Helen Police Department

Standard Operating Policies and Procedures

Chapter C-010 CJIS Operations and Security Breaches	Effective Date:	August 1, 2022	# of Pages:	30
	Revised Date:		Distribution Authorization:	Aletha C Barnett
	Special Instructions:			

I. PURPOSE:

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

II. 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.

III. POLICY:

The Criminal Justice Information System is an integral part of local law enforcement. This agency participates and has access to the state and federal criminal justice information system (computer network). Recognizing this, the Department will follow all CJIS, GCIC, and NCIC policies, procedures, rules, and regulations. These include the CJIS Network Policy Manual, GCIC Operation Manual, GCIC Rules of Council, and the NCIC Code Manual. Additionally, all Department personnel shall abide those rules and procedures contained in this policy. When a conflict occurs, GCIC/NCIC rules and procedures shall supersede.

IV. PROCEDURES:

A. GCIC Computer Terminals

The GCIC Computer shall be operated only by properly trained and certified terminal operators and/or operators in training and while going through the GCIC workbook certification program.

B. GCIC User Agreements

A formal user agreement will be maintained between the Chief of Police and the Deputy Director of the GBI. The Chief of Police is responsible for the Department's compliance with laws and policies regulating the operation of the CJIS network. Each employee of the Department is required to sign an awareness statement indicating that he/she is aware of the penalties of disseminating privileged information obtained from the GCIC network.

C. Law Enforcement Teletype Information

This terminal shall only be used for sending and receiving official law enforcement messages. It is the responsibility of the Communications Operators to enter information into the terminal and to relay necessary information to the officers. GCIC logs received by Georgia CJIS network terminals shall be retained for seven years. All printouts generated by these terminals will be retained in proper secure files or destroyed by shredding when no longer needed.

D. Terminal Agency Coordinator (TAC)

1. The Chief of Police has appointed the Communications Director as Terminal Agency Coordinator (TAC). The TAC is responsible for ensuring all Department employees adhere to all GCIC/NCIC policies pertaining to CJIS network operations.

2. The TAC will perform the following duties:

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

3. Maintain the quality of GCIC/NCIC Record entries regarding timeliness, accuracy, completeness, and validity of records.

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

5. Administer the GCIC terminal operator-training program within the Department and maintain the completed workbooks and associated information pertaining to terminal certification for each terminal user for

a period of two years + 30 days after they leave the Helen Police Department.

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

7. Ensure Department in-service training programs inform employees of requirements and guidelines for the effective use of GCIC/NCIC files and services.

8. Ensure written record validation procedures are established and followed.

9. Maintain copies of all required operation manuals, updates, and revisions, operation bulletins and broadcast messages related to CJIS network operations. Dissemination logs of criminal history records obtained via the CJIS network, and copies of signed User Agreements must also be maintained.

E. Criminal History Record Information (CHRI)

1. CHRI shall only be disseminated as permitted by law. Protected information will not be disseminated to unauthorized persons. Commercial dissemination of federal and state non-restricted (hot) files is prohibited. A criminal history broadcast over radio frequencies must be coded to ensure the message is not intercepted.

2. The type/amount of CHRI disseminated is determined 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 (Fingerprints required GCIC Rules 140-2-.09)

   c. Public and private employment (**Georgia record** only)

   d. Licensing (**Georgia record** only)

   e. Individual inspection of records (**Georgia record** only)

   f. National security checks (**Georgia record** only)

g. Other reasons as provided by law (**Georgia record** only, as determined by law)

h. Criminal histories from GCIC/NCIC terminal responses will be run in accordance with GCIC/NCIC policies and procedures. The proper purpose code will be used for each inquiry, and each will be properly logged. The attention field will be completed correctly by including the last name of the person requesting the history followed by a backslash and the initials of the person running the terminal. The ARN field will be complete, when necessary, with a department reference number such as a case number, citation number, or CAD incident number.

i. Physical Security and Maintenance of all GCIC Hot Files and Supporting Documents

j. All CHRI documents must be maintained in a secure area out of the view of the public and unauthorized personnel. When CHRI documents are not in use by authorized employees, the documents must be kept in secure storage, i.e., locking file cabinets.

k. In the event of natural disaster, the Shift Supervisor or Officer in charge shall have the responsibility of ensuring that records maintained by the department are secured and not in danger of being damaged or destroyed.

l. In the event that department records are not secured or have been damaged and/or destroyed, the Shift Supervisor or Officer in Charge shall make immediate notification to the affected division supervisor and advise them of the situation. If necessary, a police officer(s) shall be stationed in the area to secure said records until the affected area supervisor(s) responds. Affected areas include Records, Municipal Court, Identification, Evidence, Detective Division, and the Chief's Office.

m. The affected division supervisor shall be responsible for taking immediate necessary steps to ensure that all records are secured on site or that said records are removed to another location where they can be secured until such time that they can be returned and secured within the department.

