

243.10.1 EXCEPTIONS TO RETENTION REQUIREMENTS FOR BODY-WORN CAMERAS
Exceptions to the 120-day retention period for body-worn cameras are as follows (Wis. Stat. § 165.87):

(a) Recordings should be retained until the final disposition of any investigation, case, or complaint to which the recordings pertain to any of the following:

1. Death or actual or alleged physical injury to any person in the recording
2. An encounter resulting in the use of force

(b) Recordings used in any criminal, civil, or administrative proceeding may not be destroyed except upon a final disposition from the court or hearing officer after a determination the recordings are no longer needed, or by an order from the court or hearing officer.

(c) Recordings may be retained for a period beyond 120 days if a request or directive to preserve the recordings is made before the expiration of that time period by a deputy from this agency or another law enforcement agency, member of a board of fire and police commission, prosecutor, defendant, or a court.

Public Records Unit

802.1 PURPOSE AND SCOPE

This policy establishes the guidelines for the operational functions of the Milwaukee County Sheriff's Office Public Records Unit. The policy addresses agency file access and external requests for documents.

802.2 POLICY

It is the policy of the Milwaukee County Sheriff's Office to maintain agency records securely, professionally and efficiently.

802.3 RESPONSIBILITIES

802.3.1 CUSTODIAN OF PUBLIC RECORDS RESPONSIBILITIES

The Sheriff or the authorized designee shall appoint and delegate certain responsibilities to a Custodian of Public Records. The Custodian of Public Records shall be directly responsible to the Administration Divisional Commander or the authorized designee. The responsibilities of the Custodian of Public Records include, but are not limited to:

- Overseeing the efficient and effective operation of the Public Records Unit.
- Scheduling and maintaining Public Records Unit time records.
- Ensuring compliance with established policies and procedures.
- Supervising the access, use and release of protected information (see the Protected Information Policy).
- Establishing security and access protocols for case reports designated as sensitive, where additional restrictions to access have been implemented. Sensitive reports may include, but are not limited to:
    - Homicides
    - Cases involving agency members or public officials
    - Any case where restricted access is prudent
    - Open investigations

802.3.2 PUBLIC RECORDS UNIT RESPONSIBILITIES

The responsibilities of the Public Records Unit include, but are not limited to:

(a) Maintaining a records management system for case reports.

(a) The records management system should include a process for numbering, identifying, tracking, and retrieving case reports.

(b) Entering case report information into the records management system.

1. Modification of case reports shall only be made when authorized by a supervisor.

(c) Providing members of the Agency with access to case reports when needed for investigation or court proceedings.

802.3.3 PUBLIC RECORDS UNIT PROCEDURE
The Custodian of Public Records should establish procedures that address:

(a) Identifying by name persons in reports.

(b) Classifying reports by type of incident or crime.

(c) Tracking reports through the approval process.

(d) Assigning alpha-numerical records to all arrest records

802.4 FILE ACCESS AND SECURITY

The security of files in the Public Records Unit must be a high priority and shall be maintained as mandated by state or federal law. All case reports including, but not limited to, initial, supplemental, follow-up, evidence and any other reports related to a sheriff's agency case, including field interview (FI) cards, criminal history records and publicly accessible logs, shall be maintained in a secure area within the Public Records Unit, accessible only by authorized members of the Public Records Unit. Access to case reports or files when Public Records Unit staff is not available may be obtained through the Shift Commander.

The Public Records Unit will also maintain a secure file for case reports deemed by the Sheriff as sensitive or otherwise requiring extraordinary access restrictions.

802.4.1 CASE REPORTS
Should a case report be needed for any reason, the requesting agency member shall first obtain authorization from the Custodian of Public Records. All case reports removed from the Public Records Unit shall be recorded on a designated report check-out log, which shall be the only authorized manner by which a case report may be removed from the Public Records Unit.

All case reports to be removed from the Public Records Unit shall be photocopied and the photocopy retained in the file location of the case report until the original is returned to the Public Records Unit. The photocopied report shall be shredded upon return of the original report to the file.

802.5 CONFIDENTIALITY

Public Records Unit staff has access to information that may be confidential or sensitive in nature. Public Records Unit staff shall not access, view or distribute, or allow anyone else to access, view or distribute any record, file or report, whether in hard copy or electronic file format, or any other confidential, protected or sensitive information except in accordance with the Records Maintenance and Release and Protected Information policies and the Public Records Unit procedure.

Records Maintenance and Release

803.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of agency records. Protected information is separately covered in the Protected Information Policy.

