



# TYLER POLICE DEPARTMENT

## GENERAL ORDER: 23.800

	<b>TELETYPE SYSTEMS</b>	
	<b>EFFECTIVE DATE: 08-13-1994</b>	
	<b>REVISED DATE: 01-10-2023</b>	
<b>CALEA STANDARDS: 74.1.3</b>		

### 23.801 PURPOSE

The Tyler Police Department has computer links with local, state, and federal criminal justice information systems. All members of the Tyler Police Department will abide by all laws of the United States and the State of Texas, and will abide by all present or hereinafter approved rules and policies and procedures of the Federal Bureau of Investigation to include operations of: National Crime Information Center (NCIC), Texas Crime Information Center (TCIC), Motor Vehicle Division (MVD), Texas Law Enforcement Telecommunications Systems (TLETS), Federal Regulations and National Law Enforcement Telecommunications Systems (NLETS) etc., concerning the collection, storage, processing retrieval, dissemination, and exchange of criminal justice information.

### 23.802 GENERAL

- A. All users of the teletype system(s) will be advised of any changes / modification of procedures / operations of **NCIC/TLETS** by the Department's Terminal Agency Coordinator.
- B. All telecommunicators will have access to the **TCIC/NCIC** Newsletter via the [DPS TCIC 2000 Project website](#). The newsletter will be published through PowerDMS in order to maintain a record of receipt.
- C. The teletype terminals located within the Department shall be kept secure at all times. No employee's personal computer / device (i.e. laptop, cellphone, etc.) or publicly accessible computer / device shall be permitted access on the Department's **NCIC/TLETS** network. Furthermore, access to the Department's network will be restricted to only trained and authorized personnel who have submitted to and passed a national fingerprint based background check.
  1. All sworn personnel and designated non-sworn personnel with full or less than full access shall undergo training within six months and biannual after

that regarding the authorized use of the system as required by **TCIC/NCIC** policies are procedures.

2. Criminal Justice Practitioners (e.g. Administrative Personnel, Data Management) and all other department personnel who may come in contact with **TCIC/NCIC** information, but are restricted from accessing the system shall undergo a one-time basic **TCIC/NCIC** training course. The training will focus on the sensitivity and release of the information.
- D. The department's participation in the **TCIC/NCIC** system is conditional upon adherence to policy as set out in the NCIC Operating Manual and applied through these guidelines. This agency is subject to audit by the DPS and/or FBI on a biennial basis for compliance to all **TCIC/NCIC** policies.
- E. Visitors must be accompanied by a CJIS authorized Department member when in any area where hardcopy CCHs or TLETS connections are in normal use. These areas are designated by the posting of "*Authorized Personnel Only*" signs on entry doors.
- F. Non-law enforcement personnel shall be restricted from viewing CJIS information on the screen of any in-car computer.
- G. All law-enforcement vehicles containing MDTs shall be securely locked when not in use.

#### 23.803 QUALITY CONTROL

- A. DPS & FBI will send quality control messages when they find errors in agencies' records.
  1. Messages from DPS:
    - a. The communications operator on duty at the time any of these messages are received will resolve the problem at the time, if possible, and will forward the messages to the communications supervisor. If the operator cannot resolve the problem, they will send a message to DPS advising that the problem is being addressed. A supervisor will be notified of the problem. If Tyler Police Department (TPD) records reflect correct procedural application, the communications operator will notify DPS that TPD records show the entry to be valid, and forward all messages to the Terminal Agency Coordinator.
  2. Messages from FBI/NCIC:
    - a. Error messages from FBI will have "\$.E>" at the top of the message. The record will already have been canceled by FBI/NCIC. The communications operator on duty at the time will try to resolve the error and re-enter the record if possible, passing the information to

the terminal agency coordinator. If the communications operator cannot resolve the problem, they will notify the communications supervisor of the "\$.E." message.

#### 23.804 VALIDATION

- A. Each month DPS will electronically notify the communications unit of the records that we must verify as accurate and complete.
- B. The definition and procedure of validation is as follows:
  - 1. Validation (i.e. vehicle, boat, fugitives, missing person entries, and protective orders) requires the entering agency to confirm 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 files, or other appropriate sources or individual. In the event the entering agency is unsuccessful in its attempt to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available on whether to retain the original entry in the file.
  - 2. The established procedure must be formalized and copies must be on file for review during **TCIC/NCIC** audits.
  - 3. This procedure applies only to records in the Vehicle, Boat, Wanted Person, Missing Person files, and Protective Orders. NCIC has advised that the re-contacting of complainants, prosecutors, or courts does not have to be concurrent with the validation mailing, but re-contact must be made within approximately **90 days** after entry, and annually thereafter, to comply with NCIC guidelines. There is no requirement that this "*recent consultation*" be by phone, a system of written notification may be used if that is more preferable.
  - 4. The Terminal Agency Coordinator (TAC) will direct activities to accomplish the validation by the stated deadline. The TAC will send out a monthly list of entries to the appropriate investigative division for their review, to ensure the cases are still outstanding and the entries are accurate and need to remain in NCIC. Validation is a high priority records-keeping control and all employees will assist the TAC as appropriate.

