COVINGTON POLICE DEPARTMENT
STANDARD OPERATING PROCEDURE

Subject: GCIC / NCIC PROCEDURES	
Date of Issue: 12-03-2005	**Number of Pages: 8**
Policy No. A100	**Review Date: 06-01-2007**
Distribution: All	**Revision Date: 11-30-2017**

I. Purpose

To provide a general overview of the Criminal Justice Information System (CJIS) Network, the Georgia Crime Information Center (GCIC) and National Crime Information Center (NCIC) policies and operating procedures.

II. Statement of Policy

The Criminal Justice Information System is an integral part of local law enforcement; therefore, it shall be the policy of the Covington Police Department to follow all CJIS, GCIC and NCIC policies, procedures, rules and regulations. These include the CJIS Network Policy Manual, GCIC Operations Manual, GCIC Rules of Council and the NCIC Code Manual.

Information received from GCIC will be used for official use only and will not be used for personal information (GCIC Council Rule 140-2-.09). Violations of this rule will not be tolerated. (See SOP A195, §3.37).

III. Definitions

CJIS - The Criminal Justice Information System consists of all terminals operated by criminal justice agencies, the records and files accessed by those terminals, the computers and equipment utilized by GCIC and local or regional computer centers who are connected to the Georgia CJIS, and federal, state and local criminal justice agencies and employees who operate, support, use and benefit from the network.

IV. Procedures

A. GCIC Computer Terminals

The GCIC computer shall be operated only by certified terminal operators and/or operators that are going through the GCIC workbook certification program or have successfully completed the training.

B. GCIC User Agreements

A formal user agreement will be maintained between the Chief of Police and the GCIC Director. The Chief of Police is responsible for the Department's

compliance with the laws and policies regulating the operation of the CJIS network. Each employee of the department will be required to sign an awareness statement which indicates that he/she is aware of the penalties of disseminating privileged information obtained from the GCIC network.

C. Law Enforcement Teletype Information

The computer terminal interfaces with GCIC and NCIC. This terminal shall only be used for the sending and receiving of official law enforcement messages. It is the responsibility of the Customer Service Representative to enter information into the terminal and to relay necessary information to the officers and Criminal Investigators. GCIC logs and retains all messages sent or received by Georgia CJIS network terminals for seven (7) years. All printouts generated by these terminals, when no longer needed will be destroyed by shredding and/or burning.

D. Terminal Agency Coordinator (TAC)

1. The Chief of Police must appoint a Terminal Agency Coordinator. The TAC is responsible for ensuring that all departmental employees adhere to all GCIC/NCIC policies pertaining to CJIS network operations. Each TAC must successfully complete the TAC Certification Course and Examination administered by GCIC or law enforcement academies. All TACs must be certified within sixty (60) days of their appointments.

2. The TAC will perform the following duties

    a. Assist the Chief of Police in developing policies and procedures for CJIS network operations.

    b. Maintain the quality of GCIC/NCIC record entries. Quality refers to the timeliness, accuracy, completeness and validity of records

    c. Serves as the point of contact for validations and all other GCIC/NCIC network related matters.

    d. Administer the GCIC terminal operator-training program within the department.

    e. Ensure the department's in-service training programs inform employees of requirements and guidelines for the effective use of GCIC/NCIC files and services.

    f. Ensure the written record validation procedures are established and followed.

    g. Maintain copies of all required operations manuals, updates, revisions, operations bulletins and broadcast messages related to CJIS network operations, dissemination logs of criminal history records obtained via the CJIS network copies of signed User Agreements.

    h. Notify the GCIC Security Officer when a new Chief of Police is hired and arrange for the signing of a new User Agreement.

E. Criminal History Record Information (CHRI)

1. Protected information will not be disseminated to unauthorized persons. Criminal history information will not be broadcasted over the radio. If it is necessary to alert an officer that a subject has a history of violent crimes, you must use a coded warning.

2. The type/amount of CHRI disseminated by law and each requestor's authority and purpose. CHRI provided through the CJIS network may be presumed to be current and valid only at the time it is received. CHRI may be requested and disseminated for the following

   a. Investigative or court utilization

   b. Criminal justice employment (Fingerprint cards required)

   c. Public and private employment

   d. Licensing

   e. Individual inspection of records

   f. National Security Checks

   g. Other reasons as provided by law

3. The department will not sell CHRI to anyone not entitled to receive it. The department will charge $20.00 for a CHRI for persons wanting their own CHRI for employment purposes or personal reasons.

