
	MESQUITE POLICE DEPARTMENT
	311.00 TEXAS LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM
	Effective Date: May, 2016
	Approved: _____  Chief of Police

I. Policy Statement

The Mesquite Police Department recognizes the importance of CJIS integrity as well as NCIC, TCIC, and warrant enforcement. These databases are maintained by other entities, but police operation is controlled by the Department. This policy stipulates how police employees will handle NCIC, TCIC and warrant entries and how to keep access terminals secure. Inquiries made to any database accessed through Departmental systems will only be for a legitimate law enforcement purpose.

II. Procedure

- A. All Public Safety Dispatchers shall read all TCIC and TLETS newsletters and all posted notices. All notices 2002 and later can be found on the TCIC website. A permanent file of notices prior to 2002 shall be maintained in the Communications Center for reference.
- B. Each terminal with TCIC/NCIC access shall be kept secure at all times to restrict access to authorized personnel only. Each person who has access will receive the required security awareness training within six months of employment and adhere to CJIS training policy thereafter.
- C. All problems relating to TCIC/NCIC will be forwarded to a Communications shift supervisor and the Terminal Agency Coordinator (TAC) for resolution.
- D. The department's participation in the TCIC/NCIC system is conditional upon adherence to policy as set out in the NCIC Operating Manual. The department is subject to audit by the DPS and/or FBI for compliance with all TCIC/NCIC policies.
- E. Information obtained through the TLETS system shall be requested and utilized for valid criminal justice purposes only. Unauthorized use of the TLETS system is a criminal offense (481.085 Texas Government Code) and may result in criminal prosecution as well as disciplinary action up to and including termination.
- F. Entering, maintaining, or validating inaccurate records can have serious consequences for the public and the department. Negligence in entering, maintaining, or validating these records may result in disciplinary action.
- G. Original Class C warrants are maintained and audited by the Municipal Court.

III. Who Can Request TLETS Information

- A. General
 1. Within the department, only commissioned officers and other authorized persons may request teletype inquiries of any kind.
 2. A request from outside the department may be honored at the direction of the Communications Supervisor, or a command level officer, when the identity of the requestor can be verified as a commissioned officer, or other authorized person (probation officer, parole officer, judge, prosecutor, etc.) who is making the request for a criminal justice purpose.
- B. Stolen and Wanted Information
 1. Stolen and wanted information can be requested by officers as needed. The information can be broadcast over the radio without restriction.
 2. A check will be made for TCIC/NCIC warrants on all incoming arrestees, and on all prisoners prior to their release, using all alias names, dates of birth, and identifying numbers.

3. When an NCIC inquiry yields a hit, the terminal operator will provide all available identifiers from the hit to the investigating officer. The terminal operator cannot confirm that the person or property being investigated is the same person or property identified in the hit. Only the investigating officer can make that determination.
 4. Hit confirmation will be obtained from the entering agency before taking any of the following actions on hits:
 - a. arresting the wanted person,
 - b. detaining the missing person,
 - c. seizing the stolen property.
- C. Criminal History Information
1. Criminal history information is confidential and certain restrictions apply to the purposes for which it can be requested and how it can be disseminated.
 2. Who can request Criminal History information:
 - a. Within the department, only commissioned officers and other authorized persons can request criminal history checks. These requests may be made through appropriate support personnel. Logging, as indicated below, is mandatory.
 - b. Requests from outside the department may be honored at the direction of the Communications Supervisor, or a command level officer, when the requestor can be verified as an authorized person as indicated in PART 10 of the NCIC Operating Manual, "Who May Access Criminal History Data." Logging, as indicated below is mandatory.
 3. Purposes for which Criminal History information can be requested:

A Computerized Criminal History (CCH) can only be requested for a criminal justice investigation or background investigation of a criminal justice applicant (applicant at the police department, sheriff's office, or other criminal justice agency, not at a non-criminal justice city or county office). It cannot be requested by anyone regardless of rank or status for any other purpose. Communications personnel will report to their supervisor any CCH inquiries known to be for unauthorized purposes.
 4. Logging of Criminal History inquiries:
 - a. The title, first, and last name of the requestor will be logged in the REQ field. The title, first, and last name of the person actually operating the terminal will be used in the OPR field. No initials or nicknames are allowed. The Request For Inquiry (RFI) field is mandatory and a specific reason shall be listed, along with the service, arrest, case or other number associated with the request. If the requestor is an authorized person from outside the department, his name and the name of their agency will be placed in the REQ field.
 - b. Each QR, IQ, FQ, and AQ transaction will be logged in the ATN field in the same manner as described above for the REQ field in the QH transactions.
 5. Dissemination of CCH information:
 - a. The Criminal history information obtained over the TLETS system will be given only to the person listed in the REQ or ATN fields, or in the written log. It may be passed to that person through an appropriate support person.
 - b. The officer receiving the information is responsible for keeping the printout secure and immediately returning it to the appropriate file or properly disposing of it.

