




# Clayton County Police Department

# PROCEDURES

Subject		Procedure #	
<b>GCIC &amp; CENTRAL WATCH OFFICE PROCEDURES</b>		<b>D41</b>	
Authorizing Signature	Effective	<input type="checkbox"/> New <input checked="" type="checkbox"/> Amended <input type="checkbox"/> Rescinds	Total Pages
	<b>03-23-2023</b>		<b>12</b>

## I. PURPOSE

The purpose of this policy is to provide procedures for GCIC Operators and supervisors during the operation of the GCIC Terminal and the Central Watch Office, and Security Awareness for all employees regarding direct or indirect access to Criminal History Record Information (CHRI), Criminal Justice Information (CJI), Criminal Justice Information System (CJIS), etc. Also, general guidelines for the duties while assigned to the Central Watch Office to include, but not limited to building access and security procedures, impounded vehicle releases, impound/repossession database entry, parking ticket data entry, receiving *Incident Reports*, etc.

## II. POLICY

It is the policy of the Clayton County Police Department (CCPD) to comply with all GCIC rules. Employees are bound by the GCIC Council Rules on the use of CJIS. Personnel assigned to the Central Watch Office will also assist the public by providing information and taking police reports. It is the responsibility of the Central Watch Office to control visitors and the areas in which they are allowed to access. This will ensure the security of CCPD Headquarters, and the security of the records, equipment and personnel within the secure areas.

The CCPD will appoint and maintain a Terminal Agency Coordinator (TAC) to represent and speak for the Chief of Police in matters pertaining to the proper administration of NCIC/GCIC rules and regulations. An instruction from the TAC to correct a NCIC/GCIC error is to be considered a direct order from the Chief of Police and compliance is mandatory. This policy applies to all employees, staff, volunteers and/or other workers with access, directly or indirectly, to CHRI, CJI, CJIS, etc.

## III. DEFINITIONS

The following definitions are pursuant to *GCIC Council Rule 140-1-.02*:

Criminal History Record Information (CHRI): Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments,

information, or other formal charges, and any disposition arising there from including acquittal, sentencing, correctional supervision and release. Documents meeting the criteria for CHRI include, but are not limited to criminal fingerprint cards, final case dispositions, rap sheets or terminal responses (local, state, or federal).

Criminal Justice Information (CJI): Any and every type of information that is collected, transmitted or maintained by CJIS which includes all criminal justice agencies. CJI includes, but is not limited to, the following types of information: CHRI; restricted data such as procedures, manuals and data gathering techniques; secret data such as operational measures to protect CJIS and other CJI systems; sensitive data such as intelligence documents, lists and/or reports.

Criminal Justice Information System (CJIS): All agencies, procedures, mechanisms, media and forms, as well as the information itself, which are or become involved in the organization, transmission, storage, retrieval and dissemination of information related to reported offenses, offenders and the subsequent actions related to such events or persons.

Local Agency Security Officer (LASO): An individual appointed by the Chief of Police to assume ultimate responsibility for managing the security of CJIS within this Department.

Secured Areas: Areas in which a keycard or key for door that is normally locked, is required to gain access is a secured area.

Terminal Agency Coordinator (TAC): An employee designated by the Chief of Police to be responsible for ensuring departmental compliance with state and federal policies, regulations and laws established by GCIC, the FBI's CJIS Division and NLETS.

Terminal Operator: An employee whose primary job function is accessing the CJIS network.

#### **IV. GCIC TRAINING, SECURITY & DISPOSAL**

This procedure applies to all employees, staff, volunteers and other workers with access and/or the ability to access, to include physical and logistical access, CJI in any form. This procedure applies to all equipment used to access, obtain, view, disseminate and store CJIS information and/or other classified and sensitive data.

##### **A. Security Awareness Statement & Training**

All employees, interns and volunteers of this Department have access, directly or indirectly, to CHRI, CJI, CJIS, etc., and are bound by the GCIC Council Rules on the use of the CJIS.