803.1.1 DEFINITIONS

Definitions related to this policy include:

Legal custodian of records - The person designated by the Agency as the legal custodian of records to fulfill all duties required by law, if no designation is made the legal custodian of records shall be the Sheriff (Wis. Stat. § 19.21; Wis. Stat. § 19.33).

Public records - Records that are not classified, restricted, confidential or private, and may be released by law, upon request.

Record - Any material on which written, drawn, printed, spoken, visual or electromagnetic information is recorded or preserved, regardless of physical form or characteristics, which has been created by or is being kept by an authority (Wis. Stat. § 19.32).

Record subject - An individual about whom personally identifiable information is contained in a record (Wis. Stat. § 19.32).

803.2 POLICY

The Milwaukee County Sheriff's Office is committed to providing public access to records in a manner that is consistent with the Wisconsin Public Records Law (Wis. Stat. § 19.31 through Wis. Stat. § 19.39).

803.3 CUSTODIAN OF RECORDS RESPONSIBILITIES

The Sheriff shall designate a Custodian of Records. The responsibilities of the Custodian of Records include, but are not limited to:

(a) Managing the records management system for the Agency, including the retention, archiving, release and destruction of agency public records.

(b) Maintaining and updating the agency records retention schedule including:

1. Identifying the minimum length of time the Agency must keep records.
2. Identifying the agency division responsible for the original record.

(c) Establishing rules regarding the inspection and copying of agency public records as reasonably necessary for the protection of such records.

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring a current schedule of fees for public records as allowed by law is available.

(g) Ensuring the prominent display of information regarding the agency's public records policy, including the procedure to request information, the established times and places to make requests or obtain copies of records, and the costs (Wis. Stat. § 19.34).

(h) Ensuring juvenile records are distinguished from adult records and stored separately.

(i) Establishing procedures for the destruction of both adult and juvenile records, when appropriate and in accordance with established retention schedules.

803.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any agency member who receives a request for any record shall route the request to the Custodian of Records or the authorized designee.

803.4.1 REQUESTS FOR RECORDS

The processing of requests for any record is subject to the following:

(a) Although not required by law, the Agency will send an initial receipt letter informing the requester that the request has been received and that it is being addressed. If the request is unreasonably broad or burdensome, the Custodian of Recordsshould ask the requester if he/she is willing to narrow or refine the request.

(b) The Agency is not required to create records that do not exist (Wis. Stat. § 19.35(1)(L).

(c) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released (Wis. Stat. § 19.36(6)).

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the agency-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

(d) The Custodian of Records shall determine if the requested record is available and, if so, whether the record is exempt from disclosure. Either the requested record or the reason for nondisclosure will be provided as soon as practicable and without delay (Wis. Stat. § 19.35(4)).

(e) If the request cannot be completed within 10 days from the initial date of request and unless unusual circumstances preclude doing so, the requester shall be notified in writing of the delay.

803.4.2 RECORDS INVOLVING THE REQUESTER

If a request is received from an individual or a person authorized by the individual who identifies him/herself and states that the purpose of the request is to inspect or copy a record containing personally identifiable information, the request shall be granted or denied access in accordance with Wis. Stat. § 19.35(4)(c).

All requests from criminal defendants and his/her authorized representatives, including attorneys, shall be referred to the District Attorney, Milwaukee County Corporation Counsel or the courts.

803.4.3 NOTICE REQUIREMENTS IN LIMITED CIRCUMSTANCES

If a record subject to Wis. Stat. § 19.356(2) or any portion thereof, is released, the Agency shall notify the affected individual before access is granted and within three days after making the decision to grant access (Wis. Stat. § 19.356(2)(a)).

Within five days after receipt of notice by the Agency, an individual may provide written notification of his/her intent to seek a court order restraining the Agency from providing access to the requested record (Wis. Stat. § 19.356(3)).

Within 10 days after receipt of a notice by the Agency, an individual may commence an action seeking a court order to restrain the Agency from providing access to the requested record (Wis. Stat. § 19.356(4)).

The Agency shall not provide access to the requested record within 12 days of sending a notice to an individual pertaining to that record. In addition, if the individual commences a court action, the Agency shall not provide access to the requested record during pendency of the action. The Agency shall not provide access to the requested record until any appeal is decided, until the period for appealing or petitioning for review expires, until a petition for review is denied, or until the Agency receives written notice from the individual that an appeal or petition for review will not be filed, whichever occurs first (Wis. Stat. § 19.356(5)).

803.4.4 DENIALS

The denial of a request for records is subject to the following:

If a written request is denied in whole or in part, the requester shall receive a written statement of the reasons for denying the request. The denial shall inform the requester that the written request for the record release determination is subject to review by a court or upon application to the Attorney General or a District Attorney (Wis. Stat. § 19.35(4)(b)).

