FAIRBURN GEORGIA POLICE DEPARTMENT
OPERATIONS MANUAL

CHAPTER 21 **GCIC**

EFFECTIVE DATE: **04/20/2016** **NUMBER OF PAGES: 19**

REVISED DATE: **01/01/2024** **DISTRIBUTION: All**

SPECIAL INSTRUCTIONS: N/A

I. PURPOSE

The purpose of these procedures is to establish guidelines to ensure the security, privacy, accuracy and completeness of access to and dissemination of adult and juvenile record information, driver license information and tag and vehicle registration information; proper entry, maintenance and removal of all wanted/missing person and property records; and to ensure the accuracy, timeliness and completeness of all records maintained by the Fairburn Police Department.

II. SCOPE

This policy applies to all sworn and non-sworn personnel of the Fairburn Police Department, volunteers, visitors, vendors, contractors and others who have access to Criminal Justice Information Systems (CJIS) or areas that contain such information.

III. IDENTIFICATION OF AUTHORIZED PERSONNEL

Criminal History Record Information (CHRI), driver license information and tag/vehicle registration information shall be maintained in secure areas within the department. They shall only be accessed by or disseminated to those who are authorized to access or receive said information in accordance with departmental policy, state law, or by rules, regulations and policies of the Georgia Crime Information Center/National Crime Information Center (GCIC/NCIC).

Only authorized personnel are allowed access to the Criminal Justice Information System (CJIS – GCIC/NCIC) databases through departmental terminals that access GCIC and NCIC files and records. Authorized employees must successfully complete Terminal Operator Training upon initial employment, prior to accessing the CJIS system and be recertified in accordance with GCIC rules and regulations.

All employees must receive the minimum training on Security and Integrity of Criminal History (S & I) Record Information and GCIC Rules and Regulations prior to having access to a CJIS system, prior to accessing and disseminating said information and prior to recording, maintaining and destroying said records.

IV. RESPONSIBILITIES

All supervisors will ensure that security measures are followed to provide maximum security of criminal history record information and CJIS databases, records and files. Unauthorized

personnel and/or individuals will not be allowed to frequent areas where such information is maintained, stored, collected or processed.

When sworn or non-sworn personnel access an agency computer system, which accesses the CJIS system, the employee must log onto and off the CJIS system using their assigned ID and Password. If an employee must leave their computer unattended while accessing the CJIS system, the employee must log off the CJIS system prior to leaving the computer. Leaving the system includes but is not limited to break time, lunchtime and leaving work at the end of the day. If a computer is accessible by multiple users, each user must follow the above procedures.

A. Shift Supervisor shall ensure that:

1. All inquiries of the CJIS files are processed in accordance with department policy and procedures, state and federal laws and GCIC and NCIC rules and regulations.

2. Adult and juvenile arrest records will be collected, retained, disseminated and disposed of in accordance with department policy and state law.

3. When a report is taken by an officer that contains information with identifiable descriptors and said information is required by policy to be reported to NCIC, a copy of the officer's incident report containing said information, and other required documentation, will be forwarded to Fairburn GCIC Coordinator; or, after normal hours of operation to Fulton County GCIC Technician who will be available 24/7.

4. All reports with identifiable descriptors and said information is required by policy to be reported to NCIC are forwarded to Fairburn GCIC Coordinator; or, after normal hours of operation to Fulton County GCIC Technician who will be available 24/7.

5. Missing juveniles and missing persons under 21 years of age will be forwarded immediately (within 2 hours) for entry when the minimum required information has been collected. All other records must be forwarded for entry as soon as practical but within 12 hours or prior to leaving their tour of duty.

6. All reports, and other required documentation, shall be reviewed for accuracy and completeness by the supervisor prior to being forwarded to the Fairburn GCIC Coordinator; or, after normal hours of operation to Fulton County GCIC personnel.

7. All reports entered into the computers which require removal shall be removed in accordance with state law and GCIC/NCIC rules and regulations. They shall be removed in a timely manner as outlined in the CJIS Network Operations Manual by the Fairburn GCIC Coordinator or after normal hours of operation by Fulton County GCIC personnel.

8. When an existing record is to be cleared, canceled or modified, all information needed (incident report, supplemental report, etc.) will be forwarded to the Fairburn GCIC Coordinator; or, after normal hours of operation to Fulton County GCIC personnel in a timely manner. Supervisors will ensure that all information is complete and accurate.

9. Officers who receive and process criminal history, driver history, tags and VIN information will destroy said information in accordance with departmental policy, state law and rules of GCIC/NCIC.

10. Supervisors and officers will not provide criminal history, driver history, tag or VIN

information to any individual, citizen, business or other non-law enforcement party. Individuals, businesses and other non-law enforcement personnel requesting such information shall be referred to the GCIC Coordinator for inquiry, processing and dissemination of criminal history, tag and VIN information. All driver history inquiries shall be referred to the Department of Driver Services.

11. Personnel under their supervision are aware of the laws, rules and regulations governing criminal history information and those personnel under their supervision are aware of penalties for illegally disseminating criminal history information.

12. Personnel under their supervision are aware of the Georgia Computer Systems Protection Act and penalties that apply to violations of this law.

13. Personnel under their supervision have reviewed, understand and have signed a current GCIC awareness statement form. All signed forms shall be forwarded to and maintained in the department's employee personnel file.