1. Each employee, intern or volunteer is required to complete and sign a *Georgia Crime Information Center (GCIC) Awareness Statement* upon being hired or rehired, or accepted as an intern or volunteer. This requirement applies to any new hire, intern or volunteer who previously completed and signed the *GCIC Awareness Statement* with or for a former employer or agency.
2. Each employee, intern or volunteer shall complete Security Awareness Training within sixty (60) days of their employment, or initiation of internship or volunteer work. Each employee, intern or volunteer shall complete the training annually thereafter. In addition, each time an employee, intern or volunteer completes Security Awareness Training, they will complete a new *GCIC Awareness Statement*.
3. Each employee with credentials to access any system (LEMS, MCT, etc.) that possesses the ability to operate GCIC shall complete CJIS Network Operator Training annually. Each year CJIS Network Operator Training is completed, a copy of the certificate will be submitted to the Academy Unit and the departmental TAC.

4. Each completed and signed *GCIC Awareness Statement* from an employee, intern or volunteer, will be filed and maintained in that employee, intern or volunteer's departmental personnel file. Each year Security Awareness Training is completed, a copy of the certificate will be submitted to the Academy Unit along with a departmental *Training Report*.

#### B. Access to CJIS

Upon completion of CJIS Network Operator Training, as applicable, and/or required Security Awareness Training, access to CJIS may be granted. Access may be denied, revoked or temporarily suspended. Only the TAC and Local Agency Security Officer (LASO), or authorized designee, has the administrative ability to grant, deny, revoke or temporarily suspend CJIS access, at the discretion of the Chief of Police.

#### C. Security of CJI, CJIS & CHRI

1. All information obtained from CJIS, which includes, but is not limited to, CJI, CHRI, GCIC, NCIC, local data files, etc., is considered sensitive and classified. Such information shall be securely accessed, obtained, possessed, viewed and/or disseminated.
2. Employees shall maintain security over all CJI, CJIS and CHRI they access, obtain, possess, view and/or disseminate at all times. This rule is in place to protect sensitive and classified information, employees, and the Department.
3. Required Notifications Due to Misuse of CJI, CJIS, CHRI

In the event an incident of intentional or negligent misuse of CJIS, CJI or CHRI occurs or is discovered, the concerned supervisor will immediately notify the TAC, Communications & Records Division Major, Chief of Police and concerned chain of command.

- a. It will be the responsibility of the TAC or Communications & Records Division Major to notify the appointed LASO.
- b. Once the LASO has been notified, employees will adhere to and/or assist with following the *County Department of Information Technology (DoIT) Incident Response Plan* (refer to Appendix B of this procedure).

When notification of the TAC, Communications & Records Division Major, Chief of Police and concerned chain of command is completed, that does not alleviate the concerned supervisor's responsibility to adhere to CCPD SOP *E1: Internal Affairs Investigations* regarding the generation, reporting and investigation of complaints.

#### D. Disposal of CJI

1. When no longer usable or in use, or the purpose for the information is no longer needed or valid, all CJI shall be disposed of in a manner that will no longer allow access, possession, viewing or dissemination.
2. Each employee has an individual responsibility for the disposal of all CJIS information they access, obtain, view, receive or possess once it is no longer usable or in use, or its purpose is no longer needed or valid.
3. CJI documentation will be shredded. Any other method of disposing of CJI is prohibited.
4. If the Department utilizes a County-approved vendor for the shredding and/or destruction of CJI documentation, the vendor's representative must be escorted. Only an employee with current Security Awareness Training is authorized to escort the vendor's representative throughout Department buildings and/or facilities to witness the collection

and shredding and/or destruction of the CJI documentation. Generally, the Central Records & Permits Unit shall be responsible for escorting the vendor's representative for CJI disposal, unless extenuating circumstances exist.

#### E. Disciplinary Action

All investigations regarding alleged GCIC procedure violations shall be investigated in accordance with CCPD SOP *E1: Internal Affairs Investigations*.

1. Any employee who fails to secure or dispose of CJIS information in accordance with this procedure may be subject to disciplinary action, up to and including termination.
2. Any employee who intentionally or negligently misuses CJIS, CJI or CHRI in violation of this procedure may be subject to disciplinary action, up to and including termination.
3. Employees in violation of this policy will be subject to disciplinary action, in addition to any GCIC administrative sanctions or criminal action.