F. CHRI Purpose Codes

Purpose codes are used to indicate the intended use of requested CHRI. Only valid purpose codes determined by GCIC shall be utilized.

G. Logging of Dissemination

1. All dissemination of Criminal Histories must be logged. Each log entry must include:

   a. Date of inquiry

   b. Identifiers used to perform the inquiry

   c. Agency and name of person requesting the inquiry

   d. Name of person to whom the information was released

   e. Name of person releasing the record

   f. Purpose of the inquiry

2. Log entries must be maintained for four years for audit purposes. Refer to GCIC Council Rules and Regulations. If there is any doubt in reference to a method of dissemination, contact the Terminal Agency Coordinator (TAC).

H. First Offender Information

Georgia law and GCIC Council Rules regulate dissemination of CHRI on persons who have completed sentences under the provisions of Georgia's First Offender Act and GCIC Council Rules. Records containing such CHRI will be provided by GCIC (**Georgia record**) 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 another agency desires a response on a "hot file" entered into CJIS by the Department. On all hit confirmation requests, the Communications Officer must confirm, deny, or state specific time needed in response to a hit confirmation for any or all hot file entries within ten minutes if the request is urgent and within one hour if the request is routine. Terminal operators responsible for hit confirmation procedures must have immediate access to back-up case files while on duty.

J. Terminal Down Procedure

In the event that the GCIC computer is down or must be shut down, another agency will be contacted and asked to receive hits for our

department until our terminal can be put back in service. GCIC will then be notified of where to send our hits while our terminal is down.

K. GCIC/NCIC Violation Discipline Policy

1. In the event that GCIC/NCIC policies are violated, the police department will follow the progressive discipline policy laid out by the City of Helen Employee Handbook.

2. As it is not possible to anticipate the circumstances under which every conceivable infraction could take place, employees should not view the progressive discipline policy procedures as all-inclusive or as specifying the appropriate discipline. The level of discipline is determined on a case-by-case basis. Nothing in these procedures alters the fact that employment at the City of Helen is for an indefinite term. However, these procedures should provide guidance on practices the organization will attempt to follow in many situations when verbal instruction or counseling is not effective.

V. HOT FILE ENTRY AND RETRIEVAL

A. All stolen items, such as vehicles, guns, tags, etc., and reported missing persons shall be entered into the GCIC/NCIC system as soon as possible, at the maximum 12 hours. Juveniles reported missing will be entered into the computer immediately. A copy of the original incident report must support all entries. Once an item is recovered or a missing person is located, the hot file entry will be cleared as soon as possible.

1. GCIC Entry of Warrants

2. All warrants are entered into GCIC "hot files" within 12 hours of being posted (if applicable) according to GCIC policy. All information will be verified prior to GCIC entry and again after the entry. Verification is obtained from:

a. Warrant

b. Records arrest file (if applicable)

c. Issuing Department citation copy (if applicable), and

d. GCIC responses from driver's license registration file **(DQ)**, wanted persons file **(QWA)** and criminal history files **(IQ)**.

e. The Communications Officer or other authorized personnel will fill out and print Entry screen including all available information gathered

from the above-mentioned sources before entering the warrant in the GCIC system. After receiving computer verification that the entry was accepted, the NIC number issued will be recorded on the top of the Entry sheet. A copy of the computer entry verification will be made and attached to the Entry. The original Entry sheet and the original computer entry verifications will be forwarded to the next Communications Officer to be second checked for completeness by another Communications Officer and accuracy before being filed in the active warrant worksheet file by the Communications Officer or other authorized personnel. The same person who entered the warrant into GCIC will be responsible for entering the warrant into the computer warrant list.

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

1. Name as listed on warrant (or verified known alias)

a. Date of birth

b. Sex

c. Driver's license number (if known); and

d. Physical description (height, weight, hair color, etc.)