14. Personnel under their supervision have successfully completed a Terminal Operator training and Security and Integrity training prior to being allowed to access CJIS systems (GCIC/NCIC).

B. The GCIC Coordinator shall be responsible for the following:

1. Ensure that inquiries of GCIC/NCIC files are processed and maintained in accordance with state and federal laws, GCIC/NCIC rules, regulations, and policy and department policy.

2. Ensure that only authorized personnel utilize their assigned CJIS terminal during working hours. Ensure that terminal usage and messages are transferred to the Fulton County GCIC by Integrated CJIS Data Center (ICDC) when Fairburn Coordinator is unavailable.

3. Will log off the system when being relieved by another employee, at which time the relieving employee will log into the system using their Operator ID and Password.

4. Ensure that all wanted/missing person files, property files and other files are maintained and stored in accordance with state and federal laws, GCIC/NCIC rules and regulations and department policy.

5. Enter, modify, clear and cancel all wanted and missing person files and property files on scheduled workdays, excluding holidays. Personnel from Fulton County GCIC shall be responsible for making the appropriate entries, modifications, clearances and cancellations after normal hours of operation and when Fairburn GCIC Coordinator is unavailable. Missing persons under the age of 21records will be entered immediately (within 2 hours of receiving the minimum requirements for entry). All other records must be entered within 12 hours.

6. Missing Juvenile: Based on the National Center for Missing and Exploited Children (NCMEC) and the Federal Amber Alert Law missing persons who are 21 years of age or less are required by federal, state and local law to be entered into NCIC immediately (within 2 hours of receiving the minimum requirements for entry) upon receipt of a report.

   Within 24 hours, excluding weekends and holidays, after original entry, the GCIC

Technician will verify the record and secure additional information if necessary and if available. If additional information is required during a weekend or holiday period, the on-call detective will be called in to perform this function and forward the additional information to Fulton County GCIC personnel for modification to the record.

7. Ensure that all warrants issued by Fairburn Municipal Court or Fulton County Courts are completed in a timely manner with current and accurate information. That all warrants are processed, maintained and stored in accordance with state and federal laws, NCIC rules and regulations, and department policies.

8. Maintain a log of all transactions for driver and criminal histories and III files. Logs shall include but not be limited to the date of the request; type of request; name, date of birth, race, sex and social security number of person being inquired upon; agency and person making the request; the operator accessing the computer for the information; purpose for the request; departmental case number, traffic citation number or other number related to the request, Agency Reference Number (ARN), SID or FBI number if one is assigned and any other miscellaneous number associated with the request.

   If there is no identifiable number available, the GCIC Coordinator will assign an Agency Reference Number (ARN) to the requested inquiry. The GCIC Technician shall maintain a log of all ARN numbers used. The ARN is a sequential list of numbers that are maintained in a separate database and used when no other reference number is available.

9. Ensure that all criminal and driver history logs are maintained and stored in accordance with department policy, state and federal laws and GCIC/NCIC rules and regulations.

10. Requests for driver histories shall be made in person by on-duty personnel only. No requests shall be made via phone except by an on-duty officer in the field who must have the information immediately for work-related purposes. The employee receiving the request for an inquiry will verify the identity of the call prior to processing the request. All requests will be logged and maintained in accordance with department policy.

11. Maintain a log of all requests for tag, VIN and driver license information from on-duty employees. Requests from off-duty employees will be refused. Logs will include date/time of request, Requestor's name, and type of request (tag/VIN/driver license), reason, Operator and method of dissemination.

12. Requests for tag, VIN and driver license information will be made in person and by on-duty personnel only. Requests shall be made only when an officer/employee cannot access the information through their computer system. All requested information will be logged by the Operator processing the request.

13. Ensure that only authorized personnel are allowed to review files containing criminal, driver history, tag/VIN and driver license information.

14. Ensure that all computer printouts containing criminal history information, driver license or history information, tag/VIN information or other law enforcement related information is destroyed by shredding when no longer needed. Only Fairburn Police Department employees are authorized to destroy said files. At no time shall

community service personnel, trustees, volunteer or any other non-employed person destroy said files.

15. Prior to making any GCIC/NCIC file entry, the GCIC Coordinator will first transmit a wanted inquiry on the person or item.

    For wanted or missing person entries, the GCIC Coordinator will run a driver's license and a criminal history inquiry. They will check with investigators to determine if information is accurate or needs updating, check original warrant to ensure it is still valid, and check other sources of information known to provide possible additional information; such as county jail, Dept. of Corrections, etc. This will be done in an effort to develop as much information as possible prior to completing the LEDS worksheet. For property files, the GCIC Coordinator will check case files to determine if information is accurate, complete and current and contact the investigator (and owner if possible) to verify the item is still missing and secure additional information if available.

16. The GCIC Coordinator will review all portions of the LEDS worksheet prior to making entry into the system by using the CJIS Policy and Operations Manual or the NCIC on-line code manual. Inquiries against the criminal history, driver history, and driver license files will be made to develop as much information as possible prior to completing the LEDS worksheet.

17. Report unresolved problems to the Primary TAC, GCIC or NCIC.

C. Records personnel shall ensure that:

1. Access to the department's records section where criminal history record information is collected, stored, processed and disseminated shall be limited to authorized persons only. Authorized personnel are determined by the TAC, Deputy Chief or Chief of Police.

