Apex Police Department
General Order

Title	Order Number
DCI Operations and Security	1204-20
Effective Date: February 20, 2020	**Amends:** General Order 1204-16
CALEA Standard: 81.2.8, 81.3.1	**Rescinds:**
Reference:	**Pages:** 9

Forms:

F1204 – Visitor's Access Log
F1204a - NCIC Articles Entry
F1204b - NCIC Boat Entry
F1204c - NCIC Gun Entry
F1204d - NCIC Missing Person
F1204e - NCIC Wanted Person
F1204f - NCIC Vehicle Entry
F1204g - NCIC Plate Entry
F1204h - NCIC Vehicle Parts Entry
F1204i - NCIC Securities Entry
F1204j - NCIC Extradition Request

DCI Operations and Security

Purpose

The purpose of this directive is to define the department's role in ensuring compliance with the North Carolina Division of Criminal Information (DCI) operations and security procedures and protocol.

Policy

It is the policy of the Apex Police Department to comply with all security, dissemination, and operator certification requirements in accordance with applicable federal and state laws pertaining to the State Bureau of Investigation (SBI) Criminal Information and Identification Section (CIIS) DCI network information and operations, and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division. (81.2.8)

Definitions

Criminal Information and Identification Section (CIIS) – A branch of the North Carolina SBI Division of Criminal Information (DCI) that maintains North Carolina's statewide computer network for the exchange of law enforcement/criminal justice information.

Criminal Justice Information Service (CJIS) – A division of the FBI that maintains a repository of criminal history records and fingerprint classification records.

National Crime Information Center (NCIC) - A nationwide computerized information system that is operated by the FBI. NCIC provides the capability of nationwide information sharing and data warehousing.

Procedure

Network Diagram

1. The Police Records/IT Manager will ensure that a complete topological drawing depicting the interconnectivity of the department's network to criminal justice information systems and services is maintained in a current status. (SOURCE: CJIS Manual)

2. The network topological drawing will include the following:

    - All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point
    - The logical location of all components (e.g. firewalls, routers, switches, hubs, servers, encryption devices and computer workstations)
        - Individual workstations (clients) do not have to be shown; the number of clients is sufficient
    - "For Official Use Only" (FOUO) markings
    - The agency name and date (day, month and year) the drawing was created or updated

Confidentiality and Release of Information

1. All DCI network users are required to comply with the SBI CIIS DCI Network Personnel Security Agreement. (**SOURCE:** 12NCAC 04H.0301)

    - Any employee who violates CJIS policies and/or misuses DCI network systems is subject to disciplinary action in accordance with General Order 310 – *Disciplinary System and Grievance Procedures.*
    - Additionally, the employee and/or the department may be subject to possible penalties as outlined in North Carolina Administrative Code (NCAC)

Title 12, Chapter 4, for the misuse of CJIS data and/or DCIN terminals and computer systems.

2. DCI network users will not share or use another network user's password. In the event a network user forgets his/her assigned password, the Terminal Agency Coordinator (TAC) or Assistant Terminal Agency Coordinator (ATAC) should be notified immediately to request a password change.

3. DCI network users must keep the DCI network terminal in a position so that information displayed on the screen may not be read or viewed by unauthorized persons.

4. Network users will not release DCI network records by telephone or otherwise, to anyone other than authorized law enforcement or criminal justice personnel.

    - If the requesting person does not meet the authorization criteria, or if it is unknown whether the person is authorized to receive such records, the network users will not release any information.

5. Network users will not broadcast DCI network records information over the police radio unless the information may indicate that an officer or citizen may be in danger from a specific individual. (**NOTE:** Exceptions include the following information pertaining to driving records that may be broadcast over the radio:

    - Prior, current or limited revocation or suspension of driving privileges for Driving While Impaired (DWI) and corresponding date(s)
    - Prior, current or limited revocation or suspension of driving privileges for any other violation and corresponding date(s)
    - License pick up
    - Registered sex offender
    - Gang member

Security (81.3.1)

1. CJIS may only be accessed from a secure computer terminal within the police facilities or from inside a police vehicle.

2. Any application or file that contains CJIS information must be kept out of the view of all visitors.

3. Support personnel, contractors and custodial workers with access to secure locations or areas with controlled access within the police facilities are subject to a state and national fingerprint-based, record check unless escorted by authorized personnel at all times.

4. All other visitors who have not had a fingerprint-based, records check will be escorted while inside the secure portions of the police facility. (**NOTE:** This includes spouses and children of employees.)