#### 23.805 HIT CONFIRMATION

- A. The Tyler Police Department telecommunicator receiving a request for warrant confirmation has a responsibility, whether the request is from another agency or an officer in the field, to 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 and the record is valid;
  3. Obtain a decision regarding the extraction of the wanted person from the system;
  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; and
  6. The telecommunicator will be especially careful to ensure that the person or property in custody is the same as the person or property in the theft report or warrant, regardless of whether we are requesting the confirmation ourselves or replying to another agency's request for confirmation on one of the Departments records.
- B. When the Department is asked for hit confirmation on our records:
1. The telecommunicator will reply to all requests for hit confirmation within **10 minutes**. If they are unable to provide the positive or negative confirmation within the prescribe time, they will immediately send a message to the requesting agency giving them a specific amount of time needed to confirm or deny.
  2. The department will confirm all hits by reviewing the original case report or warrant to accomplish the six (6) six items listed in the above sub-section.
- C. When the Department requests another agency for confirmation of one of their records:
1. It will be the telecommunicator's responsibility to follow **TCIC/NCIC** guidelines for this confirmation. Under no circumstances will this agency permit a hit confirmation request directed to this department to go unanswered.
  2. It will be the officer's responsibility to:
    - a. Understand the hit alone is not probable cause to affect an arrest.
    - b. Understand the hit confirmation process and that they are responsible for ensuring that the person / property in custody is the same person / property of the record.
    - c. Obtain a hit confirmation from the entering agency before taking any action.

- 1) For immediate action, confirmation can be verbal or in writing. The confirming agency must follow up with a confirming teletype message.

#### 23.806 ENTRY OF RECORDS - THEFTS

- A. Records will be entered only when a valid theft report is on file or when other **TCIC/NCIC** criteria are met. This will be completed by the Communications Unit.
- B. The record will be entered as soon as possible after the report has been filed.
- C. It will be the officer's/investigator's responsibility to:
  1. Complete an official theft report, and ensure other entry criteria are met;
  2. The report information is accurate and includes all required information; and
  3. Provide this information to the telecommunicator in a timely manner.
- D. It will be the Telecommunicators responsibility to (prior to entry):
  1. Verify the information meets **TCIC/NCIC** criteria;
  2. Verify vehicle registration through MVD and through Parks and Wildlife for boats;
  3. Notify the Communications Supervisor if data is missing. Enter the data with available data, if possible;
  4. Confirm information on screen before actual entry to **TCIC/NCIC**; and
  5. Place in a proper holding file and to include date, operator's name, and hard copy of entry.
- E. It is a Communications Unit Supervisor's or their designee's responsibility to:
  1. Verify the validity of the record.
  2. Complete review of all information against the actual report.
  3. Ensure entry to **TCIC/NCIC** in a timely manner.
  4. Coordinate with the reporting officer / investigator when information is incomplete.

#### 23.807 ENTRY OF RECORDS - PERSONS

- A. Records will be entered only when a valid warrant or missing persons report is on file or when other **TCIC/NCIC** criteria are met.

- B. The record will be entered as soon as possible after the report has been filed.
- C. It will be the officer's / investigator's responsibility to:
  - 1. Complete a warrant or missing person report.
  - 2. Ensure the information is accurate and complete.
  - 3. Obtain a forecast of extradition for wanted persons.
  - 4. Provide this information to the telecommunicator in a timely manner.
- D. It will be the telecommunicator's responsibility to (prior to entry):
  - 1. Verify the information meets **TCIC/NCIC** criteria.
  - 2. Verify vehicle registration through MVD, DL and CCH checks.
  - 3. Notify a Communications Unit Supervisor if data is missing or incorrect.
    - a. This shall including alias information only when there is a high degree of certainty that the DL and CCH returns are for the wanted person.
    - b. If possible, enter the record information with available data.
  - 5. Confirm information on the screen before actual entry into **TCIC/NCIC**.
  - 6. Place information in the proper holding file that includes the date, operator's name, and a hard copy of the **TCIC/NCIC** entry.
    - a. Forward a copy of the information to the officer / investigator for inclusion in the case file.
  - 7. Enter the wanted person into **TCIC/NCIC**, and specify extradition or transportation as indicated.
- E. It is the Communications Unit Supervisor's or their designee's responsibility to:
  - 1. Verify the validity of the record.
  - 2. Conduct a review of all record information against the actual report or MVD, DL, CCH; include **TCIC/NCIC** as appropriate.
  - 3. Ensure entry to **TCIC/NCIC** in a timely manner.
  - 4. Coordinate with the reporting officer / investigator when information is incomplete.