2. Warrant Service

3. When a warrant has been served, the arresting officer will notify the Communication Officer. On-duty communication personnel will perform a "clear" transaction on the GCIC "hot file" entry (if applicable). The warrant will then be copied and both copies will be stamped Warrant Cleared and Communications officer clearing the warrant date and initial in the places provided. The original warrant will be sent to Courts with copies of the GCIC paperwork. A copy of the warrant and the original computer clear verification will be attached to the paperwork removed from the active warrant worksheet file. Both the information just gathered and the paperwork from the active warrant file will be combined and placed in the inactive warrant worksheet file.

C. Warrant Recall/Cancellation

Only the Judge or Court of record has the authority to cancel or recall a warrant issued by the Judge. The Court will communicate this by filling out Cancel Warrant form and giving it to the Communications Officer on

duty. Upon receiving this written notification that a warrant has been recalled, the communications officer will sign and date the form then "cancel" the warrant from the GCIC file. After being signed, the Cancel Warrant form will be given back to the Court. The signed Cancel Warrant form will then be attached to the inactive warrant paperwork and filed in the inactive warrant file.

D. Warrant Arrest/Hold for other Agency

Request to detain and/or attempt to locate individuals wanted by another agency may be received by telephone, fax, or the GCIC terminal. The minimum information required for this agency to hold or attempt to locate is:

1. Name as listed on warrant
2. Date of birth
3. Sex
4. Race
5. Warrant number
6. Charge (code section)
7. Location to check
8. Request to arrest and/or hold

E. Administrative Messages

All administrative, All Points Bulletins (APB), and Be on Look Out for (BOLO) messages sent to other jurisdictions are for official criminal justice business only. For specific requirements and restrictions, refer to the CJIS Network Policy Manual.

F. Stolen Article Entries

1. When articles such as televisions, VCRs, telephones, stereo systems, computers, cable boxes, bicycles, lawn mowers, tools, and equipment, etc. have been stolen, an incident report shall be completed by the investigating officer. Non-recovered stolen property with a serial number for which a theft report has been completed is entered into the GCIC article files. The article file does not include vehicles, guns, boats, tags, and securities.

a. Once the report is completed, it shall be copied and sent to the Communications Officer for entry. All entries must be made within 12 hours of the report being taken.

b. The Communications Officer or other authorized personnel will first fill out and print the Entry sheet including all available information. They will then enter the stolen article into the GCIC computer. After receiving computer verification that the entry was accepted, the NIC number issued will be recorded on the top of the Entry sheet. The entire Entry Sheet and the computer entry verification will be secured together and forwarded to the next Communications Officer to be second checked for completeness and accuracy before being filed in the active article file by the Communications Officer or other authorized personnel. The same person who entered the article into GCIC is required to supply the reporting officer with the NIC number. The reporting officer is then required to enter the number into their report on the record management software in the appropriate property screen.

2. The following items which have a unique manufacturer's serial number or owner-applied number shall be entered into the GCIC files:

a. Any stolen item with a value of $500 or more

b. All office equipment, regardless of value (typewriters, adding machines, etc.)

c. All television sets, regardless of value

d. All bicycles, regardless of value

e. Any stolen article, regardless of value, if the total value of the articles taken in a theft exceeds $5,000

f. Food stamps

g. Any stolen article if circumstances indicate that the articles may be moved across state lines, or the articles are needed for investigative purposes

3. The following information must be included in the incident report for GCIC entry:

a. Brand name of stolen property

b. Date of theft

c. Agency case number

d. Manufacturer's serial number

e. Owner applied number

f. Model number

g. Miscellaneous information about the property (such as color, personal identification markings, etc.)

h. Value of stolen property

G. Stolen Boat and Motor Entries

1. When boats and/or motors have been stolen, an incident report shall be completed by the investigating officer and entered in the GCIC boat files.

   Once the report is completed, it shall be copied and sent to the dispatcher for entry. All entries must be made within 12 hours of the report being taken.

      The Communications Officer or other authorized personnel will first fill out and print an Entry sheet including all available information. They will then enter the stolen boat/motor into the GCIC computer. After receiving computer verification that the entry was accepted, the NIC number assigned will be recorded on the Entry sheet. The entire Entry sheet and the computer entry verification will be secured together and forwarded to the next Communications Officer to be second checked for completeness and accuracy before being filed in the active boat/motor worksheet file by the Communications Officer or other authorized personnel. The same person who entered the stolen boat/motor into GCIC is required to supply the reporting officer with the NIC number. The reporting officer is then required to enter the number into their report on the record management software in the appropriate property screen.