5. Sworn law enforcement officers from Wake County agencies who are conducting official law enforcement duties with departmental members are not required to be escorted at all times within the police facility; however, they must comply with facility requirements in accordance with this General Order and other applicable written directives.

6. Form F1204 – *Visitor's Access Log* will be maintained in each police facility and will include:

    - Name of the Visitor
    - Agency of the Visitor (if applicable)
    - Form of Identification
    - Date of Access
    - Time of Entry and Exit
    - Purpose of Visit
    - Person Visiting
    - Badge Number
    - Badge Returned

    NOTE: All visitors, regardless of their status, are required to be signed-in and out by a member of the department.

7. Visitor's Access Logs are located at the Records Section window, or a similar location in other police facilities.

8. Visitor's Access Logs are to be reviewed on a quarterly basis by the Police Records/IT Manager or his/her designee.

    - The purpose of the documented review is to ensure visitor sign-in and out procedures are being followed and accounting for all identification badges.
    - Documentation of the review will be forwarded to the Chief of Police through the chain of command for review and approval.

9. Visitor's Access Logs will be forwarded to the Administrative Division when completed and reviewed, and must be kept on file for a minimum of 12-months. These records may be subject to review on a bi-annual basis by the FBI and/or the SBI CIIS Audit Team.

Identification/Access Badges/Cards

1. All support personnel, contractors and custodial workers who have had a fingerprint-based, records check may be issued an identification card, which will include their name, company name, photograph, and issue date.

    - All issued identification cards must be returned to the Administrative Division Commander once authorized support personnel, contractors and custodial workers are no longer providing authorized services to the department.
    - The Administrative Division Commander is responsible for the proper destruction of identification cards.

2. The Administrative Division Commander will ensure a list is generated and maintained to document the names of support personnel, contractors, and custodial workers who are authorized to access the police facility and who have been issued an identification card. Additionally, the list will include the Town of Apex employees authorized to access the police facility as outlined in this General Order and who have been issued an access card. The list will include, at a minimum, the following information:

    - Name of authorized person
    - Company name/Town of Apex employee
    - Whether issued an identification card or access card
    - Identification card issue date

3. A copy of the list will be maintained within the Communications Center and Records Section, and will be used by departmental employees to verify that the person presenting an approved identification card, as outlined in this General Order, and requesting access to the secured area of the police facility are authorized.

4. Sworn officers from Wake County law enforcement agencies who are conducting official law enforcement duties with departmental members will be given a temporary green LEO “No Escort Required” identification badge.

5. All other visitors will be given a temporary blue “Escort Required” identification badge.

6. Visitors are required to wear their identification badge visibly on the outermost garment at all times while in the secured portion of the police facility.

7. All support personnel, contractors, and custodial workers are required to wear their issued “No Escort Required” access card, and identification card visible on the outermost garment at all times while in the secure portion of the police facility.

- Authorized, contractors, and custodial workers will return issued "Contractor" access cards to the Communications Center staff prior to leaving the police facility.

8. All visitor identification badges outlined in this General Order must be returned to the Records Section area, or in other police facilities, the location where the log is maintained, at the end of their visit.

9. Town of Apex employees authorized by the Chief of Police and who have had a fingerprint-based, records check may be issued an access card to access authorized areas within the police facility unescorted.

    - Authorized Town of Apex employee may include:
        - Director of Information Technology
        - Facility maintenance personnel
        - Other Town of Apex employees who provide a specific service to the department and have a demonstrated need for access
    - All authorized Town of Apex employees are required to wear their issued access card and Town of Apex identification card visible on the outermost garment at all times while in the secure portion of the police facility.
    - All issued access cards must be returned to the Administrative Division Commander once the Town of Apex employee is no longer providing authorized services to the department, no longer assigned to the approved position, or when requested by the Administrative Division Commander or the Chief of Police.

10. Annually, as part of the documented review of all computers and authorized users and password audit as outlined in General Order 403 – *Computer/Software Security,* the Police Records/IT Manager will:

    - Verify the established list of authorized support personnel, contractors, custodial workers and Town of Apex authorized employees is current and up-to-date
    - Verify the personnel information, employment status and photo is up-to-date for all authorized support personnel, contractors, custodial workers and Town of Apex authorized employees
    - Ensure issued identification cards are valid and accounted for
    - Ensure issued access cards are accounted for
    - Ensure identification cards are being surrendered as outlined in this General Order

Sanitization and Disposal Requirements

1. The department follows the electric media sanitization and disposal requirements as outlined in the US Department of Justice, FBI CJIS Security Policy Manual.