23.808 HANDLING OF INFORMATION OBTAINED OVER THE TLETS TERMINAL

- A. Who can request information?
1. Within the Department, only sworn employees and authorized non-sworn employees can make inquiries of any nature.
  2. Requests from outside the Department will be honored only when the requestor is identified as a commissioned police officer or an authorized person (e.g. judge, probation officer, parole officer, etc.).
    - a. In the event the requestor is from a different agency, the telecommunicator will use the requesting agency's ORI number.

**NOTE:** Access will be granted for official, criminal justice purposes ONLY.

- B. Stolen and wanted information:
1. Stolen and wanted information can be requested by sworn employees as needed. Dissemination logging is not required. Information can be provided over the radio if requested.
  2. All arrested persons will be checked through **TCIC/NCIC** prior to being released. These checks may include alias names, dates of birth, and/or other identifying information as necessary.
  3. When a **TCIC/NCIC** hit is indicated, the telecommunicator will log on and this printout the following:
    - a. How,
    - b. When, and
    - c. To whom the information was given.
  4. The telecommunicator shall make a notation that includes their initials / name and date before forwarding the information to inquiring officer or agency for inclusion into its case file.

- C. Criminal History Information:
1. Criminal history is confidential and certain restrictions apply regarding its dissemination.
  2. Who can request Criminal History Information?
    - a. Within the Department, only sworn employees and authorized non-sworn employees can make requests for criminal history information (CCH).

- 1) Logging of the request is mandatory.
- b. Requests from outside the Department will be honored only when the requestor can be verified as a commission police officer or authorized person (e.g. judge, probation officer, parole officer, etc.).
  - 1) Logging of the request and the use of the requestor's ORI number is mandatory.
3. Purpose for which a CCH can be requested:
  - a. The request must involve a criminal justice investigation or an investigation of the background of a criminal justice applicant (i.e. applicant at the police department or other criminal justice agency). A non-criminal justice entity cannot have access to this agency's **TCIC/NCIC**.
    - (1) All Users are required to report any unauthorized inquiry / dissemination violation to a Telecommunications Shift Supervisor.
    - (2) Inquiries for unauthorized purposes or persons by any person is strictly prohibited.
    - (3) The reason for inquiry must be logged in the RFI field and specific in nature (e.g. case number, theft suspect, homicide suspect, etc.).
  - b. Department personnel violating **TLETS/NLETS, TCIC/NCIC** policies and procedures are subject to administrative and/or criminal penalties based upon the severity of the abuse. Violations may result in any of the below listed disciplinary outcomes:
    - 1) Counseling;
    - 2) Oral Reprimand;
    - 3) Written Reprimand;
    - 4) Suspension; or
    - 5) Termination.
4. Logging of CCH inquiries:
  - a. Each QH transaction will be logged in the REQ field. The actual rank, name (not initials) of the employee, and assigned identification number can be used.



- 1) No generic entries shall be permitted (e.g. DA Office, Homicide, etc.).
  - b. Inquiries for outside agencies shall require the agency's name and the individual's name in the REQ field.
  - c. The complete name of the person actually operating the teletype will be entered in the OPR field.
    - 1) No initials will be permitted (a QR transaction will be logged in the ATN field in the same manner).
  - d. Each IQ, FQ, and AQ transaction by any individual will be logged manually on a written log and maintained in the Communications Unit.
5. Dissemination of CCH information:
- a. Criminal history information obtained via teletype will be given only to the person in the REQ, ATN, or written log. It can be provided "passed" to this person through an appropriate support person.
  - b. The authorized person receiving the information is responsible for keeping the printout secure and immediately placing it in the appropriate file or proper disposal / destruction of it.
  - c. Release of any CCH information will require the original receiving person to document the actual release or transfer of the CCH. This can be accomplished by completion of the CCH Information Log that will be maintained by the Communications Unit. The log is to indicate the receiver's name, date, name of person on CCH, and disposition of the CCH (e.g. released to prosecutor, destruction, etc.).
    - 1) Communication Unit supervisors are responsible for periodically reviewing CCHs and the CCH Information Log to assure compliance.
  - d. If the printout is to be provided to an authorized person / agency outside of this Department after the initial request, that dissemination must be logged.
  - e. This agency will maintain an audit trail of the handling of the CCH printout within the department; keeping it with the case file at all times or by disposing / destroying it immediately after its use should no case file exists.
  - f. Destruction of CCH information requires all documentation to be rendered unreadable. Acceptable destruction methods included: tearing, shredding or burning.