2. All arrest records shall be collected, stored, processed and disseminated with accuracy and completeness. All arrest information will be retained for the specified length of time as designated by state law.

3. All department reports, criminal and driver history, driver license and tag/VIN information that is to be destroyed is destroyed by shredding. Only Fairburn Police Department employees are authorized to destroy said files. At no time shall community service personnel, trustees, volunteers or any other non- employed person destroy said files.

4. All employees who access the CJIS database files have received training in Security and Integrity (S&I), have successfully completed the Terminal Operator training and receive S&I training every 2 years.

5. All employees have read, understand and signed a current GCIC awareness statement form.

V. NATURAL AND/OR MAN-MADE DISASTERS

In the event of a natural or man-made disaster, the Shift Supervisor shall have the responsibility of ensuring that areas where records are maintained by the department are secure and that department records are not in danger of being damaged or destroyed.

In the event that an area has been identified as being unsecured and department records maybe or have been damaged and/or destroyed, the Shift Supervisor shall make immediate notification to the affected division supervisor and advise them of the situation. A police officer(s) shall be stationed in the area(s) to secure unsecured areas and/or records until the division supervisor responds and assumes control of the affected area and records. Affected areas include Records, Municipal Court, Identification, Evidence, Detective Division, Office of Professional Standards and the Chief's office.

The affected division supervisor shall be responsible for taking immediate necessary steps to ensure that the affected area(s) and all records are secured on site. If the affected area is not able to be secured, the records and files affected shall be removed to another location where they can be secured until such time that the records and files can be returned and secured within the department.

VI. DISSEMINATION OF CRIMINAL/DRIVER HISTORY INFORMATION, DRIVER LICENSE AND TAG/VEHICLE REGISTRATION INFORMATION

All criminal history, driver history, tag/vehicle registration information shall be disseminated in accordance with department policy, state law and GCIC/NCIC rules and regulations.

Terminals, which access CJIS files, shall be located in a secure area, out of view of unauthorized personnel or the public, and in an area restricted to authorized personnel only. Files shall be stored in locked file cabinets when not in use.

Only authorized personnel shall access the CJIS database system and make inquiries. Authorized personnel are the Chief of Police, Deputy Chief, Captains, Lieutenants, Sergeants, Corporals, Detectives, SPOs, Officers, GCIC certified Administrative Services personnel, Court Services personnel and TAC.

Officers have access to driver license information and tag/vehicle registration files through their vehicle mobile data terminals. All documentation must be placed in a case file or destroyed in accordance with agency policy and shall not be left out in plain view or thrown into the trash can.

Any Police Officer will not directly access criminal history information from a CJIS system but will request the information through their supervisor or the Fairburn GCIC Coordinator or Fulton County GCIC or Fulton County Emergency Communications Technician when it is necessary to access CCH files for work related purposes. All records accessed shall be documented in accordance with department policy. All documentation must be placed in a case file or destroyed in accordance with agency policy and shall not be left out in plain view or thrown into the trash can.

A. Criminal History and Driver History Access and Dissemination

1. Only authorized personnel shall make inquiries and receive Criminal or Driver History Record Information and only when it is job related and in accordance with department policy, GCIC/NCIC rules and regulations, state and federal laws.

2. Authorized persons who make inquiries into driver and/or criminal history files will be logged on the logbook located with each operator.

3. All logs shall include but not be limited to the date of the inquiry; type of request; name, date of birth, race, sex and social security number of the person being inquired upon; the agency and person making the request; the operator accessing the information and the

purpose of the request (C, J, P, E, W, N, M, Z or F)when inquiring in criminal history files; the departmental case number, ticket number, Agency Reference Number (ARN) or other number related to the request; and the SID or FBI number if one is assigned.

4. All logs shall be maintained for a period of four years. These logs shall be maintained in a locking file cabinet in the office where the CJIS terminal is located.

5. Logs shall be inspected periodically by a TAC.

6. Driver history and/or criminal history information received but not maintained or disseminated shall be shredded. Only Fairburn Police Department employees are authorized to destroy criminal history and driver history records.

7. When a request is made for a criminal history of an individual and a signed consent form is received, the original consent form shall be kept on file for a period of two years. Consent forms shall be destroyed by shredding. The State records retention laws will be followed.

8. When officers, supervisors, detectives or other personnel receive driver history or criminal history information, the information shall be placed in a file maintained by the employee or in a case file. Employees will destroy all information not used by shredding said information.

9. At no time shall criminal or driver history information be left lying around on tables or other objects, left in department vehicles, thrown in the trash can or given to unauthorized persons or businesses.

10. Violations of said policy and/or state law will result in disciplinary action and/or criminal prosecution.

11. The commercial dissemination of Federal and/or State non-restricted files (HOT files) is prohibited. Fairburn Police Department shall not practice disseminating information obtained from these files for payment.

B. Information may be disseminated to individuals as follows and as designated by state law:

1. To other criminal justice agencies for the administration of criminal justice, disseminate all CHRI including first offender complete information to the requester, Purpose Code C, no requirement of consent form or fingerprints.

2. To the Federal Bureau of Investigation, Defense Investigative Service, U.S. State Department, Central Intelligence Agency, and Office of Personnel Management for national security purposes only, without a signed notarized consent form or fingerprints of the person being checked for security clearance and persons being considered for employment in sensitive national security jobs, disseminate all CHRI using Purpose Code E.