F. Physical Security and Maintenance of Criminal History

All CHRI documents must be used to indicate the intended use of requested CHRI valid purpose codes and their respective definitions are:

"C" Criminal justice administration. (Must include; requestors name, operators initials, case number, Social Security number, citation number, docket number or other number which links the request to a criminal case file or investigation, and must be placed in the "ARN" field of the IQ and/or FQ screen.

"J" Criminal justice employment checks

"E" All other purposes including:

- Public or private employment
- Georgia Firefighters employment
- Licensing
- International Travel

Purpose code E refers to GCIC files only. When using purpose code E, requestors must provide:

Applicant fingerprint cards or an original signed consent

Form of the person whose records are being requested.

Refer to GCIC Council Rule 140-2-.04(1) (b) (1).

"P" Georgia convicted felon. Consent form is not required.

G. Logging of dissemination

1. All dissemination of Criminal History and Driver History Records Information must be logged. Each log entry must include:

   a. Date of inquiry

   b. Identifiers used to perform the inquiry

   c. Type of history (Criminal or Drivers)

   d. Purpose code

   e. Operator performing inquiry

   f. Name of person to whom the information was released

   g. Case number if history is for investigator or officer.

2. Logged entries must be maintained for four (4) years for audit purposes.

3. If there is any doubt in reference to a dissemination or method of dissemination, contact the Terminal Agency Coordinator (TAC)

H. First Offender Information

Dissemination of CHRI on persons who have completed sentences under the provisions of Georgia's First Offender Act is regulated by Georgia law and GCIC Council Rule 140-2-04. Records containing such CHRI will be provided by GCIC only when purpose code "C" is used. Such records may not be used for any employment or licensing purposes.

I. Hit Confirmation Request/Response

A hit confirmation request occurs when an agency desires a response on a "hot file" entered into GCIC by the department. On all hit confirmation request, the Customer Service Representative (CSR) must confirm, deny or state specific time needed to respond to request. There are two priorities requested:

1. Urgent- which requires you to answer request within 10 minutes

2. Routine-which requires you to answer request within one (1) hour.

Terminal Operators responsible for hit confirmation procedures must have immediate access to all files needed for request.

J. Warrants

1. The active warrant file is maintained and stored in Support Services under lock and key. The warrant files are accessible 24 hours a day; seven days a week by authorized personnel only.

2. Warrants are issued by the Judge and Led worksheets completed by Court Services personnel. Once completed, a Drivers inquiry (DQ) and Criminal inquiry (IQ) are ran and attached to the LEDS worksheet. Court Service personnel will post the warrant in the in-house computer warrant file. Court Service personnel will bring completed LED sheets to the CSR for entry. Minimum information to be entered is as follows:

    a. Defendants name

    b. Date of birth

    c. Social Security number

    d. Warrant Number

    e. Charge and/code section violated (including original charges if probation or contempt

    f. Date warrant issued

3. The warrant file is checked periodically by the TAC to check for discrepancies, verify validity.

4. All warrants are entered into GCIC "hot files" within 12 hours of being posted (if applicable) according to GCIC policy.

5. All information will be verified prior to GCIC entry. Verification is obtained from:

    a. Issuing department copy of citation (if applicable)

    b. GCIC responses from driver's license registration file, wanted persons and criminal history file inquiries.

6. The following criteria must be verified and matched prior to confirming validity and/or requesting a hold on a wanted person located by another agency:

    a. Name as listed on warrant (or verified alias)

    b. Date of birth

    c. Sex

    d. Drivers license number (if known)

    e. Physical description

7. After a warrant has been served, the arresting officer will notify the Support Service Division. The CSR will:

    a. Perform a "clear" transaction on the GCIC "hot file" entry

    b. Show status as "served" in the in-house computer warrant file.