6. Broadcasting of CCH information via radio or laptop:
  - a. NCIC policy states that the radio / laptop will not be used routinely for the transmission of CCH beyond that information necessary to effect an immediate identification or to provide adequate safety for officer or public.
  - b. CCH request will only be made when an immediate need exists for the information to further an investigation or a situation affecting an officer or the general public.
  - c. Department personnel will not indicate over the radio that an individual has a CCH when the officer has not declared a need for the record information.

7. Records cancellation and clearing:

- a. It is the officer's responsibility to:
  - (1) Notify the Communications Unit as soon as possible of a valid theft warrant.
  - (2) Notify the Communications Unit as soon as possible when property is recovered, a warrant is served, or the record is inactive.
  - (3) The case report is to indicate the **TCIC/NCIC** status.
- b. It is the telecommunicator's responsibility to:
  - (1) Remove the **TCIC/NCIC** record as soon as they are notified by an officer.
  - (2) Forward the hard copy of the teletype return indicating Cancel or Clear to the officer who is to include the teletype with the case file.
  - (3) Verify the clearance of both **TCIC/NCIC**.
- c. It is the Communications Supervisor or their designee's responsibility to ensure that the records are cleared from **TCIC/NCIC** in a timely manner using the proper message key.

D. Handling of Storage Media

1. Removal of CJIS (Criminal Justice Information System) Information Required
  - a. When no longer usable, diskettes, tape cartridges, ribbons, external hard drives, flash memory, and all other items used to process or

store CJIS data shall be destroyed using any method that is available, appropriate, and cost effective.

- 1) The employee responsible for creating the stored information on removable media will also be responsible for CJIS information removal. If that employee no longer exercises control of the media at destruction / removal time, the employee in control of the media is responsible for complying with this order.
  - b. Computer systems that have processed or stored CJIS data shall not be released until all stored CJIS information has been removed. City Information Services will oversee the removal of CJIS information from City owned or leased computers prior to the release of these systems.
    - 1) City Information Services will use a storage media wiping procedure meeting Department of Defense standard 5220-22-M.
2. Notification of Information Removal or Destruction
- a. Personnel conducting the removal or destruction of the CJIS information from storage media are required to notify the Technology Unit Sergeant of this action via email. The notification should include:
    - 1) Type of media,
    - 2) Label or ID number of media if present,
    - 3) Date / time of removal or destruction,
    - 4) Process used to perform removal or destruction,
    - 5) Name of person performing removal or destruction,
    - 6) Final disposition of Storage media
3. Logging Requirements
- a. The Technology Unit Sergeant shall maintain a record of all storage media Information Removal or Destruction Notifications.

### 23.809 ADDING or DISABLING USERS

- A. Adding an Agency User account
  1. Employees must be fingerprinted through Fingerprint Applicant Services of Texas (F.A.S.T) Program.

2. Agency must receive background results
  3. Terminal Access Coordinator completes TCIC Use Request Form, writes [URF] in the email subject line and email the form to [TLETS@dps.texas.gov](mailto:TLETS@dps.texas.gov). AN email confirmation will be sent upon completion. No handwritten user requests will be accepted. If technical difficulties occur, a typed user request form may be faxed to (512) 424-7164
- B. When an employee with CJIS access is no longer employed by this agency, the Terminal Agency Coordinator shall notify TLETS of the personnel change. The status of the employee will be changed via the OpenFox Console. The employee's ID and badge will be disabled. Any keys issued to the employee will be returned.
1. Terminal Agency Coordinator completes TCIC User Request Form and emails it to [TLETS@dps.texas.gov](mailto:TLETS@dps.texas.gov) or TAC with SAGY permissions will disable user in OpenFox Configurator.
  2. The department will disable the electronic access badge through the department's controlled-access system. All persons having unescorted access are logged and maintained in this system.
- C. Review of Authorized Users
1. The User/Operator list shall be reviewed annually and as needed
  2. Reviews should be documented
  3. Changes to the authorized personnel will be immediately updated.

#### 23.810 TERMINAL SECURITY

- A. In the event that a computer capable of accessing CJIS systems becomes lost or stolen, dispatch shall be notified immediately.
1. If the computer is part of an in-car computer system the notification shall include the vehicle's assigned number.
  2. Notifications involving an office computer shall include a description of the location the computer usually occupies and the computer's assigned or designed user(s).
- B. Dispatch will contact the city's Information Technology Department, which maintains listing off all MDT/computer devices used to access CJIS. If the notification occurs after normal business hours (Monday – Friday, 8a.m. – 5p.m.), dispatch will contact the city's emergency on-call IT technician.
- C. The IT Department shall disable the connection from the device to any CJIS network.

Approved: 01/10/2023



Jimmy Toler  
Chief of Police