2. The following information must be included in the incident report for GCIC entry:

   a. Registration/document number, state and year

   b. Boat hull number

c. Owner applied number

d. Propulsion type

e. Boat year

f. Boat make

g. Boat type, length, and color

h. Date of theft

i. Agency case number

j. Miscellaneous information

3. For supplemental stolen boat parts, the following must be included in the report for GCIC entry:

a. Registration/document number

b. Boat hull serial number

c. Agency case number

d. Serial number

e. Owner applied number

f. Brand code

g. Engine power/displacement

h. Miscellaneous information

i. Stolen Gun Entries

4. Serial numbered weapons (and accessories) which use explosive, compressed air, or carbon dioxide to propel a projectile and have been reported stolen or recovered (found by our agency but reported stolen by another agency) shall be recorded on an incident report by the investigating officer and entered in the GCIC gun files. BB guns and pellet guns which are less than .22 caliber should not be entered in these files. They should be entered in the article file

1. Once the report is completed, it shall be copied and sent to the Communication Officer for entry. All entries must be made within 12 hours of the report being taken.

2. The Communications Officer or other authorized personnel will first fill out and print an entry sheet including all available information. They will then enter the stolen gun into the GCIC computer. After receiving computer verification that the entry was accepted, the NIC number assigned will be recorded on the top of the Entry sheet. The entire Entry sheet and the computer entry verification will be secured together and placed into the letter bin to be second checked for completeness and accuracy before being filed in the active gun worksheet file by the Communications Officer or other authorized personnel.

5. The following weapons shall be entered in the gun files:

   a. Pistols (including starter pistols)

   b. Rifles

   c. Shotguns

   d. Machine guns

   e. Antique guns

   f. Cannons

   g. Disguised firearms (cane guns, pen guns, etc.)

   h. Firearm mufflers or silencers

   i. Firearm frames or receivers

   j. Grenades

   k. Mines

   l. Missiles and rockets

6. The following information must be included in the incident report for GCIC entry:

   a. Serial number

b. Make

c. Model

d. Caliber

e. Type of gun

f. Date of theft

g. Agency case number

h. Miscellaneous information

H. Vehicle, Abandoned Vehicle, and Tag Entries

1. A vehicle is any motor driven means of transportation designed to carry an operator, except a boat. Stolen vehicles abandoned vehicles and stolen tags shall be recorded on an incident report by the investigating officer and entered in the GCIC vehicle files. Automotive accessories (radios, tape players, etc.), bicycles, tag renewal decals, vehicle emission stickers should not be entered in the vehicle file but should be entered in the article file.

2. Once the report is completed, it shall be copied and sent to the Communication Officer for entry. All entries must be made within 12 hours of the report being taken.

3. The Communications Officer or other authorized personnel will first fill out and print an Entry sheet including all available information. They will then enter the stolen vehicle into the GCIC computer. After receiving computer verification that the entry was accepted, the NIC number assigned will be recorded on the top of the entry sheet. The entire Entry sheet and the computer entry verification will be secured together and forwarded to the next Communications Officer to be second checked for completeness and accuracy before being filed in the active stolen vehicle worksheet file by the Communications Officer or other authorized personnel. The same person who entered the stolen vehicle into GCIC is required to supply the reporting officer with the NIC number. The reporting officer is then required to enter the number into their report on the record management software in the appropriate property screen.

4. The following stolen, felony or abandoned/recovered items are included in the vehicle file:

a. Aircraft

b. All-terrain vehicles

c. Automobiles

d. Construction equipment

e. Farm and garden equipment

f. License plates (stolen/missing)

g. Motorcycles

h. Snowmobiles

i. Special vehicles (golf carts, dune buggies, etc.)

j. Trailers (all but boat trailers)

k. Trucks

l. Vehicle parts (transmissions, engines, certificates of title, registration, origin, VIN plates, wheels, and outboard motors)

5. The following information must be included in the incident report for GCIC entry:

a. License plate number

b. License state

c. License/decal issue year

d. License type

e. Date of theft

f. Vehicle year

g. Vehicle make

h. Vehicle model

i. Vehicle style

j. Vehicle identification number

k. Owner applied number

l. Vehicle color

m. Agency case number

n. Miscellaneous information

I. Abandoned Vehicles -- Georgia law requires law enforcement agencies to enter records on vehicles which have been abandoned and impounded by law enforcement agencies or vehicles which have been reported as impounded by operators of wrecker services or vehicle storage facilities in the abandoned vehicle file. Abandoned and impounded vehicle information shall be recorded on an incident report by the investigating officer then copied and sent to the Communications Officer for entry. All entries must be made within 12 hours of the report being taken.