2. The Police Records/IT Manager or designee will sanitize (i.e., overwrite at least three times or degauss) electronic media prior to disposal or release for reuse by unauthorized individuals. For inoperable electronic media, it will be destroyed (i.e. cut up, shredded, etc.). All approved sanitization or destruction methods will be witnessed or carried out by authorized personnel.

3. The Police Records/IT Manager is responsible for maintaining written documentation of the steps taken to sanitize or destroy electronic media.

NCIC Entries

1. Any request for NCIC entries must be submitted to the Communications Center along with the appropriate NCIC entry form that coincides with the entry type.

    - F1204a - *NCIC Articles Entry*
    - F1204b - *NCIC Boat Entry*
    - F1204c - *NCIC Gun Entry*
    - F1204d - *NCIC Missing Person*
    - F1204e - *NCIC Wanted Person*
    - F1204f - *NCIC Vehicle Entry*
    - F1204g - *NCIC Plate Entry*
    - F1204h - *NCIC Vehicle Parts Entry*
    - F1204i - *NCIC Securities Entry*

2. Under no circumstances should a Telecommunicator fill out the entry paperwork for the officer; these forms should be typed by the officer to avoid any entry errors. All NCIC Entry paperwork will be maintained within the Communications Center in accordance with applicable laws, rules and regulations.

Wanted Persons

1. Except when otherwise prescribed by federal law or when documentation exists to support delayed entry, the National Crime Information Center (NCIC) mandates that all warrants be entered immediately when the conditions for entry are met. Warrant entry is the responsibility of the case officer and must take place within three days (72 hours) following receipt of the warrant.

2. Only a District Attorney or an Assistant District Attorney is authorized to sign and approve an out-of-state extradition. A signed copy of Form F1204j -*NCIC Extradition Request* must be attached to the NCIC entry.

Criminal Histories

1. Any network user running a criminal history will put the requestor's name in the ATTN 1 Field. The network user will also put the OCA Number and reason for running a criminal history check in ATTN 2 Field.

2. All CCHs for employment or volunteer work are to be searched using purpose "Code J". (**NOTE:** This includes police officers, Telecommunicators, civilian positions, volunteers, interns, CAPA team members and Citizens Police Academy applicants.)

3. The Communications Manager or designee will maintain a copy of automated criminal history logs for a period of 12 months from the date produced, and will then destroy them through approved methods (i.e., shred).

    - The destruction of such files is to be notated in the Communications Center Monthly Report.

NICS Query Disposition of Firearms

1. Prior to returning a firearm to the owner or prospective transferee, a *Query Disposition of Firearms – (QDOF)* will be completed to determine eligibility to receive or possess a firearm.

2. When the QDOF transaction has been transmitted, an automatic spin-off of a Query AOC for Criminal Defendant Name (QACD) transaction, will be sent to the NC Administrative Office of the Courts(AOC) database.

3. When the QDOF transaction has been transmitted, and the code in the Citizenship (CTZ) field is NON-US CITIZEN (Code F), an automatic spin-off of an Immigration Alien Query (IAQ) transaction will be sent to Immigration and Customs Law Enforcement Support Center (ICE).

4. If a "hit" is received in NICS utilizing the QDOF, then operators will use the NICS Specific Record (QNR) transaction to receive the full record(s). If after reviewing the record(s) it is determined the individual is ineligible to receive or possess a firearm, the agency will notify NICS of the denial by using the Enter State Denial Notification (NDN) transaction. If the agency should need to overturn the denial, NICS will be contacted by using the State Denial Overturned Message (NDO) transaction.

DCIN Security Awareness Training

1. All employees are required to complete DCIN Security Awareness Training at least bi-annually.

    - Newly hired employees will receive initial training during an approved field-training program (i.e., CTO, FTO Program) or an appropriate Civilian Employee Orientation Training Program.
    - The department's primary Terminal Agency Coordinator will coordinate with the Administrative Division Commander (as the department's Training Coordinator) to ensure this training is completed, as required by the North Carolina SBI.
    - This training requirement will be satisfied through use of the CJIS Training Portal
    - All training records will be maintained in accordance General Order 501 – *Training: Organization and Administration*.

    Text in "Green" denotes a significant change in policy

BY ORDER OF:

John W. Letteney
Chief of Police