Refer to CCPD SOP *B11: Disciplinary Procedures, Appendix A: Discipline Guide*, regarding progressive discipline for violations of this procedure.

### V. GCIC TERMINAL PROCEDURES

A. One (1) certified terminal operator will be assigned to the Central Watch Office at all times. A terminal operator must have completed the GCIC terminal operator course and should have forty (40) hours of training working in the Central Watch Office. Whenever an operator is relieved, they will be replaced by another certified operator. The terminal operator may take short five (5) minute breaks outside of the Watch Office during their shift without being relieved, but these are limited to no more than three (3) per shift.

#### B. Terminal Operator Responsibilities

1. Requirement to Notify GCIC due to Extenuating Circumstances
  - a. In the event that the extenuating circumstances interrupt, delay or cease operation of the GCIC terminal, GCIC shall be notified by the Terminal Operator immediately via phone (404-244-2770). Notification shall be made by the Terminal Operator as soon as possible via both of the following methods: [1] Administrative Message (AM), [2] email [gcicidc@gbj.ga.gov](mailto:gcicidc@gbj.ga.gov).
  - b. Once the GCIC terminal is operational again, the Terminal Operator will notify GCIC immediately via all three (3) notification methods.
2. Urgent Requests for Hit Confirmations
  - a. All urgent requests for hit confirmations will be acknowledged within ten (10) minutes. At a minimum, the requesting agency will be notified confirming the request was received and advised of an estimated time that the confirmation will be completed.
  - b. Terminal operators will attempt to confirm or deny hit requests as soon as possible, and will keep the requesting agency informed of the progress on the request.
  - c. If a second or subsequent urgent request for hit confirmation is received:
    - 1) The terminal operator will acknowledge the request as stated above and contact the TAC to advise them that a failure to respond has occurred. If the failure to respond occurs when the TAC is unavailable, the shift commander will be notified.

- 2) The terminal operator will complete a "Departmental Use Only" *Incident Report* detailing the circumstances of the failure to respond and attach all documentation concerning the incident. The report will be forwarded to the TAC.
  - 3) Any incident involving the failure to respond to an urgent request for hit confirmation shall be investigated and documented by an immediate supervisor.
3. All other confirmations will be made within GCIC prescribed time limits.
  4. GCIC entries are the responsibility of the GCIC Operator.
    - a. If a report requiring an entry is taken over the phone, one (1) of the two (2) Central Watch Office employees will take the report and the entry will be made by the GCIC Operator. This includes calls transferred from a sector precinct.
    - b. Phone calls that do not require an entry to be made may be transferred to the appropriate sector precinct so that a report may be taken.
    - c. If the terminal operator is a reporting officer, an *Incident Report/Supplemental Report* shall be completed for all GCIC entries, modifications, removals and Criminal History Record Information (CHRI) queries. If the terminal operator is not a reporting officer, then the *Incident Report/Supplemental Report* from the reporting officer is sufficient.
      - 1) Terminal operators will print out all entry screens and GCIC responses, and complete a character-by-character comparison of all supporting documents for verification purposes, and initial the paperwork and write their names, the corresponding case number and the reporting officer's name on each document.
      - 2) Terminal operators will ensure their name is in the miscellaneous field of all GCIC entries they complete.
      - 3) A vehicle registration will be checked to ensure the victim is the owner of the vehicle/tag being reported stolen. The GCIC registration paperwork will be attached to the operator's paperwork.
      - 4) All copies of reports will be labeled as "copy."
  5. GCIC Entry for Theft by Conversion-Motor Vehicle

The criminal elements of OCGA § 16-8-4 apply. The following procedures do not apply when exigent circumstances exist.

- a. Conversion without a Written Contract

- 1) At the time of the report, the reporting officer shall inform the complainant or victim of the applicable requirements and procedures described below.