- c. Any dissemination of Criminal History information outside the department must be logged in the manual log in the Communications Center (other than a routine dissemination to the District Attorney as part of the case file).
- d. An audit trail of the handling of Criminal History printouts within the department will be maintained by keeping the printout with the case file at all times, or by disposing of it immediately after its use when there is no case file.
- e. Officers requiring a printout of the CCH will advise the terminal operator to "Hold" the printout. The officer requesting the printout must sign the Disposition of Printout log that will be maintained in the Communications Section. If a printout is not requested the return will be shredded. When there is no longer a need for CCH printout, it shall be returned to the Communications Center for shredding.
- f. Broadcasting of CCH information on the radio:
 - (1) NCIC policy states that the radio will not be used routinely for the transmission of criminal history beyond that information necessary to effect an immediate identification or to ensure adequate safety for the officers and the general public.
 - (2) It is the officer's responsibility to request criminal history information over the air only when he has determined that there is an immediate need for the information to further an investigation, or there is a situation affecting the safety of an officer or the general public. The terminal operator will then broadcast details of the criminal history record.
 - (3) The terminal operator will not indicate over the radio whether or not a subject has a CCH in situations where the officer has not determined a need for the record information.
 - (4) Criminal History responses are possible indications only. Positive identification requires fingerprint comparison.

IV. Record Entry - Property

- A. Record entries will be made only by the Communications Section.
- B. Records will be entered only when a valid theft report is on file or other TCIC/NCIC entry criteria are met.
- C. The record will be entered as soon as possible after the theft report has been received.
- D. It is the Investigating Officer's responsibility to:
 - 1. Ensure that an official theft report is made,
 - 2. Ensure that all information in the theft report is accurate and that all required information is included, and
 - 3. Provide the information to the terminal operator as soon as possible.
 - 4. Ensure that the NCIC number is electronically recorded in the report within the records management system.
- E. It is the Terminal Operator's responsibility to:
 - 1. Verify the information meets TCIC/NCIC entry criteria.
 - 2. Verify vehicle registrations through DMV and boat registrations through the Parks and Wildlife Department.
 - 3. Coordinate with the investigating officer to obtain complete information when it is not on the report.
 - 4. Enter the record as soon as possible after receipt of a theft report.
 - 5. Bring to the attention of the shift supervisor any missing or incorrect data. Enter the record with available data, if possible, and modify the entry with additional data as soon as possible.

6. Double check the information on the screen before entry.
 7. Submit to a second authorized terminal operator for verification of entry.
 8. Provide the NCIC number to the reporting officer.
- V. Record Entry - Persons
- A. Records will be entered only when a valid warrant or missing person report is on file or other NCIC entry criteria are met.
 - B. The record will be entered as soon as possible after the warrant or missing persons report has been received.
 - C. It is the investigating officer's responsibility to:
 1. Make sure that an official warrant is issued or missing persons report is made.
 2. Make sure all information in the warrant or missing persons report is accurate and all required information is included.
 3. Obtain a forecast of extradition of wanted persons.
 4. Provide the information to the Communications Section as soon as possible.
(Missing Juveniles shall be entered within two hours of the initial call as required by the Adam Walsh Child Protection Act of 2006.)
 5. Ensure that the NCIC number is electronically recorded in the report within the records management system.
 - D. It is the Terminal Operator's responsibility to:
 1. Verify that the information in the warrant or missing persons report meets TCIC/NCIC entry criteria.
 2. Verify vehicle registrations through DMV, and identification information through DL and CCH checks. Include in the entry alias information from DL and CCH returns, but only when there is a high substantial degree of certainty that DL and CCH returns are for the subject of the warrant, i.e. pack the record with information.
 3. Coordinate with the investigating officer to obtain complete information when it is not included in the warrant or missing person report.
 4. Bring to the attention of the shift supervisor any missing or incorrect data. If possible, enter the record with available data, and modify the entry with additional data as soon as possible.
 5. Enter the wanted person record into TCIC only or into TCIC and NCIC, as indicated by the forecast of extradition.
 6. Double check the information on the screen before entry.
 7. Write the NCIC number, date, and terminal operator's initials on the warrant or missing persons report.
 8. Submit to a second authorized terminal operator for verification of entry.
 9. After second verification, the report is to be placed in the Records folder.
- VI. Hit Confirmation
- A. During NCIC/TCIC and Regional hit confirmation, whether this agency is requesting it from, or providing it to, another agency, the Department must accomplish the following:
 1. Ensure that the person or property inquired upon is identical to the person or property identified in the record.
 2. Ensure that the warrant, missing person report, or theft report is still outstanding.
 3. Obtain a decision regarding the extradition of the wanted person.
 4. Obtain information regarding the return of the missing person to the appropriate authorities.
 5. Obtain information regarding the return of stolen property to its rightful owner.
 - B. Confirmation requests of MPD records:
 1. The terminal operator on duty will reply to all non-regional requests for hit confirmations within the designated time frame listed on the teletype request.
 2. Current NCIC policy establishes two priorities for confirmation.