J. The Communications Officer or other authorized personnel will first fill out and print an Entry sheet including all available information. They will then enter the abandoned vehicle into the GCIC computer. After receiving computer verification that the entry was accepted, the NIC number assigned will be recorded on the Entry sheet. The entire Entry sheet and the computer entry verification will be secured together and forwarded to the next Communications Officer to be second checked for completeness and accuracy before being filed in the active abandoned vehicle file by the Communications Officer or other authorized personnel. The same person who entered the abandoned vehicle into GCIC is required to supply the reporting officer with the NIC number. The reporting officer is then required to enter the number into their report on the record management software in the appropriate property screen.

1. Georgia law (O.C.G.A. 35-3-33, 35-3-36 and 40-11-2) requires law enforcement officers to:

a. Enter abandoned vehicle records in the computerized abandoned vehicle file after the wrecker service or vehicle storage facility has given notice in writing.

b. Furnish legitimate operators of wrecker services and vehicle storage facilities with the names and addresses of the last known registered owner of the recovered abandoned vehicle.

c. When vehicles are recovered, the vehicle owner must be notified within 72 hours of the vehicle's recovery and location. Notification is the responsibility of the investigating officer.

2. The following information must be included in the incident report for GCIC entry:

a. Vehicle make, model, style, and year

b. Agency case number

c. License plate number

d. License decal issue year

e. Vehicle identification number

f. Vehicle color

g. Miscellaneous information

VI. VALIDATION OF GCIC ENTRIES

A. Validations are conducted monthly to check validity, status, correct spelling and add additional information if needed. A record is valid if supporting documentation exists and is current, wanted persons not apprehended, missing persons not found, or stolen property not recovered. On all validations, the individual case files shall be reviewed to determine if information is accurate, complete, and current.

B. An e-mail sent from GCIC to the TAC to ensure that the FS VALD screen is completed on the CJIS network to verify that the validation notice has been received. The confirming computer printout that returns in response to the VALD entry is to be saved and attached to the monthly validation paperwork.

C. Validation of Wanted Persons:

D. The TAC or other designated person will check case files to determine if the information in the warrant entry is accurate, complete, and current (i.e., when using a caution INDICATOR – C, to indicate that caution should be taken, an explanation must be placed in the miscellaneous filed).

E. The TAC or other designated person will check the original warrant, warrant docket, magistrate, state, and superior courts, or other sources to ensure that each warrant supporting the record entry is still valid (i.e., has warrant been served, dismissed, or recalled).

F. The TAC or other designated person will contact the prosecutor to determine whether extradition from all jurisdictions within the limits cited in each record entry is still applicable (i.e., a case where an agency receives information that a state will not honor the extradition of an individual, modify the miscellaneous field to show the words will not extradite from…)

G. The TAC or other designated person will check with the investigator and prosecutor to determine if the case can and will be prosecuted.

H. The TAC or other designated person will inquire into the Driver's License and Criminal History files (DQ and IQ) to obtain any additional information that can made the entry more complete or accurate and update the warrant entry as needed.

I. Missing Persons Validation:

1. The TAC or other designated person will check case files to determine if the information is accurate, complete, and current.

2. The TAC or other designated person will check with investigators to determine if the subject is still missing and is still being sought. Also, to ensure that missing information is also correct, (i.e., social security number, blood type, jewelry, etc.).

3. The TAC or other designated person will contact the person reporting the incident to determine if the subject is still missing and obtain any additional information that will make the record entry more complete.

4. Unidentified Bodies Validation:

5. The TAC or other designated person will check case files to determine if information is accurate, complete, and current.

6. The TAC or other designated person will contact the investigator to determine if the body has been identified.

J. Stolen Vehicle Validation:

1. The TAC or other designated person will check the case files to determine if the information is accurate, complete, and current.

2. The TAC or other designated person will determine if the National Insurance Crime Bureau (NICB) interest is indicated on each record entry by checking the Vehicle Ownership Data (VOD) field for the presence of the letter A, C, D, N, or S. (*see below*)

3. The TAC or other designated person will contact the appropriate NICB office to determine each new owner's name.

    a. A - ILNATBCII (Atlanta, Georgia)
    b. C - ILNATBC00 (Chicago, Illinois)
    c. D - TXNATBDOO (Dallas, Texas)
    d. N - NYNATBNOO (New York, New York)
    e. S - CANATBSOO (San Francisco, California)

4. The TAC or other designated person will contact the investigator and owner/new owner to determine if the vehicle has been recovered or if there is additional information to add to the record entry.