If an alleged theft by conversion-motor vehicle incident involves two (2) or more parties loaning or borrowing a motor vehicle **without** a lease or rental agreement (written contract), the *Incident Report* will be titled 'theft by conversion-motor vehicle;' and GCIC entry will not be made until the following has been obtained:

- a) Written statement from the complainant or victim reporting the theft; **and**
  - b) Proof or confirmation of ownership.
- 2) Generally, for theft by conversion-motor vehicle cases involving two (2) or more parties renting or leasing a motor vehicle **without** a lease or rental agreement

(written contract), the Department shall be responsible for pursuing any applicable arrest warrant(s) and criminal prosecution. This is due to the fact that a follow-up investigation may be required to obtain the necessary evidence to establish probable cause. However, circumstances and evidence may dictate otherwise.

b. Conversion with a Written Contract

- 1) At the time of the report, the reporting officer shall inform the complainant or victim of the aforementioned requirements and procedures described below.

If an alleged theft by conversion-motor vehicle incident involves two (2) or more parties renting or leasing a motor vehicle **with** a lease or rental agreement (written contract), the *Incident Report* will be titled 'theft by conversion-motor vehicle; and GCIC entry will **not** be made until **all** of the following have been obtained and completed:

- a) Written statement from the owner or owner's agent reporting the theft;
- b) Copy of the lease or rental agreement (written contract); **and**
- c) Proof of documentation that five (5) days have passed, weekends and holidays excluded, since the motor vehicle owner or owner's agent has mailed, via certified or registered mail or statutory overnight delivery, return receipt requested, to the lessee or renter's last known address, a letter demanding return of the motor vehicle, pursuant to OCGA § 16-8-4(c)(2).

- 2) For theft by conversion-motor vehicle cases involving two (2) or more parties renting or leasing a motor vehicle **with** a lease or rental agreement (written contract), the owner or owner's agent shall be responsible for pursuing any applicable arrest warrant(s) and criminal prosecution. This is due to the fact that the owner or owner's agent has possession of all necessary evidence and knows the identity of the suspect(s).

- c. In addition to the field reporting procedures outlined in CCPD SOP *D9: Field Reporting*, the corresponding *Incident Report* narrative shall explain what criteria has or has not been met for a GCIC entry of a theft by conversion-motor vehicle incident, to include indicating whether or not the GCIC entry was made."

6. GCIC Actions Taken on Behalf of Other Agencies

There are other law enforcement agencies that rely, either full/part time, on the CCPD for the completion of GCIC actions. Due to the GCIC services provided by this Department to other agencies, all GCIC Terminal Operators shall perform the following in addition to standard GCIC procedures:

- a. Any CCPD GCIC Terminal Operator who completed a GCIC action on behalf of another agency shall obtain a departmental case number from E911/Communications by requesting a "Code 4 case number." The Code 4 case number, when used for GCIC actions taken on behalf of other agencies, does **not** require the completion of an *Incident Report* or *Supplemental Report*.
- b. The GCIC Terminal Operator shall complete a *Report of GCIC Action Taken for Other Agency* (refer to Appendix A of this procedure) to document the action taken.

c. Submission, Review & Approval of Forms

For review and approval purposes, forms shall be submitted in the same manner as any other departmental reports with all related GCIC documentation and printouts attached to the form at the time of submission.

- 1) Refer to standard operating procedure *D9: Field Reporting* regarding the proper submission of reports and forms for review, approval and corrections.
- 2) Refer to *section VI.* of this procedure regarding the departmental GCIC validation procedures.
- 3) Approved forms and supporting documentation will be filed and maintained in Central Records & Permits in the same manner as all other departmental reports and/or forms bearing a departmental case number.

C. GCIC Entry Procedures

1. When any vehicle, article, gun, person, etc. is entered into GCIC files, the Entry Worksheet and all printouts will be retained in the Central Watch Office until called for by the officer making the report.
2. The GCIC operator will check the Repossession Listing prior to making an entry for a stolen vehicle. The officer making the report can also do this, but it must be documented in their report.
3. The officer making the report will request the entry by case number and give the Watch Officer their completed report (in person, fax, or email).
  - a. The Watch Officer will then check the report to verify that all information necessary to make an entry is contained in the report prior to making the entry. If necessary, the report will be returned to the requesting officer for correction.
  - b. The Watch Officer will then make the entry and initial the entry.
  - c. The officer requesting the entry is then responsible for either picking up a copy of the entry at the Central Watch Office or ensuring it is faxed to their specific precinct and/or emailed to them by the Watch Officer.
  - d. If the report was completed in the Central Watch Office, the other watch officer working will double check the entry and initial the report.
  - e. It is the responsibility of the officer making the report to ensure the entry is made.