- a. Priority 1 - Urgent
Confirm the hit within ten minutes. In those instances where the hit is the only basis for detaining a suspect or the nature of a case requires urgent confirmation of a hit, the highest level of priority should be used.
 - b. Priority 2 - Routine
Confirm the hit within one hour. Generally, this priority will be used when the person is being held on local charges, property has been located under circumstances where immediate action is not necessary, or an urgent confirmation is not required.
- 3. If the terminal operator is unable to provide the positive or negative confirmation within the specified time, he will immediately send a message to the requesting agency giving them a specific amount of time needed to confirm or deny.
- 4. All confirmations will require a teletype. A "Hit" may be confirmed by telephone, but a confirmation by administrative teletype, or YQ, must follow.
- C. Confirmation requests to another agency for their records:
 - 1. It is the terminal operator's responsibility to:
 - a. Notify the officer of the hit, and give all identifiers available from the hit and confirmation in order that the officer can identify the person or property being investigated as the subject of the hit.
 - b. Notify the officer that confirmation is being requested.
 - c. Send a teletype to the agency that made the NCIC/TCIC entry using the established format (YQ) for requesting Hit confirmation. Upon request the operator will designate the priority of the request in the Hit Confirmation Request Number (RNO) field, and fully describe the person or property in custody. Regional warrants may be confirmed by phone.
 - d. If within the designated time frame the entering agency does not provide confirmation, or the specific amount of time they need to confirm or deny, the operator will send another YQ requesting confirmation to the agency, placing a number 2 in the RNO field:
 - e. If within 10 minutes after the second request the agency does not provide the confirmation, the operator will ensure a teletype is automatically generated and sent to the TCIC Control Terminal at DPS in Austin; to the NCIC Control Terminal in Washington, D.C.; and, if the entering agency is an out-of-state agency, to the entering agency's NCIC Control Terminal, at the NLETS ORI found in the back of the introduction of the NCIC Operating Manual. (Note- this does not apply to Regional warrant hits.)
 - 2. It is the officer's responsibility to:
 - a. Understand that the hit alone is not probable cause to arrest. The hit confirmed with the originating agency is one factor to be added to other factors at the scene to arrive at an arrest decision.
 - b. Understand the hit confirmation process and ensure that the person/property being investigated or in custody is the same as the person/property of the record.
- D. After a hit confirmation has been received from another agency, the terminal operator shall place a locate on that record, if it has not been cleared by the entering agency.
- E. Hit confirmation, together with investigative results developed at the scene, will be made before taking any of the following actions on hits:
 - 1. arresting the wanted person,
 - 2. detaining the missing person,
 - 3. seizing the stolen property.

- F. NCIC guidelines describe hit confirmation via teletype; however, there is no NCIC requirement that hit confirmation be written. Telephone hit confirmations will be accepted when teletype confirmation is impossible for some reason. The agency will be requested to follow-up with teletype confirmation when it becomes possible.
 - 1. The department will provide written hit confirmation to requesters whenever possible. If it is impossible for some reason, confirmation will be made over the phone with a teletype to follow when possible.
 - 2. Under no circumstances will a hit confirmation request made to this agency go unanswered.
 - 3. Failure to respond to an Urgent Hit Request within 10 minutes will be investigated by the on duty supervisor for possible disciplinary action.
- VII. Record Cancellation and Clear
 - A. Proper deletion of records which are no longer valid is a matter of high priority.
 - B. It is the officer's responsibility to:
 - 1. Notify the Communications Section as soon as possible when information becomes available indicating that a theft report or warrant is invalid.
 - 2. Notify the Communications Section as soon as possible when the property of a theft report is recovered, or a warrant is served, recalled, or in any other manner becomes inactive.
 - 3. Clearly mark the case files to indicate the status of the enclosed theft reports/warrants, and file appropriate hard copy teletype returns to document the status of the TCIC/NCIC records involved.
 - C. It is the Terminal Operator's responsibility to:
 - 1. Remove records from the system as soon as possible after being notified that the case has been cleared or that the record was invalid.
 - 2. Immediately bring to the attention of the shift supervisor any removal request for which a record cannot be located on the system.
 - 3. Ensure that a second operator verifies the removal of a record from the system and that the removal form has been acknowledged.
 - 4. Immediately follow up any discrepancies.
 - 5. Ensure the Municipal Court is promptly notified of any municipal court warrant discrepancies.
- VIII. Validation
 - A. Every month the DPS will electronically transmit one month's records that shall be verified for accuracy, validity, and completeness.
 - B. Validation (vehicle, boat, fugitives, and missing person entries) requires the originating agency to confirm that the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry file or other appropriate sources or individual. In the event the agency is unsuccessful in attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file.
 - C. Validation procedure:
 - 1. Upon receipt of the validation list, the pages will be numbered and copied.
 - 2. Copied pages will be given to the following personnel for verification:
 - a. Communications personnel responsible for performing the validation.
 - b. The Records Supervisor.
 - 3. The original validation list will remain in Communications for verification. The first year after the items/person is stolen/missing, the Records Supervisor will contact the complainant by generating a letter to be mailed to the complainant for verification that the report is correct. Each year thereafter, the record will be