3. For all inquiries for the purposes of issuance of a pistol totters permits, refer all requests to the Fulton County Probate Office.

C. Requests by Firefighter Applicants

1. All requests shall be made by submitting a signed consent form for a Criminal History.

2. All CHRI except first offender complete information shall be forwarded to the Fire Chief or his designee. The GCIC Coordinator shall make local and state CHRI inquiries for the Fire Chief using Purpose Code E.

3. Single requests shall be completed in a timely manner. Multiple requests shall take the appropriate amount of time per the number of applicants.

4. No fees shall be assessed for the completion, processing and obtaining of CHRI information from local and/or state files.

D. Requests by Prospective Employers and Others Request

1. All requests for CHRI by prospective employers shall be in accordance with department policy, state law and GCIC/NCIC rules and regulations. Record inquiries may be made for local and/or state records. All requests shall be made to the Fairburn GCIC Coordinator.

2. The prospective employer must furnish the Fairburn GCIC Coordinator with a signed, notarized consent form by the individual whose record is being checked. If needed, blank forms shall be provided by the GCIC Coordinator or Records personnel. Purpose Code M shall be used for individuals working with the mentally disabled. Purpose Code W shall be used for individuals working with children. Purpose Code N shall be used for Nursing Home employment. For all other employment reasons not covered in this policy, Purpose Code E shall be used.

3. Single requests shall be processed in a timely manner. Multiple requests shall take the appropriate amount of time per the number of requests. Information disseminated from local or state (GCIC) files shall only be that information which matches the individual being inquired upon.

4. If an adverse employment decision is made due to the criminal history inquiry, the contents of the record received and the affect the record had on the employment decision must be made known to the applicant/employee by the employer, organization or agency.

5. Personnel shall be referred to the local Georgia Applicant Processing Services (GAPS) office for processing applicant fingerprints.

E. Requests by Private Attorney or Defense Attorney

1. Requests for criminal history record information by a defense attorney for use in pending criminal cases shall be referred to GCIC.

2. Requests for criminal history record information by a defense attorney in a civil case shall be referred to the Fulton County District Attorney's office.

F. Transmission of Criminal History Record Information

1. Criminal history record information (CHRI) shall be disseminated to non-criminal justice individuals by the following methods:
    a. person to person,
    b. in writing.

2. Criminal history record information (CHRI) shall be disseminated to criminal justice

individuals by the following methods:

a. person to person,
b. in writing,
c. over the telephone if the requester is known,
d. by fax machine if the requester is at the fax machine where the information is to be faxed.

3. Police radios MAY BE used for the transmission of CHRI if the information is necessary to affect an immediate identification or to ensure adequate safety for police officers or the general public.

G. Restriction of Records

Application process for expungement for violations occurring before July 1, 2013:

1. Individuals seeking to have a record restricted from their local file must first request from the original arresting agency in writing their request that the record be restricted using the form prescribed by GCIC. Individuals may secure a blank restriction form from the Fairburn Court Clerk. The form can also be found online at: https://gbi.georgia.gov/georgia-criminal-history-record-restrictions

2. The Fairburn Court Clerk will process restriction requests from individuals making the request of their own file. An attorney may make the request on behalf of a client.

3. The Court Clerk shall receive and process all requests for record restriction. The Court Clerk shall complete a GCIC inquiry regarding the described arrest record. Upon completion, the Court Clerk will forward the request to the Fulton County District Attorney's Office or the Solicitors who will then determine if the record meets the criteria set forth in state law.

4. Once the Fulton County District Attorney's Office or the Solicitors Office has processed the request, they shall notify the Court Clerk that all criteria has been met or has not been met. This process can take up to six months.

5. The Fulton County District Attorney's Office or the Solicitors Office shall notify the Fairburn Court Clerk as to whether the request was approved or denied. The requesting individual may check with the Court Clerk's office to inquire about the process. If approved, the Court Clerk will then notify the applicant.

6. Once approved, the applicant must bring a $25 money order to the Court Clerk's office. The money order must be made out to the GBI and it must be turned in to the Court Clerk's office in order to be mailed with the application. Without the money order, the GBI will not accept the application.

7. Once the GBI receives the approved application and money order, the GBI will begin the process of restricting the record electronically.

For offenses occurring July 1, 2013 and after, the Court Clerk shall restrict any charge electronically via the CCH system no later than 30 days after the disposition of the case. The charge must have a disposition as follows in order for a restriction to be applied automatically: dismissed, nolle prosequi / nolle prossed, placed on the "dead docket" or found not guilty.

More information on record restrictions can be found (as well as the form for expungement) here:

https://gbi.georgia.gov/georgia-criminal-history-record-restrictions

VII. AGENCY COORDINATOR

The Chief of Police shall appoint a GCIC Coordinator to serve as the agency point of contact regarding record validations, hit confirmations, training and other GCIC and NCIC related matters. The GCIC Coordinator shall abide by state law and GCIC rules and regulations.

A. The GCIC Coordinator is responsible for the following:

1. The administration of training for all sworn and non-sworn departmental personnel related to privacy and security, the dissemination of CHRI, use of CJIS terminals, proper use of GCIC and NCIC procedure books, completion of a terminal operator training and other related training.

2. The administration of terminal operator training and certification and re-certification testing programs required and developed by GCIC. The administration of a terminal operator training and training program.