**NOTE:** In cases such as a carjacking, the vehicle will be entered onto GCIC immediately by the terminal operator, without the completed report. The officer must ensure that all required information for the entry is provided to the terminal operator. The report will then be completed as soon as possible and delivered (in person, fax, or email) to the terminal operator.

4. Once the officer obtains their copy of the entry, they will check the information in their report against the entry. The officer must ensure the VIN, tag, caliber/make/model of weapon or serial numbers on the entry are correct. The officer will complete a character-by-character comparison on all supporting documents to verify the information is correct and/or initial their copy of the entry.

5. Any officer completing a recovery report, missing person located report, or notification that another agency has reported a recovery is to ensure the entry has been cleared from GCIC.
6. The only exception to the above procedures is if GCIC is down during the shift in which the report was taken. If this occurs, the report will be left in the Central Watch Office after receiving approval by a supervisor. When GCIC returns to service, the appropriate entry/clear will be made. The report and all printouts will be retained in the Central Watch Office and the terminal operator will notify a supervisor to come review the reports as soon as possible.
7. Supervisors are responsible for checking reports and verifying the appropriate GCIC entry was properly made prior to signing the report. Any supervisor checking an *Incident Report* that includes an entry will complete a character-by-character comparison of all supporting documents and/or initial the copy of the entry to verify it was checked and is accurate.
8. The timely correction of NCIC/GCIC errors are critical to the law enforcement community. Upon being notified by a supervisor or the TAC, any and all corrections must be completed immediately, unless circumstances are beyond the control of the concerned officer(s).
9. Any person under the age of twenty-one (21) requiring entry into GCIC are to be entered immediately, but not later than two (2) hours after obtaining all required information for the entry. Officers will complete their report and deliver (fax, email, or in person) the report to the Central Watch Office as soon as possible so the entry can be made.

## VI. VALIDATION PROCEDURES

### A. Responsibility

The GCIC/UCR Unit is managed by the TAC who serves as the Department's liaison between the Chief of Police and the GCIC for operational matters, and between the Chief of Police and the Clayton County CJIS. The TAC is responsible for ensuring the accuracy of Uniform Crime Reporting (UCR) and validations data submitted to the State of Georgia on a monthly basis, and compiling records and information necessary for GCIC/UCR audits.

### B. General Procedures

The following procedures are performed by the Terminal Agency Coordinator (TAC) to participate in the CJIS Validation Program.

1. Notification of number of records to validate is emailed to the TAC forty-five (45) days before due date.
2. The TAC will retrieve the GBI-GCIC Validation List from the GCIC CJIS Launch Pad.
3. The TAC will prepare the GCIC/NCIC record *Validation Report* via Records Management System (RMS).
  - a. The report will include the date of report, offense, case number, NIC number, victim information, the serial/VIN, license plate number and other information, as applicable.
  - b. Each NIC number will be queried as well as a Drivers Query (DQ) and will be attached to the *Validation Report* as well as verified for accuracy.
  - c. Each victim will be contacted by phone and the GCIC/NCIC *Validation Report* will be marked according to the response. The *Validation Report* will then be signed by the person making contact.