validated by verifying there is not any documentation that the records should be removed from NCIC/TCIC.

4. If a reply is received from the complainant indicating the property has been recovered or corrections to the report need to be made, the Records Supervisor will notify the assigned Investigator, the TAC or TAC designee.
5. Communications personnel will verify the original validation list.
6. Communications personnel shall verify that all entries on the copied page of the Missing Persons file are accurate.
7. When copies are received in the Communications Center, the Terminal Agency Coordinator shall compare the validation and the copies. Any discrepancy will be corrected and the correction noted.
8. When validation is complete, the validation list shall be certified by the Terminal Agency Coordinator via the DPS website. The Terminal Agency Coordinator will direct activities to accomplish the validation by the stated deadline. Validation is a high priority records control function and all employees will assist the TAC as appropriate.
9. Two employees will be assigned to audit each validation for accuracy prior to submitting it to DPS. This will be done by taking random samples from each validation list and reviewing the records for accuracy. Any record that is found to be inaccurate will be corrected and the employee that validated that record may be subject to additional training and/or disciplinary action.

IX. Quality Control

- A. DPS and FBI will send quality control messages concerning errors in agencies' records.
 1. Messages from DPS
 - a. The terminal operator on duty at the time quality control messages are received will check MPD records for correctness and validity and respond to DPS. If the operator cannot resolve the problem, a message will be sent to DPS advising that we are looking into the problem. All messages will be forwarded to the Terminal Agency Coordinator and placed in the TAC folder.
 2. Messages from FBI/NCIC
Error messages from the FBI will be identified. The record will already have been canceled by FBI/NCIC. The terminal operator receiving the message will try to resolve the error and re-enter the record if possible, passing information to the shift supervisor. If the operator cannot resolve the problem, they will notify the shift supervisor of the error message.

X. CJIS Integrity Procedures

- A. Terminals
 1. CJIS, TLETS, TCIC and NCIC data shall be accessed ONLY from secure locations, which are those locations that are not open to the public.
 2. When transporting personnel who are not authorized to view protected information, officers shall take action to prevent unauthorized viewing of data. All vehicles containing MDCs shall be securely locked when not in use.
 3. TLETS terminal screens located in office space shall be positioned to prevent unauthorized viewing. The Department will maintain a roster of authorized personnel with unescorted access into physically secure areas. This roster will be maintained by the Planning and Research office.
 4. The local CJIS network equipment shall be located in a physically secure location.
 5. All computers used for processing CJIS data shall have anti-virus software installed and the latest available updates for the operating system.

6. No personal hardware or software shall be allowed on the agency's TLETS network.
- B. User Procedures
 1. Changes in authorized personnel should be immediately reported to the System Administrator.
 2. All printouts of CJIS data shall be promptly filed or shredded per city policy.
 3. All storage media containing or used for CJIS data that is no longer used shall be secure-formatted using methodology that over-writes all data in three iterations or degaussed prior to disposal or release for reuse by unauthorized personnel; if no longer needed, media will be destroyed.
 4. Inoperable electronic media shall be physically destroyed. Sanitation or destruction will be witnessed or carried out by authorized personnel. This task will be conducted by the city of Mesquite IT department.
 5. The IT department shall keep a list of all computers so that devices can be promptly disabled, should the need arise.
 6. It shall be the responsibility of each authorized user to report any violations of this security policy.
 7. The agency shall establish a Security Alert and Advisories process. This will be the responsibility of the IT department.
 8. All personnel will be required to complete CJIS training every two years.

EFFECTIVE: September, 1990; REVISED: January, 1996; REVISED: March, 1997; REVISED: November 1999; REVISED: August, 2003; REVISED: August, 2011; REVISED: March, 2013; REVISED: April, 2014; REVISED: June, 2015; REVISED: May, 2016