5. The TAC or other designated person will contact the owner/complainant to determine if the vehicle has been recovered.

6. The TAC or other designated person will check the NICB file by running a NAQ inquiry to determine if ownership has changed or if the vehicle has been impounded or recovered.

7. A loaned, rented, or leased vehicle must have an official theft report from the company who owns the vehicle or who filed the complaint that resulted in the issuance of the warrant.

K. Other Property (Boats, Securities, Guns) Validations:

1. The TAC or other designated person will check case files to determine if the information is accurate, complete and current.

2. The TAC or other designated person will contact the investigator and owner to determine if property has been recovered.

L. When the previous steps one through five have been completed, the TAC or other designated person will take the following actions.

M. Cancel all records that are invalid, have no case file documentation, or are no longer of interest, except for stolen gun records. Stolen gun records will remain in the system until such a time that the Chief should decide that they can be removed.

N. Clear all records showing a Locate posted by another agency or recovered by your agency that have not already been cleared.

O. Make supplemental entries when additional information becomes available.

P. If records indicate that a caution indicator should have been used on a person entry, cancel and reenter using caution screen.

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

R. When the five steps above have been completed, the TAC or other designated person will certify validations via the CJIS Network using the GTA web site and validation screen.

VII. HOT FILE CLEARANCE AND CANCELATION

A. When a stolen item is recovered that was in the Hot File, the record must be ***cleared*** from the GCIC computer. This is to be done by the Communication Officer on duty. The Communication Officer is to clear the item(s) from the GCIC computer using the appropriate clearance message key for that item(s). The officer taking the report of the recovered item it responsible for going back to the original report of the stolen property, if it was our report, to show who removed that the item from the GCIC computer and when it was removed. If the property is recovered somewhere else and the Communications Officer receives a Locate message, the Communications Officer will verify the information and then clear the item from the GCIC computer using the appropriate message key for that item. The Communications Officer will also pull the active file for the item and attach the original GCIC print out of the clearance and move the file to the inactive files. The Communications Officer will call an officer in to do a supplemental report of the recovered property to be added to the original report of the stolen property. The officer doing the supplemental will then go into the original report and show who and when the item was removed from the GCIC computer.

B. When a stolen item is determined to no longer be a valid GCIC entry, it must be ***cancelled*** from the GCIC computer using the appropriate message key for that item. It is the responsibility of the Communications Officer on duty to cancel the item from the GCIC computer upon verification of the non-valid status. The Communications Officer will also pull the file from the active files and attach the GCIC computer printout of the cancellation to it and move it to the inactive files. The Communications Officer will call an officer to do a supplemental report for the original file to show why that the item was cancelled and when it was removed from the GCIC computer and who removed it.

C. When a person is arrested on a Helen Municipal Warrant, the arresting officer is responsible for notifying the Communications Officer of the service. The Communications Officer is responsible for removing the warrant from the GCIC computer, the RMS system, and pulling the active warrant and

attaching a copy of the GCIC computer printout to it and returning it to the Helen court.

VIII. SECURITY INCIDENT REPORTING HANDLING FOR INFORMATION DERIVED FROM THE GEORGIA CRIME INFORMATION CENTER (GCIC) CRIMINAL JUSTICE INFORMATION (CJIS) NETWORK

A. The Helen Police Department shall ensure the protection of Criminal Justice Information (CJI) / Criminal History Record Information (CHRI). All agency employees and vendors/contractors with access, to include physical and logical access, to GCIC/NCIC materials, records and information are required to ensure proper preparation, detection, analysis, containment, recovery, user response, tracking, documenting, handling and incident reporting procedures are followed for all security incidents.

B. Definitions:

1. Local Agency Security Officer (LASO) – The LASO is an individual appointed by the Chief to assume ultimate responsibility for managing the security of CJIS systems within the agency.

2. Information Security Officer (ISO) – an individual appointed by GCIC and serves as the security point of contact to the FBI CJIS Division ISO and is responsible for establishing and maintaining information security policies, assesses threats and vulnerabilities, performs risk and control assessments, and oversees the governance of security operations.

3. Physically Secure Location – A facility, a police vehicle, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associate information systems.

C. Agency employees and vendors / contractors with access, to include physical and logical access, to GCIC materials, records, and information 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.

Authorized personnel of the agency shall protect and control electronic and physical CJI/CHRI while at rest and in transit. The department will take appropriate safeguards for protecting CJI/CHRI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate disclosure must be reported to the Chief, TAC, LASO, and GCIC.