4. Based on the best information and knowledge available, the entering authority will then decide to retain the original entry and/or modify or cancel the entry. The GBI-GCIC/NCIC *Validation Report* will then be marked as is, modify, or cancel respectively.
5. Validation is completed on the GBI CJIS Validation website prior to the GBI requested due date to avoid failure to purge.
6. Due to the volume of records to validate and process, the GCIC/UCR Unit is working on two (2) months of validation records, current month and next month.
7. The CCPD does not validate or store records for other agencies.
8. Missing Persons and Missing Juvenile
  - a. Check Unit case file, including CID case file, to review *Incident Report* and determine if information is valid, accurate, complete, and current.
  - b. Check with the lead detective to determine if the subject is still missing/being sought, and to ensure additional information is being sought. (e.g., social security number, blood type, jewelry, fingerprints). If the person was found, the Central Watch Office will be notified for removal from GCIC. The reporting officer will verify such removal.
  - c. An attempt to obtain medical and dental records must be made within sixty (60) days of the missing person entry.
  - d. Contact the complainant to determine if the missing person remains missing and obtain any additional information that will make the record entry more complete.
  - e. Complete a "QM" inquiry and compare all fields (Including the ORI field) character-by-character against all supporting documentation including investigative case files.
  - f. Complete a "DQ" Driver License and "IQ" Criminal History files to obtain any additional information that can make the record more complete.
  - g. Inquire into local files or other resources to obtain additional information that can make the entry more complete.
  - h. Modify any incorrect information if possible or cancel and re-enter the record with the correct information.
  - i. Add any additional information to the entry and cancel any invalid record entries. Another officer and/or supervisor must then check any additions or modifications to ensure the record is complete and accurate, by completing a character-by-character comparison of all supporting documentation.
  - j. Validate record in the On-Line Validation System.
  - k. A *Validation Checklist* will reflect the status and be placed in the Unit's case file.
9. Stolen Vehicles and Serial Numbered Property
  - a. Check Unit case file, including CID case file and RMS, to review the Incident Report to determine if information is valid, accurate, complete, and current.
  - b. Complete a "QV" (or QG, QB, QS) inquiry and compare all fields (including the ORI field) character-by-character against all supporting documentation including the assigned detective's case file.
  - c. Complete an "NAQ" inquiry for all stolen cars, trucks, vans, ATV's, and motorcycles that were manufactured after 1980 and are entered with a VIN.

- d. If the NAQ indicates that an insurance company has taken over ownership of a stolen vehicle, contact the insurance company at the phone number listed on the response to determine if the vehicle has been recovered.
  - e. Complete a "RQ" to ensure the validity of the registration and/or if the vehicle has been registered to a different owner.
  - f. Contact the complainant to see if the stolen vehicle or stolen serial numbered property has been recovered or if ownership has changed.
  - g. Add any additional information to the record, modify incorrect information if possible, or cancel and re-enter with the correct information. Cancel any invalid record entries. Another officer and/or supervisor must then check any additions or modifications to ensure the record is complete and accurate, by completing a character-by-character comparison of all supporting documentation.
  - h. Validate record in the On-Line Validation System.
  - i. A *Validation Checklist* will reflect the status and be placed in the Unit's case file.
10. Identity Theft
- a. Check Unit case file, including CID case file and agency RMS, to review the *Incident Report*, including all *Supplemental Reports* to determine if information is valid, accurate, complete and current.
  - b. Review the required consent form completed by the victim to allow the entry into NCIC making sure all information is accurate and that a password has been established by the victim to be included in the identity theft record entry.
  - c. Complete a "DQ" Driver License and "IQ" Criminal History files to obtain any additional information that can make the record more complete.
  - d. Contact the victim of the identity theft to ensure the case remains active and that victim wishes to remain in the identity theft NCIC file.
  - e. If the victim wishes to be removed from the file, a written removal request must be submitted to the agency by the victim.
  - f. Add any additional information to the record, modify incorrect information if possible, or cancel and re-enter with the correct information. Cancel any invalid record entries. Another officer and/or supervisor must then check any additions or modifications to ensure the record is complete and accurate, by completing a character-by-character comparison of all supporting documentation.
  - g. Validate record in the On-Line Validation System.
  - h. A *Validation Checklist* will reflect the status and be placed in the Unit's case file.

## VII. CENTRAL WATCH OFFICE PROCEDURES

- A. The Central Watch Office will normally (depending on workforce) have two (2) employees assigned.
- B. All walk-ins to the Central Watch Office requesting a report will be handled at that location. When there are two (2) employees assigned, the second employee will have primary responsibility to handle the "window" at the Central Watch Office.