803.4.5 RECORDS DESTRUCTION

No record shall be destroyed at any time after the receipt of a request for inspection or copying of the record until after the request is granted or until at least 60 days after the date that the request is denied or, if the requester is a committed or incarcerated person, until at least 90 days after the date that the request is denied.

If the Agency receives written notice that an action relating to a record has been commenced in court, the record may not be destroyed until after the order of the court is issued and the deadline for appealing that order has passed, or, if appealed, until after the order of the court hearing the appeal is issued. If the court orders the production of any record, and the order is not appealed, the record may not be destroyed until after the request for inspection or copying is granted (Wis. Stat. § 19.35(5)).

803.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address and telephone number; and medical or disability information that is contained in any driver license record, motor vehicle record or any agency record, including traffic crash reports, are restricted except as authorized by the Agency, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722; Wis. Stat. § 19.36(10)).

(b) Any record containing personally identifiable information that is collected or maintained in connection with a complaint, investigation or other circumstance and that may lead to an enforcement action, administrative proceeding, arbitration proceeding or court proceeding. This includes any record that is collected or maintained in connection with such an action or proceeding (Wis. Stat. § 19.35(1)(am)).

(c) Any record containing personally identifiable information that, if disclosed, could result in (Wis. Stat. § 19.35(1)(am)):

1. Endangering an individual's life or safety.
2. Identifying a confidential informant (Wis. Stat. § 19.36(8)).
3. Endangering security, including that of the staff or population of a detention facility.

(d) Any record that is part of a records series that is not indexed, arranged or automated in a way that the record can be retrieved by use of an individual's name, address or other identifier (Wis. Stat. § 19.35(1)(am).

(e) Any record with the home, school or work address of a participant in the Wisconsin Department of Justice Address Confidentiality Program (Wis. Stat. § 19.35(1)(am)2m).

(f) Crime victim and witness information (Wis. Stat. § 950.04).

(g) Juvenile-related information (Wis. Stat. § 938.396; Wis. Stat. § 48.78; Wis. Stat. § 48.396; Wis. Stat. § 938.78).

(h) Search warrants until they have been executed (Wis. Stat. § 968.21).

(i) Investigative information obtained for law enforcement purposes, when required by federal law or regulation to be kept confidential, or when confidentiality is required as a condition to receipt of state aids (Wis. Stat. § 19.36(2)).

(j) Information in employee personnel records (Wis. Stat. § 19.36(10)).

(k) Patient health care records (Wis. Stat. § 146.82).

(l) Records where the government's interest in nondisclosure outweighs the public's interest in disclosure.

803.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Custodian of Records for review and processing. While a

subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, Milwaukee County Corporation Counsel or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Agency and/or the Professional Standards Division so that a timely response can be prepared.

803.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the agency name and to whom the record was released.

Each audio/video recording released should include the agency name and to whom the record was released.

803.8 EXPUNGEMENT

Expungement orders received by the Agency shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall expunge such records as ordered by the court (Wis. Stat. § 973.015; Wis. Stat. § 938.355). Records may include, but are not limited to, a record of arrest, investigation, detention or conviction. Once the record is expunged, members shall respond to any inquiry as though the record did not exist.

803.9 SECURITY BREACHES

Members who become aware that any Milwaukee County Sheriff's Office system containing personal information may have been breached should notify the Custodian of Records as soon as practicable.

The Custodian of Records shall ensure the required notice is given to any person whose unsecured personal information is reasonably believed to have been acquired by an unauthorized person. If the breach involves more than 1,000 individuals, notice of the timing, distribution and content of the notices shall also be given to each consumer reporting agency (Wis. Stat. § 134.98).

Notice shall be given within a reasonable time, not to exceed 45 days, after the Milwaukee County Sheriff's Office discovers the breach. Notice may be delayed if notification will impede an investigation or homeland security (Wis. Stat. § 134.98).

For the purposes of the notice requirement, personal information includes an individual's first name or first initial and last name in combination with any one or more of the following (Wis. Stat. § 134.98):

(a) Social Security number

(b) Driver's license number or Wisconsin identification card number

(c) Full account number, credit or debit card number or any required security code, access code or password that would permit access to an individual's financial account

(d) The individual's DNA profile (as defined by Wis. Stat. § 939.74), or the individual's biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation

If the breach reasonably appears to have been made to protected information covered in the Protected Information Policy, the Custodian of Records should promptly notify the appropriate member designated to oversee the security of protected information (see the Protected Information Policy).

