| DOUGLAS COUNTY SHERIFF'S OFFICE | | Policy and Procedure |
|---|---|---|
| **Specific Policies**<br>**CCIC & NCIC Usage** | | **P&P-B-133** |
| Effective Date: 01-19-21<br>Supersedes: 02-15-18 | Approval: Sheriff | Number of Pages: 3 |
| References: | Reevaluation Date:<br>Annually | Standards: |

## I. POLICY

Colorado Crime Information Center (CCIC) is a computer for law enforcement purposes. It is a component of the statewide computer system originating in Denver, connected with the National Crime Information Center (NCIC) in Washington, D.C. The computer is used to obtain checks on wanted persons, vehicles, guns, and articles; as well as to send messages to agencies in the United States and to enter UCR / NIBRS statistics.

## II. PROCEDURE

When required by job function, and upon request of the member's supervisor or their designee, members of this agency will be assigned an OSN number by the CCIC Coordinator.

Any member of this Office that may come in contact with CCIC/ NCIC information will have a valid CCIC OSN or have a CCIC Security Awareness login. The CCIC Coordinator can be contacted for a CCIC Security Awareness Login.

All users with an assigned OSN or CCIC Awareness login will test every two years following their last certification, (per CJIS Policy). Users who fail to complete the testing process and let their CCIC/CJIS credentials expire will have their proximity card deactivated and will not be allowed to have access to any secured areas in the Sheriff's Office unless escorted by a member of the Office with current CCIC/CJIS credentials. The expired user will not be allowed any CCIC information or department reports containing CCIC information per CJIS Security policy and may face disciplinary procedures. Once the user has successfully completed the required training and with the approval of his or her immediate supervisor, the user's access will be reinstated. The Test Activity report and Certificates are available to the CCIC Coordinator in the CJIS Testing portal.

Individual CCIC / NCIC operators / users shall maintain security of the system. This security is required by State and Federal regulations. CCIC / NCIC operators make available to law enforcement personnel the most complete and accurate information possible, utilizing the various files available through the CCIC / NCIC system.

Information received for CCIC / NCIC may be released to criminal justice agency personnel **only.** Release to non-criminal justice agency personnel may result in loss of the operator's security number (OSN) and authority to use the system. No pictures of CCIC / NCIC information are permissible.

It is the responsibility of each member to be aware of every change or addition in procedures concerning the operation of the CCIC computer. This is possible by reading the CCIC newsletter available through the CJIS Portal Launch Pad. The newsletter advises of any additions, deletions, or changes in the system. The CCIC Coordinator may distribute the CCIC newsletter to interested members in copy form upon request.

## III. DEPARTMENT MEMBER ACCESS

CCIC/NCIC may be accessed or released as follows:

A. Members may access or otherwise obtain records or CCIC/NCIC information and department files only in accordance with their official duties.

B. A member may not access confidential information until a background investigation has been completed on the member and approved and until he/she has completed all required training.

C. CCIC/NCIC shall be used solely for the purpose for which it was obtained.

    1. Utilization of the CCIC/NCIC system is authorized for criminal justice purposes only as defined in 28CFR20.

D. Members may not use CCIC/NCIC information in any unauthorized manner, for any unauthorized purpose, or disclose CCIC/NCIC information to any person who is not entitled to the information. This includes using CCIC/NCIC for personal gain. Examples of misuse would be:

    1. Querying one's own record.
    2. Querying peers, souses, ex-spouses, romantic interests
    3. Querying elected or public officials
    4. Curiosity queries – queries made for personal knowledge, not a law enforcement purpose
    5. Giving out copies of CCIC/NCIC criminal history information to the public.
    6. Any other personal reason

E. Unauthorized access or release of information may subject the member to criminal prosecution.

    1. Members violating this policy may also be subject to administrative action pursuant to the Policy and Procedures Manual.

F. Members are responsible for maintaining the confidentiality of their Operator Security Number (OSN) and password.

G. Members are responsible for adhering to the CCIC Declaration of Understanding (DOU) to which the user agrees prior to taking their user certification test.

## IV. SECURITY INCIDENT REPORTING/HANDLING

When an allegation of misuse is reported, the Colorado Bureau of Investigation (CBI) and Internal Affairs will be notified. These notifications will be completed that business day. If the allegation occurs during non-business hours the notification will be made on the next normal business day. Once the investigation is completed CBI will be notified of the case disposition.

## V. ACCOUNT MANAGEMENT

The agency CCIC Coordinator or their designee shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The CCIC Coordinator or their designee shall validate information system accounts at least annually and shall document the validation process. Account management includes the identification of account types, establishment of conditions for group membership, and assignment of associated authorizations. The CCIC Coordinator or their designee shall identify authorized users of the information system and specify access rights/privileges. The CCIC Coordinator or their designee shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The CCIC Coordinator or their designee will be responsible for account creation or cancellation when notified of:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

## VI. LOCAL AGENCY SECURITY OFFICER (LASO)

The agency LASO is responsible for ensuring the security of CJI per the current CJIS Security Policy. Specifically, the LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

By Order of the Sheriff