3. Monthly completeness of GCIC/NCIC record validations to ensure that records are valid, complete, accurate, current and active. Validation reports are to be completed accurately and in a timely manner.

4. Utilize resources to assist in confirming that entered records are valid. Resources to include but not limited to: Wanted/Missing Persons - Clerk of Municipal Court, other law enforcement agencies, family members, driver license files, criminal history files, county jail; Stolen Entries - victims, family members, investigators, National Insurance Theft Bureau, insurance companies, other police departments, motor vehicle dealerships, Department of Driver Services.

5. Assist personnel with responding to hit confirmations, administrative and NLET messages when necessary.

6. Assist personnel with removal of invalid records from the terminal and proper procedures for clearing/canceling said records.

7. Ensure that CHRI logs are properly maintained by department personnel.

8. Ensure that all department personnel review and sign awareness statements and that these forms be maintained in the employee's personnel file.

9. Ensure that volunteers, community service workers, and other non-employee individuals who frequent areas where CHRI is processed and/or maintained are given instructions regarding confidentiality of department records. Such individuals are to review and sign an awareness statement and forms shall be maintained on file by the TAC.

10. Receive training, testing and certification as mandated by GCIC.

11. The administration of terminal operator training, certification/recertification testing and the reporting to GCIC the certification/re-certification status of all terminal operators employed by the Fairburn Police Department.

12. Assist with the development of policies and procedures for CJIS network operations.

13. Maintain CJIS network related documents such as: Operations Manual, Policy Manual, Council rules, updates, revisions, Operations Bulletins, broadcast messages and other CJIS related materials.

14. Notify the GCIC Security Officer when a new agency head is appointed or elected and arrange for the completion and signing of a new User Agreement.

VIII. User Account Access-Validation and Removal of Access Policy

Purpose: The Fairburn Police Department shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling and removing accounts. The Fairburn Police Department shall validate system accounts at least annually and shall document the validation process.

Policy: All accounts shall be reviewed at least annually by the Terminal Agency Coordinator (TAC), Local Agency Security Officer (LASO) or designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain criminal justice information. The TAC may also conduct periodic reviews.

The TAC, LASO or designee must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

The TAC, LASO or designee must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). The Chief of Police or his designee will notify the TAC, LASO or designee of any terminations, resignation, etc. The TAC, LASO or designee will remove or disable all access accounts for separated or terminated employees immediately following separation from the Fairburn Police Department.

Primary responsibility for account management belongs to the TAC. The TAC, LASO or designee shall:

- Modify user accounts in response to events like name changes, accounting changes permission changes, office transfers, etc.,
- Periodically review existing accounts for validity, and
- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

The Fairburn Police Department shall review CJIS access authorizations when personnel are reassigned or transferred to other positions within the Fairburn Police Department and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

IX. DOCUMENTATION OF LEDS FILES

All entries shall be supported by official police reports (incident, supplemental, arrest, etc.).

1. Incident reports shall be prepared and completed by the officer taking the report or assigned the case before the end of his/her shift.

2. When the report cannot be completed by the end of the officer's shift, as much

information as possible will be furnished. The full report will be completed as soon as possible.

3. The incident report shall be checked by the reporting officer's supervisor for accuracy and completeness.

4. The officer shall complete the LEDS worksheet. Before the end of the shift the officer shall submit a copy of all incident reports, LEDS and other documents containing information that is to be entered into the GCIC/NCIC files to the Fairburn GCIC Coordinator; or, if after normal hours of operation, fax a copy to the Fulton County Police GCIC Missing persons under the age of 21 shall be entered immediately (within 2 hours after the minimum requirements are obtained). All other records shall be entered as soon as practical but within 12 hours.

5. When LEDS and reports are faxed to Fulton County Police GCIC for entry the originals should be placed in the black tray on the second desk or in the blue folder labeled New Entries. A file will be made on the next work day of the Fairburn Police GCIC Coordinator and placed in the GCIC file cabinet.

6. When additional information that can be included in the record entries is developed, the officer or detective will forward copies of all updated or supplemental reports containing such information through the shift supervisor to the Fairburn GCIC Coordinator; or, if after normal hours of operation fax to Fulton County GCIC Technician. The original record will then be updated.

7. Copies of all terminal transaction printouts will be attached to the LEDS worksheet along with a copy of the incident report and any other necessary documentation. Copies will be maintained in the Fairburn GCIC files and the Fulton County Police GCIC files.

8. When Fulton County GCIC make entries, modification, clearances or cancellations for Fairburn Police a printout will be mailed to our agency weekly. The printouts shall be attached to the original LEDS and reports in the GCIC files.

X. PROCEDURES FOR HANDLING "HITS" REQUEST

When the "Hit" is on a record entered by another agency, the Fulton County GCIC Technician shall send a "Request for Hit Confirmation" message IMMEDIATELY.

A. When receiving a "Hit" response on an inquiry on a person, vehicle or article that has been inquired upon by an officer, the Fulton County GCIC Technician shall notify the originating agency that entered the record that a "Hit" has been received. The Fulton County GCIC Technician shall follow procedures as outlined in the CJIS Policy and Operations Manual.