Protected Information

804.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the Milwaukee County Sheriff's Office. This policy addresses the protected information that is used in the day-to-day operation of the Agency and not the public records information covered in the Records Maintenance and Release Policy.

804.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the Milwaukee County Sheriff's Office and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

804.2 POLICY

Members of the Milwaukee County Sheriff's Office will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

804.3 RESPONSIBILITIES

The Sheriff shall select a member of the Agency to coordinate the use of protected information.

The responsibilities of this position include, but are not limited to:

(a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Transportation (DOT) records and the Transaction Information for the Management of Enforcement (TIME) system.

(b) Developing, disseminating and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy.

(c) Developing, disseminating and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information.

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

804.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Milwaukee County Sheriff's Office policy or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and will subject a member to disciplinary action up to and including termination and/or criminal prosecution.

804.5 RELEASE OR DISSEMENATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Custodian of Records for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Agency may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Public Records Unit to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of deputies, other agency members or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

804.6 SECURITY OF PROTECTED INFORMATION

The Sheriff will select a member of the Agency to oversee the security of protected information.

The responsibilities of this position include, but are not limited to:

(a) Developing and maintaining security practices, procedures, and training.

(b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.

(c) Establishing procedures and coordinating with the Information Management Services Division to provide for the preparation, prevention, detection, analysis, and containment of security incidents including computer attacks.

(d) Tracking, documenting, and reporting all breach of security incidents to the Sheriff and appropriate authorities.

804.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

804.6.2 DESTRUCTION OF CHRI

When any document providing CHRI has served the purpose for which it was obtained, it shall be destroyed by shredding in compliance with the organization's records retention schedule.

Each member shall be responsible for properly destroying the CHRI documents he/she receives.

804.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

Public Record Request Procedure

806.1 PURPOSE AND SCOPE

The purpose of this procedure is to provide the Milwaukee County Sheriff's Office's Records Custodian and other authorized members guidance in the process of responding to a public records request in compliance with Wis. Stat. § 19.34.

806.2 POLICY

The Wisconsin Public Records Law (Wis. Stats. §§ 19.21-19.39) provides that all persons are entitled to the greatest possible information regarding government affairs and the official acts of government officers. Although Wisconsin's Public Records Law is broad in scope and application, the public's right to access public records is not absolute.

806.3 PUBLIC RECORDS DEFINED

Public records are "any material on which written, drawn, printed, spoken, visual or electromagnetic information or electronically generated or stored data is recorded or preserved, regardless of physical form or characteristics, which has been created or being kept by an authority" (Wis. Stat. § 19.32(2)).

806.4 PROCEDURE

806.4.1 PUBLIC RECORDS REQUEST

Requests for public records can be made by:

- Email
- In person
- U.S. mail
- Fax

Upon receipt of a public records request, the request should be entered into the Public Records Database, which generates a number for each request. The requestor will receive a confirmation letter stating that the request has been received and is being addressed. Although there is no set time frame to respond to a public records request, the Agency must address a request as soon as practical and without delay. The Wisconsin Department of Justice recommends that 10 working days is generally a reasonable amount of time for responding to a simple request for a limited number of easily identifiable records. If the request is particularly large and complex, the Records Custodian or other authorized member should inform the requestor that it may take a longer than normal amount of time to process. If the request is unreasonably broad or burdensome, the Records Custodian or other authorized member should ask the requestor if he/she is willing to narrow or refine the request.

Once the records are located, the Records Custodian shall examine each record to see if any portions need to be redacted pursuant to statute or case law and if not, to apply the required balancing test to each individual record. The exceptions to disclosure will be dictated by circumstance. Common information statutorily exempted from disclosure includes Social Security numbers, employees' personally identifying information, and law enforcement records pertaining to juveniles (Wis. Stats. §§ 19.36(5), 10(a), (11), (13)). Determining whether a record should be disclosed under the balancing test requires a deep analysis of competing public policies. There are no blanket exceptions under the balancing test. Each record must be examined on a case-by-case basis.

If the request is denied, the requestor will receive a denial letter stating why the request has been denied. The requestor may file a petition for a writ of mandamus under Wis. Stat. § 19.37(1) or on an application to the attorney general or district attorney, or an action for mandamus (Wis. Stat. § 19.37(1)).

806.4.2 FEES

The requestor will receive a billing invoice along with his/her fulfilled request. Invoices may be paid by check to the address listed on the invoice. Invoices can also be paid in-person by check or cash in room 102 of the Safety Building. Fees may be waived on a case-by case basis.