3-07/260.30 - Access to Electronic Communications and Access Records

For the purpose of this section, “electronic communications and access records” includes all such records maintained or managed by the Sheriff’s Department, including but not limited to:

- E-mails;
- Internet access records, including any electronic transactions conducted using the Department’s internet access;
- Global Positioning System (GPS) forensic data from Mobile Digital Computers (MDC);
- Department phone records;
- Records of electronic requests sent through the Justice Data Interface Controller (JDIC); and
- Records or electronic requests sent through systems maintained by the Department.

This section does not mandate the maintenance of any records of electronic communications, nor does it modify or supersede any rule, regulation, or law regarding the retention of those records. This section only establishes a procedure for requests, processing requests, and certain access to electronic communications records which are maintained or managed by the Sheriff’s Department.

Units requesting information for electronic records pursuant to fulfilling an oversight agency request shall comply with the provisions in MPP section 3-04/040.10, Audit and Accountability Bureau Purpose and Authorization.

Requests for access to electronic communications and internet access records may be made to the Data Systems Bureau or Communications and Fleet Management Bureau by any division chief, division director, or a person of higher rank. The request must include the following:

- Name and rank of the requestor (concerned division chief, division director, or higher);
- Name and rank of the investigator authorized to receive the record(s);
- Name(s) and employee number(s) for the record(s) requested;
- Type of record(s) requested;
- Dates of the record(s) requested;
- Reason for the request. If the reason is for an internal investigation, the request should include an Internal Affairs Bureau (IAB) number, Watch Commander Service Comment Report (WCSCR) number, Policy of Equality (POE) number, and/or Uniform Report Number (URN). Valid reasons may also include inquiries, administrative reviews, and/or audits; and

- If the request is for GPS forensic data from the MDC, the request shall include an IAB number or WCSCR number. Risk Management Bureau's Traffic Services Detail requires only an URN number.

Additional Persons Authorized to Initiate Requests for Electronic Records

Based on a need for immediate response and/or an anticipated volume of requests, the following are exempt from the requirement for division chief, division director, or higher authorization. Under these exceptions, the designated person may make the request directly to the concerned unit commander or designee:

- Homicide Bureau - If investigations require immediate access to electronic records to pursue a homicide investigation, an on-duty homicide lieutenant may authorize the request. The homicide lieutenant must provide justification for the immediate need;

- IAB - If investigators require access to electronic records to pursue an internal administrative investigation, the IAB captain or lieutenant may authorize the request. The requestor must provide an IAB investigation number, URN, or other justification;

- Internal Criminal Investigations Bureau (ICIB) - If investigators require access to electronic records to pursue a criminal investigation, the ICIB captain or lieutenant may authorize the request. The requestor must provide an IAB investigation number, URN, or other justification;

- Civil Litigation Unit (CLU) - If investigators require access to electronic records in anticipation or preparation for a claim or lawsuit involving the Department, the Risk Management Bureau captain, or operations lieutenant may authorize the request. The requestor must provide identifying information about the claim or lawsuit;

- Audit and Accountability Bureau (AAB) – AAB is granted complete access to all Department records including electronic communications described under this section. The AAB captain or operations lieutenant may authorize requests for electronic records. The requestor must provide documentation pertaining to the inquiry; and

- Other emergency requests - Other emergency requests may be authorized by the concerned unit commander or designee upon presentation of sufficient explanation to justify the emergency.

Upon retrieval, an electronic copy of the requested records shall be made. The copy shall be released to the identified investigator. This copy may be maintained as long as needed for the investigation, inquiry, audit, or review. Any purge date on the original record shall not be changed without the concerned unit commander's approval; however, a verified copy shall be maintained until released for deletion by the requestor or their designee.

Once retrieval has been completed, handling personnel shall notify the following:

- The requestor;

- The investigator authorized to receive the record(s); and

- The concerned unit commander or designee.

Based on the request, all incoming requests and retrievals shall be logged by the receiving unit, including all information required for the request.