8. Upon verification from Court Services that a warrant has been recalled, the CSR will:

   a. Remove the warrant from the active file

   b. Note on warrant date of recall and by whom

   c. Change status in the in-house computer warrant file to reflect "recalled", and

   d. Perform a "cancel" transaction to the GCIC "hot file"

9. Request to hold and to attempt to locate individuals wanted by another agency may be received by fax (to include copy of warrant) or GCIC terminal. The minimum information required for this agency to hold or attempt to locate is:

   a. Name as listed on warrant

   b. Date of birth

   c. Sex and race

   d. Warrant number

   e. Charge

   f. Location to check, and

   g. Request to arrest and/or hold

10. In case of a disaster, where the police department facility has to be evacuated, the Department TAC will be responsible for moving all the active warrant files located in Support Services to the 911 Center for protection.

K. Hot File Entry/Removal

All stolen items (vehicles, guns, tags, and articles) and reported missing persons should be entered into the GCIC hot files as soon as possible. Stolen items will only be entered after an incident report has been completed and approved by supervisor. Juveniles reported missing must be entered immediately. Once a stolen item and/or missing person have been recovered, the hot file must be removed as soon as possible.

L. Administrative Messages

All administrative messages sent to other criminal justice terminals are for criminal justice purposes only, this includes All Point Bulletins (APB), Be on Lookout (BOLO). For specific requirements and restrictions, refer to the CJIS Network Policy manual, section 5.3.1 and 5.3.2.

M. Validations

1. A validation packet is prepared monthly by GCIC and sent to the department to check validity, active status, correct spelling, and additional information on all GCIC hot files entered by the department.

2. A record is valid if supporting documentation exists and is current. Wanted persons have not been apprehended, missing persons not found, and stolen property not recovered. On all validations, the case files are reviewed to determine if information is accurate, complete and correct. In addition, the tasks listed below should be performed by the Terminal Agency Coordinator (TAC) for the following items:

    a. Wanted persons. The original warrant, Court services or other sources are checked to ensure each record entry is still valid (i.e. has warrant been served, dismissed or recalled. Determine whether extradition is still authorized from all jurisdictions within the city limits cited in each entry. Fifty (50) miles is standard unless circumstances require otherwise.

    b. Missing person. Check case file to determine if subject is still missing and still being sought after. Contact complainant. A validation checklist will reflect status and be placed in case file. If person has been found, the CSR shall be notified to remove GCIC hot file. Such action will be noted on checklist.

    c. Vehicles. Check with owner of vehicle to determine if he/she has recovered vehicle or an insurance claim was filed. If so check with insurance company. Case status or the removal of vehicles should be noted on validation checklist and placed in case file.

    d. Stolen Articles. Check with owner to see if property has been recovered or if insurance claim was filed. All information shall be noted on checklist and place in case file.

    e. Other Property (Boats, Guns, Securities). Owner will be contacted to check for recovery and/or insurance claim filed. Case status or removal will be noted on checklist and placed in case file.

3. When the previous steps have been completed, the TAC should take the following actions:

    a. Cancel all records that are invalid, that have no case file documentation or that are no longer of interests.

    b. Clear all records showing a "Locate" posted by another agency or by the department.

    c. Modify all record entries reflecting inaccurate or outdated information and that do not show a twenty four-hour number for hit confirmation in the miscellaneous field.

    d. Make supplemental entries when additional information is available to increase the value of record entries.

e. Take no action on records that are complete, accurate, do not show a "locate" and are still valid.

4. After all records have been validated, a message is sent to GCIC advising that validation has been completed for the specific month.

N. Disaster Plan

In the event of a natural or manmade disaster, which necessitates the evacuation of the Covington Police Department building, the GCIC files maintained at the front desk consisting of warrants and LEDS will be safely removed from the building by the CSR on-duty and given to an on-duty officer or supervisor, and taken to the Covington-Newton County 911 Center or wherever the current command station is located at that time.

O. Security Incident Reporting

1. Any security incidents that may arise shall be reported immediately to the agency's LASO. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

2. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the LASO.

3. Once notified the agency's LASO will notify the Agency Head and GCIC. If deemed necessary the agency's LASO will:

    a. Notify GCIC to relay the preliminary details of the incident.

    b. Investigate the reported incident and submit an incident response form to GCIC once all the information has been gathered.

4. Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules of evidence in accordance with agency's standard operating procedure regarding evidence procedures.

This SOP supersedes any SOP previously issued.

BY ORDER OF THE CHIEF OF POLICE:

Stacey L. Cotton

Stacey L. Cotton
Chief of Police