Personally owned information systems shall not be authorized to access, process, and store or transmit criminal justice information. All devices with access to CJI must be authorized and must meet the requirements set forth by the CJIS Security Policy.

D. Security Incident Preparation, Prevention and Handling:

1. The Chief shall ensure the perimeter of all physically secure locations are prominently posted and separated from non-secure locations by physical controls.

2. The Department's Terminal Agency Coordinator (TAC) shall:

a. Ensure general incident response roles and responsibilities are included as part of required security awareness training.

b. Maintain personnel listings with authorized access to physically secure location.

c. Control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

3. The agency's LASO shall:

a. Maintain automated mechanisms to assist in the reporting of security incidents. The Helen Police Department currently employs:

1. Microsoft Advanced Threat Protection that provides comprehensive computer protection against known and new threats, network and phishing attacks, and other unwanted content. Each type of threat is handled by a dedicated component. Components can be enabled or disabled independently of one another, and their settings can be configured.

2. Microsoft Advanced Threat Protection and internet security software that prevents, detects, and removes malicious software.

b. Ensure proper tracking and documentation of information system security incidents on an ongoing basis.

c. Identify who is using approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

d. Identify and document how the equipment is connected to the state system.

e. Ensure that personnel security screening procedures are being followed as stated in this policy.

f. Ensure the approved and appropriate security measures are in place and working as expected.

g. Ensure advanced authentication, encryption, security-related updates, official use guidance, data at rest encryption, and prevention of data compromise is utilized for all departmental approved mobile devices with access to CJI.

h. Be able to easily identify connected users and devices of all departmentally approved devices with access to CJI.

i. Track, log and manage every personally used device allowed to connect to agency technology resources for secure CJI access.

j. Identity individuals who are responsible for reporting incidents within their area of responsibility.

k. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.

l. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.

m. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement point of contacts within the area.

n. Act as a single point of contact for their jurisdictional area for requesting incident response assistance.

o. Track and document information system security incidents on an ongoing basis.

p. Maintain completed security incident reporting forms until the subsequent GCIC triennial audit or until legal action (if warranted) is complete; whichever timeframe is greater.

4. All authorized personnel of the agency shall:

a. Monitor physical access to the information system to detect and respond to physical security incidents.

b. Control physical access by authenticating visitors before authorizing escorted access to the physically secure location.

c. Ensure all visitors to the physically secure location are escorted by authorized personnel and monitored at all times.

d. Authorize and control information system-related items entering and exiting the physically secure location.

e. Securely store electronic and physical media within physically secure locations or controlled areas. The Helen Police Department shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted.

f. Protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

g. Utilize local device authentication to unlock mobile devices authorized by the agency for use in accessing CJI.

h. Use caution when downloading internet content or clicking on web-based pop-ups/windows, unknown emails, embedded objects and email attachments or utilizing removable devices such as flash drives, CDs, etc.

i. Be familiar with the City of Helen Personnel Policies and Procedures Manual Section 8 Discipline and Appeals policy.

5. Security and Incident Reporting:

a. Any security incidents that may arise shall be reported immediately to the Chief of Police, LASO, TAC and GCIC. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

b. All employees and contractors shall be made aware of the procedures for reporting the different types of events 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.

c. Once notified the department's LASO will notify the Chief of Police, TAC, and GCIC.

d. If deemed necessary, the department's LASO will notify GCIC to relay the preliminary details of the incident.

e. If deemed necessary, the Chief of Police or his/her designee will conduct an investigation of the reported incident and submit an incident response form to GCIC once all the information has been gathered.

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

6. Security Incident Reporting for Mobile Devices:

a. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

b. All employees of the agency with approved mobile device access to CJI shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses.

c. If deemed necessary, the LASO will:

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

2. Notify the Chief of Police and TAC to relay the preliminary details of the incident.

3. Assist the Chief of Police or his/her designee with the investigation and submission of an incident response form to GCIC once all the information has been gathered.

d. Where a follow-up action against a person or department after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to

conform to the rules for evidence in accordance with agency's standard operating procedure regarding evidence procedures.

e. Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control – The device is in the physical control of a non-CJIS authorized individual, or the device is left unattended in an unsecure location (e.g., counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device setting could be tampered with or data on the device could be illicitly accessed.

2. Total loss of device – The physical location of the device is unknown, the device has been accidentally destroyed beyond means of information retrieval (i.e., incinerated, shredded), or the device has been dropped in an area that prevents retrieval such as the lake or ravine.