- C. The Central Watch Office will be responsible for releasing vehicles, whenever the Records Unit is closed. Refer to standard operating procedure *D31: Vehicle Impounds and Release*.
- D. Both employees must be proficient with Clayton County Parking Ticket procedures, specifically how to convert a civil parking ticket to a traffic citation.
  - 1. Employees utilize option forty-seven (47) on the “Green Screen” to access the parking ticket screen.
  - 2. They then utilize option seventeen (17) to access the conversion screen to suspend the timing on a civil ticket. This screen will also advise the employee if a case number has already been assigned.
  - 3. They will obtain a case number, if one has not been assigned, and issue a *Uniform Traffic Citation* (UTC).
    - a. The Watch Officer will issue the citation with the current traffic court date.
    - b. They will place the name, employee number, and agency of the individual who initially issued the citation in the remarks section.
    - c. They will issue the yellow copy to the individual requesting a court date and turn the rest of the ticket in with their paperwork.
    - d. The employee must ensure all information is properly entered into the parking ticket system.
  - 4. Any questions and/or problems should be directed to a concerned supervisor or DoIT.
- E. Both employees will be familiar with and able to enter vehicles into the vehicle impound/repossession database.
- F. A Sector 4 supervisor is responsible for checking the reports in the Central Watch Office at least once per shift, unless call volume does not permit it.

## **VIII. BUILDING SECURITY AND ACCESS**

- A. Visitor Information Requirements
  - 1. Employees shall maintain a calm and professional demeanor, and willing to help any person in need of assistance at headquarters.
  - 2. Employees will attempt to obtain the following information from visitors, when they request to speak with personnel inside restricted areas of headquarters:
    - a. The purpose of their visit;
    - b. If they spoke with personnel, prior to their arrival, if so, provide information (e.g., rank, name(s), division and/or unit);
    - c. If they have an appointment, or were they provided with instructions;
    - d. Their name, and agency/business name (if applicable);
    - e. Their case number and/or type of incident (if applicable); and
    - f. Any additional information, as deemed necessary.
  - 3. Once pertinent information is obtained, employees shall let the visitor know they can wait in the lobby or atrium area, while their request is being processed.

4. Next, employees shall make contact with the requested employee, division and/or unit, and instruct them to come to the front lobby area, so they can meet with the visitor and/or escort them back to the appropriate area.
  5. **Visitors that enter any restricted areas of headquarters shall be escorted by a Department employee at all times, until they are escorted back to the lobby.**
- B. It is the escorting employee's responsibility to make sure visitors are escorted while inside the restricted areas of headquarters. At the conclusion of the visit, an employee shall escort the visitor back to the lobby.
- C. Security is every employee's responsibility. When a visitor is discovered inside a secured area of headquarters and they are not being escorted, immediate action must be taken.
1. Non-sworn employees will immediately alert a sworn employee, if they discover an unescorted visitor inside a secured area of headquarters.
  2. Sworn employees who encounter an unescorted visitor inside a secured area of headquarters, will immediately ask the visitor for the purpose of their visit and the name of the employee they are supposed to be with. If the escorting employee cannot be located, the sworn employee, will escort the visitor back to the lobby to wait for their escort and/or further instructions.
- D. Employees that are not required to wear a uniform to work, must wear their identification card on the outermost clothing so that it is visible at all times while they are inside headquarters.
- E. Employees of other public safety agencies not in uniform, County employees (e.g., Building & Maintenance, DoIT), and contract maintenance technicians must wear their identification card(s) on their outermost clothing so that it is visible at all times while inside headquarters.
- F. Training and Other Department Functions Conducted at Headquarters
- Personnel from outside agencies or organizations that are attending training or another function in the Media Room or Community Room will remain in the front lobby. The employee, or authorized designee, responsible for the training or function, will ensure that participants are escorted or familiar with the location of the room that is being utilized.
- The Community/Media Room kitchen area is reserved for Department use only. The kitchen area shall remain locked, when not in use. These guidelines and others, must be met prior to use of the Media/Community Room.
- For additional information regarding Media/Community Room requirements, refer to CCPD SOP *B21: Use of the Media/Community Room*.

## IX. CANCELLATION

- A. This procedure amends and supersedes the following standard operating procedure: *D41: GCIC & Central Watch Office Procedures*, dated November 21, 2022.