B. GCIC/NCIC "Hit" is not in itself probable cause to make an arrest, detain a missing person record subject, or to seize property. Only after a "Hit" has been confirmed by the originating agency, and after the Fairburn Police Department officer evaluates the age of the record, closeness of the match between the subject or property described in the record and hit confirmation message, can there be probable cause to arrest or detain a subject or seize stolen property. If the officer has any doubts, he should contact his shift supervisor for additional directions.

C. If the person, vehicle or article is “Not confirmed” they or the property will be released.

D. If the person, vehicle or article is confirmed a “Locate” must be placed and a “AM message” {detailing the location property or person was located; officer; circumstances; their case number; perps.; vehicle damages; if tag is with vehicle and/or impound location} will be sent.

E. If a wanted person is confirmed, they will be taken into custody and held for the entering agency. If property is confirmed it will be placed in the property room for safekeeping.

XI. PROCEDURES FOR HANDLING "CONFIRMING OUR ENTRIES"

A. The Fulton County Police GCIC Technician will notify the Fairburn GCIC Coordinator; or, if after normal hours of operation, the shift supervisor whenever a request for "Hit Confirmation" is received.

B. If Fulton County GCIC has to get the shift supervisor to confirm the Hit they should request additional time to allow time for the supervisor to return to HQ and locate the file.

C. The Fairburn GCIC Coordinator or shift supervisor will locate the original entry documents; and verify the information contained in the request for "Hit Confirmation" against the original documents supporting the entry.

D. The Fairburn GCIC Coordinator or the shift supervisor will respond to the request from Fulton County GCIC for confirmation as: confirmed, not confirmed or requiring additional time. Fulton County GCIC will respond to the requesting agencies "Hit Confirmation" within 10 minutes or 1 hour depending on the urgency by:

1. Confirming the "Hit",

2. Denying the "Hit", or

3. Requesting more time stating the amount of time needed to confirm/deny the "Hit".

E. If a "Hit" is denied because the record is not valid, the Fairburn GCIC Coordinator or shift supervisor will notify Fulton County GCIC Technician that the record is not valid and request that the record be "Cancelled" immediately.

F. If a “Hit” is confirmed by the shift supervisor a note should be place on the person, vehicle or article that is confirmed {confirmed by whomever, date, and locating agency}. Upon receipt of the "Locate" and AM message {detailing the location property or person was located; officer; circumstances; their case number; perps.; vehicle damages; if tag is with vehicle and/or impound location}, the GCIC Technician will "Clear" the record. Located wanted person are ONLY cleared if they are released to our agency.

G. If the arresting agency has charges on the subject a “Detainer” will be placed on the subject once the “Locate” is received. The file will be paced in the black tray on the 2nd desk in the GCIC office with a note {confirmed by whomever, date, and locating agency}.

H. Once the person, vehicle or article has been located and/or cleared the Detective will be notified.

I. Once Fairburn Police is notified that the wanted person is ready to be picked up the shift supervisor will be notified. An officer will be dispatched, and the subject will be taken to the jail. The supplement, citation(s), A & B, original warrant(s) marked with an “S” and

fill out, criminal process form will be furnished to the GCIC technician and the subject will be cleared from the system.

J. The G.C.I.C. Technician shall refer to procedures outlined in the CJIS Policy and Operations Manual for additional information and instructions.

XII. VALIDATION PROCEDURES

To ensure that all computer entries, hot files and wanted/missing person files are accurate, complete, current and maintained properly and securely, records shall be validated on-line each month when received from GCIC and in accordance with GCIC/NCIC rules and regulations.

A. The GCIC Coordinator shall ensure that all records received from NCIC shall be reviewed in a timely manner. Information received shall be compared with LEDS worksheets, investigative case files and all other documents on which the record entries were based.

B. Statute of Limitation. All warrants less than 5 years old shall remain on NCIC. Any warrant that is older than 5 years old Fairburn GCIC shall furnish a copy of the report, criminal history and driver history {traffic charges} to the Chief Judge. No warrant will be taken off NCIC for expiration of statute of limitation without the approval of the Chief Judge.

C. Personnel shall consider all possible alternatives for obtaining additional information to determine current status stolen property, wanted/missing persons. The following resources should be considered when determining the status of a record or when obtaining additional information about a person or item:

1. Compare all fields in the LEDS worksheet, computer printouts to the supporting documentation to ensure that records are complete and accurate. Make corrections when necessary.

2. Check driver license, driver's history, criminal history and vehicle registration files to obtain possible additional information.

3. Consult with investigators to ensure the proper status of the warrant, to obtain additional information regarding a wanted/missing person or stolen property.

4. Consult with the Fulton County District Attorney's office to ensure the warrant is prosecutable and has not been dismissed. Ensure extradition is authorized.

5. Check all original warrants; ensure they are complete, current, accurate and valid.

6. Make phone contact with victims and/or other parties listed to ensure that reported items are still missing and have not been located/recovered and to get additional information if available. To ensure that individuals are still missing.

7. Make phone contact with other local resources to identify additional information necessary to ensure proper validation of records.

8. When unable to make phone contact with property owners, send written notice requesting confirmation of record status and addition of other identifiable information.

9. Modify record entries which contain erroneous information, or which are incomplete.

Add supplemental information when appropriate.

10. Remove incorrect information from the records and re-enter the correct information.

11. Cancel invalid record entries from the NCIC files that cannot be corrected. A file that can be corrected will be immediately updated and re-entered with the correct information.