3. Device compromise – This includes rooting, jail breaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions).

f. In the event of a total loss of device, loss of control, or device compromise, the LASO will:

1. Notify the Chief, TAC, and GCIC to relay the preliminary details of the incident.

2. Enable mobile device locating features if the security device has not been compromised. (i.e., the device has been misplaced within the department or another secure location)

3. Contact the mobile device carrier and request assistance with device tracking.

a. If tracking for the mobile devices is unsuccessful the department LASO will:

1. Secure, control, or remotely erase all data on any department issued mobile device with CJI assess as deemed necessary.

2. Utilize remote features to “lock/kill” all device hardware.

3. Once the “lock/kill” feature has been activated, the LASO will contact the device carrier to ensure the mobile device has been successfully “locked/killed”.

4. If remote “lock/kill” feature is unavailable, a request to disable the mobile device via the network will be made to the carrier.

4. Notify GCIC of loss and request assigned ORI to be deactivated.

5. Assist the Chief of Police or his/her designee with the investigation and submission of an incident response form to GCIC once all the information has been gathered.

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

E. All security incidents and/or GCIC violations will be reported in writing to the GCIC Deputy Director by the Chief or his/her designee, in accordance with GCIC policies and procedures.

IX. USER ACCOUNT ACCESS-VALIDATION AND REMOVAL OF ACCESS

A. The Helen Police Department shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Georgia Crime Information Center (GCIC) / National Crime Information Center (NCIC) User Account Access shall be validated at least annually, and the Terminal Agency Coordinator (TAC) shall document the validation process.

1. All accounts shall be reviewed 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.

2. All guest accounts (for those who are not official employees of the criminal justice agency with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor

personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

3. 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.)

4. 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 TAC, LASO or designee will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

5. Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC).

6. The TAC, LASO, or designee shall:

   a. Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,

   b. Periodically review existing accounts for validity, and

   c. Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

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

X. MEDIA PROTECTION

A. The Helen Police Department will ensure the protection of Criminal Justice Information (CJI) / Criminal History Record Information (CHRI). All agency employees, vendors / contractors with access, to include physical and logical access, to any electronic or physical media containing CJI/CHRI while being stored, accessed or physically moved from a physically secure location. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.
Authorized personnel shall protect and control electronic and physical CJI/CHRI while at rest and in transit. The Helen Police Department will take

appropriate safeguards for protecting CJI/CHRI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate disclosure and/or must be reported to the Chief or designee and the Local Agency Security Officer (LASO). All employees and vendors / contractors are required to follow the policies, rules and procedures set forth by GCIC, GCIC Council Rules, FBI CJIS Security Policy, and the Laws of the State of Georgia.

Controls shall be in place to protect electronic and physical media containing CJI/CHRI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disc, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI/CHRI.

B. Media Storage and Access: To protect CJI/CHRI, personnel shall:

1. Securely store within a physically secure location or controlled area.

2. Restrict access to unauthorized individuals.

3. Restrict the pickup, receipt, transfer and delivery to authorized individuals.

4. Ensure that only authorized users remove printed form or digital media from the CJI/CHRI.

5. Physically protect the media end of life.

6. Not use personally owned information to access, process, store, or transmit CJI/CHRI.

7. Not utilize publicly accessible computers to access, process, store, or transmit CJI/CHRI. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public libraries, public kiosk computers, etc.

8. Store all hard copy printouts maintained in a secure area accessible to only personnel whose job function require them to handle such documents.

9. Safeguard against possible misuse.

10. Take appropriate action when in possession, while not in a secure area.

a. Must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

1. When CJI is at rest (i.e., stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, and laptops, etc.

2. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

c. Lock or log off computer when not in immediate vicinity of work area.

d. Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality.

C. Electronic Media Sanitization and Disposal:

The Helen Police Department shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release to reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.) The Helen Police Department shall maintain written documentation of the steps taken to sanitize or destroy electronic media. The destruction must be carried out by the LASO and be witnessed by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures.

D. Violation of any of these requirements in this policy by any authorized personnel will result in suitable disciplinary action, as outlined in The City of Helen Personnel Policies and Procedures Manual Section 8 Discipline and Appeals. Violations must be immediately brought to the attention of the Chief of Police. Chief of Police must report all GCIC violations in writing to the GCIC Deputy Director.

XI. Violation of any of the requirements in this policy by any authorized personnel may result in criminal prosecution by the State of Georgia, and/or administrative

sanctions including, but not limited to, termination of employment with the Helen Police Department.