D. Personnel validating records shall document action taken with each record. Problems concerning any record shall be reported to the GCIC Coordinator or Chief of Police and corrective action taken immediately.

E. The validation process shall be completed when all record entries have been verified as accurate, complete and current or when records have been modified or canceled. The validation certification shall be completed and returned on-line to GCIC during the specified time frame.

XIII. Rapid ID fingerprint software, MC-75 handheld fingerprint reader.

I. PURPOSE: The purpose of this policy is to establish guidelines for the training, use and management of Rapid ID fingerprint software and handheld fingerprint reader.

II. POLICY: It is the policy of the Fairburn Police Department to enhance patrol capabilities by utilizing the latest technologies for crime prevention and apprehension of criminals. The handheld fingerprint reader and the Rapid ID Digital Fingerprint Software utilize such technology to scan fingerprints and assist in the identification of individuals under appropriate circumstances. The MC-75 handheld fingerprint reader and Rapid ID Digital Fingerprint Software may be used in a variety of circumstances; however, employees must be aware that there are specific requirements and guidelines for its use.

The MC-75 Digital Fingerprint reader will be used and maintained in accordance with manufacturer recommendations and this policy. The Fairburn Police Department will use the agency approved Motorola MC-75 handheld devices which conform to the standards set forth by the Georgia Bureau of Investigations (GBI).

III. DEFINITIONS: Rapid ID Device (RIDD) - A wired or wireless fingerprint identification scanning device that communicates via a secure internet connection with a centralized database system housed at the GBI. The device submits scanned fingerprints to the GCIC System database for comparison to criminal prints on file. Results of the automated comparison are sent to the originating device, affirming the identity of the scanned subject if the subject's known fingerprints exist in the database.

Once a fingerprint is submitted, the system processes the fingerprint inquiry and returns a "Hit" or a "No Hit" response to the RIDD. If a "Hit" is located, as part of the identification check, data is automatically submitted through the Law Enforcement Message Switch (LEMS) portal/Portal XL for an NCIC check on wanted files, watch lists, sex offender registries, and probation/parole registries. If "No Hit" is the response, it indicates that a match was not located on an individual with a prior fingerprint-based arrest record within the state of Georgia and therefore an automatic NCIC check cannot be performed. A "No Hit" response does not preclude the existence of a record in other biometric or name-based repositories and it is recommended that a traditional CJIS criminal history and/or warrant search be performed when receiving a "No Hit" response.

Agency Rapid ID System Administrator (RSA) - The person designated by the

Fairburn Chief of Police to administer and oversee the deployment and use of the Rapid ID System. The RSA will ensure that all training requirements and the GCIC Terminal Operator Certification have been completed prior to deployment and use.

XIV. PROCEDURE:

A. Issuance of the Rapid ID Device (RIDD)
A wireless Rapid ID Device will be issued only to employees who are currently certified to run GCIC inquires and that have had training on the operation of the unit. Training shall include considerations and requirements for use of the device under various circumstances.

All Rapid ID Device units must be properly maintained in accordance with the manufacturer's recommendations as detailed in the training provided prior to use. Wireless Rapid ID Devices shall be stored and secured in the Fairburn Police Department. The wireless devices shall be assigned to designated Fairburn Police Department employees. Only Fairburn Police Department employees who have received training on the Rapid ID Devices will be allowed to utilize the Rapid ID Device for authorized law enforcement purposes.

B. Training:

The Agency Rapid ID System Administrator (RSA) or his/her designee will be responsible for overseeing the development and administration of the training process for assuring proficiency of the operators with the Rapid ID Device.

C. Training will include at a minimum:
- GCIC terminal operator certification (inquiry level at minimum);
- Setup and maintenance procedures;
- Proper use and guidelines;
- Legal issues involved with the use of the Rapid ID Device;
- Reporting requirements;
- Other issues as deemed necessary and established by the RSA

Before being authorized to use a Rapid ID Device, users shall obtain a unique user name and password from the agency's RSA. Password requirements:

- Must contain at least 3 of the following: lower case letter, upper case letter, number, or special character.
- Must be a minimum of 8 characters; cannot be a dictionary word or proper name; User ID's and passwords cannot be the same; passwords expire every 90 days; no repeating passwords for 10 passwords.

XV. RAPID ID GUIDELINES FOR USE:

1. The Rapid ID Device may be used in situations where the subject to be fingerprinted has given a knowing and willing voluntary consent or permission for the employee to use the device. This may include consent given during a lawful encounter (i.e. traffic stop).

    a. Verbal consent is acceptable. Consent shall be made in front of a camera when possible and require at least one other employee present as a witness to the consent.

b. As with other forms of consent, the consent can be limited or withdrawn at any time by the subject.

c. If consent is withdrawn, use of the Rapid ID Device is NOT authorized and its use must stop immediately. Officers shall not force or coerce anyone to submit to the scan.

d. The Rapid ID Device is not to be used for any unlawful purpose. Improper or unauthorized use of the Rapid ID Device may result in disciplinary actions.

2. The Rapid ID Device may be used in situations where reasonable suspicion can be articulated that the subject to be printed has committed, or is about to commit a criminal act, when there is a justifiable and reasonable belief that such printing via the Rapid ID Device will either establish or nullify the subject's connection with that crime. The key here is that the use of the Rapid ID Device is used quickly as possible after reasonable suspicion is established.

XVI. STANDARD OPERATING PROCEDURE

A. Failure to comply with the officer's requests to provide a Rapid ID scan under these circumstances may constitute a form of obstruction. However, it may be more appropriate to use the "failure to comply" as further evidence of suspicion of the suspect crime and simply proceed with the investigation without the scan.

B. The Rapid ID Device may be used in situations where the subject to be printed would otherwise be required to give traditional fingerprint samples. Some examples would include:

a. Probable cause criminal arrest situations.

b. When a subject is issued a citation or summons, but does not have valid identification, a Rapid ID might be used to ensure the identity given by the subject is accurate.

c. Positive identification during the execution of a warrant where the subject attempts to present themselves as another and where sufficient identifiers (height, weight, hair and eye color, scars, marks or tattoos) match the identification of the wanted person.

d. The Rapid ID may be used in situations where the use of the device has been specifically authorized pursuant to a valid subpoena; however, if the subpoena is not for immediate compliance, the subject should be allowed to appear for fingerprinting at the future time indicated on the subpoena.

e. When officers use the Rapid ID Device and receive a "HIT" on the suspect(s) fingerprinted, the employee will verify the "HIT" through Fulton County Emergency Communications. The suspect(s) may be legally detained until a positive confirmation is received through Fulton County Emergency Communications.

C. Use of the Rapid ID Device for random or generalized investigation or intelligence gathering, with no focused case or other reason is NOT AUTHORIZED. Special care should be taken to ensure devices are not used for purposes that may lend themselves to the inference of improper "profiling".

Any specialized non-standard use of the Rapid ID Device shall require and authorization by the officer's immediate supervisor/or Division Commander.

D. Examples of non-standard use may include:

   a. Request from an outside agency to fingerprint a suspect in custody. (As long as the requesting agency complies with the procedures set forth in this policy.)

   b. Homicide investigation in which there is no other identifying paperwork for the victim.

   c. To identify an unconscious or otherwise incapacitated subject who cannot be identified by any other means.

   d. To identify persons suffering from a mental disorder and are incapacitated and cannot knowingly object. Guidelines cannot be written to encompass every possible application for the use of a Rapid ID Device. Officers, therefore, should keep in mind the guidelines set forth in this policy to assist them in deciding whether the device may be used or not. Officers are expected to be able to justify, based on these guidelines, training, experience, and assessment of the circumstances, how they determined that the use of the Rapid ID Device was justified under the circumstances. In all cases if there is doubt regarding the appropriate use of this device, a supervisor should be consulted.

XVII. RESPONSIBILITY

Any officer that becomes aware that the Rapid ID Device in their vehicle is not operating properly should immediately notify their supervisor. The supervisor will make timely notification to Internal Affairs or his/her designee. The device will be removed from service until repaired or replaced and in proper working order.

Supervisors shall ensure that all necessary repairs and or replacements of damaged or nonfunctional Rapid ID Devices are documented and repairs performed according to manufacturer's recommendations. The on-duty patrol supervisors shall monitor and ensure officers on their shift follow established guidelines and procedures for the proper use and maintenance of the Rapid ID Device.

XVIII. PHYSICAL SECURITY

A. Criminal history record information and all LEDS files will be maintained in a locking cabinet and/or in a locking and restricted location 24 hours a day.

B. Only authorized personnel specifically authorized by the Primary TAC, Deputy Chief or Chief of Police will operate the terminal.

C. The location where terminals are located shall be off limits to all personnel except those specifically authorized by the Primary TAC, Deputy Chief or Chief of Police, and GCIC/NCIC personnel upon the presentation of official credentials.

D. Criminal justice information received over the terminal will be kept out of public view, stored in locking file cabinets when not needed, and shall be destroyed by department personnel only and shall be destroyed by shredding or burning.

DISCIPLINARY ACTIONS

XIX. Purpose

The purpose of this policy is to establish guidelines for disciplinary action in regard to violations concerning the Georgia Crime Information Center (GCIC) Criminal Justice Information System (CJIS) Network/National Crime Information Center (NCIC) and information obtained thereof.

This policy applies to all agency employees, non-paid employees and vendors/contractors with access, to include physical and logical access, to GCIC/NCIC materials, records and information.

This policy will establish guidelines for disciplinary action in regard to the usage of GCIC/NCIC and information obtained thereof. All personnel with access to Criminal Justice Information (CJI) or any system with stored GCIC/NCIC CJI have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit CJI is a privilege. To maintain the integrity and security of the systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse computing and network resources and systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

All employees are required to follow the policies, rules and procedures set forth by GCIC, NCIC, FBI CJIS Security Policy, and the laws of the State of Georgia.

A. The following disciplinary action will be taken for general working errors that involve violations which are determined to be accidental errors or errors made due to the need of additional training. The severity of the error will be evaluated by the Terminal Agency Coordinator (TAC). This is a general guideline and its use will be determined by the TAC, Deputy Chief and/or Agency Head.
   - 1st offense (for less severe errors) Verbal Warning – additional training.
   - 1st offense or 2nd offense (determined by the severity of error) – written reprimand – additional training.
   - 3rd offense – written reprimand with possible suspension or termination –extensive additional training.
   - 4th offense – employment termination.

B. For deliberate violations and/or misuse of GCIC/NCIC or information obtained thereof: 1st offense – immediate termination and possible criminal prosecution.