OFFICE OF INVESTIGATIVE SERVICES
POLICY & PROCEDURE #380

GCIC/NCIC AND CRIMINAL HISTORY RECORDS CHECK

GCIC/NCIC POLICY STATEMENT:

I. AUTHORITY

A. PURPOSE

To define terminology and establish authority over CJIS network systems.

The Georgia Crime Information Center's Policy Manual, the Georgia Crime Information Center's Council Rules and the Georgia CJIS Network Operations Manual are referenced, and hereby adopted, and made part of the Office of Investigative Services Policy and Procedure Manual.

B. USAGE

CJIS Network computers and data will be used solely for the purpose of authorized inquiries and dissemination of CJIS Network information.

C. CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

The CJIS network has four major components:

1. The terminal operated by criminal justice agencies in Georgia.
2. Records and files accessed by those terminals.
3. Computers and associated equipment used by GCIC and local or regional computer centers which are connected to the Georgia CJIS network.
4. Federal, state, and local criminal justice agency employees who operate, support, use and benefit from the CJIS network.

D. NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (NLETS)

The National Law Enforcement Telecommunications System provides access to NLETS files and criminal justice agency terminals and files in other states.

E. INTERPOL

Interpol is an information exchange agency between domestic and international law enforcement agencies. Interpol forwards your message to an international agency and relays a response back to your agency. To contact Interpol, send an administrative message to DCINTER00 or call 202-616-9000.

F. NATIONAL CRIME INFORMATION CENTER (NCIC)

The National Crime Information Center, a division of the Federal Bureau of Investigation (FBI), maintains files and records, which are available nationwide. The Georgia Bureau of Investigation (GBI) is the NCIC control terminal for Georgia.

II. TERMINAL AGENCY COORDINATORS

A. PURPOSE

To develop a section in the Office of Investigative Services devoted to the supervision, accuracy, custody, and control, and verification of all GCIC paperwork and entries.

B. TERM DEFINED

A Terminal Agency Coordinator (TAC) is an employee designated by the Office of Investigative Services (OIS) Director to serve as liaison between the OIS Director and the Georgia Crime Information Center for CJIS network related matters.

C. APPOINTMENT

It shall be the responsibility of the Office of Investigative Services Director to appoint Terminal Agency Coordinators. The OIS Agency shall ensure that proper TAC training is administered within 60 days of appointment.

D. TAC MINIMUM STANDARDS

A person must meet the following requirements to be eligible for appointment as Terminal Agency Coordinator.

a. Have an acceptable and satisfactory performance evaluation as based on the last year prior to appointment as TAC.
b. Have made no serious errors or violations of GCIC rules and regulations within the last year.
c. Overall terminal errors maintained at an extremely low rate.
d. Demonstrate an ability to handle extra duties and goals.
e. Have an above average understanding of the GCIC Operations Manual.

III. GCIC USER AGREEMENT

A. PURPOSE

The user agreement between the DHR/Office of Investigative Services and the Georgia Crime Information Center states the duties and responsibilities of criminal justice agencies and GCIC concerning the use of the GJIS network, training, and compliance with state and federal laws and rules.

B. LOCATION OF AGREEMENT

The user agreement between the DHR/OIS and GCIC will remain on file with the Office of the Division Director.

IV. HIT COMFIRMATION REQUESTS

A. PURPOSE

To establish HIT confirmation request guidelines.

B. HIT CONFIRMATION REQUEST DEFINED

1. A HIT confirmation request is a process that must be initiated by the Inquiring agency, after receiving a positive hit response, whenever the information in a response describes the person or property in question and the inquiring agency has control of the person or property.

2. There are two types of HIT confirmation requests:

    a. Urgent-Within 10 minutes
    b. Routine-Within 1 hour

C. RECEIPT OF HIT CONFIRMATION REQUEST

HIT confirmation requests will be received via GCIC computer printouts. It shall be the responsibility of the console operator, assigned to that terminal, to check the printer for incoming HIT confirmation requests.

D. PROCESSING OF HIT CONFIRMATION REQUEST

Once a HIT confirmation request is received, the receiving operator will immediately attempt to verify the record by accessing the GCIC hardcopy files, which will be secured in the communications center.

E. RESPONSE TO HIT CONFIRMATION REQUEST

A response must be sent to the requesting agency by the time specified on the type of hit received. Operators will respond with:

1. Confirmation of the HIT – this will advise the agency that the HIT is accurate, current, and valid.
2. Deny the HIT – this will advise the requesting agency that the information in the HIT message is no longer valid or that it does not match our current GCIC file entries.
3. More time needed – if more time is needed to obtain or review the case file to determine the validity of the record, respond to the requesting agency specifying the amount of time needed.

F. METHODS TO RESPOND TO HIT CONFIRMATION REQUEST

An Operator may respond to a request for HIT confirmation by:

1. Telephone
2. Appropriate GCIC computer response

A GCIC computer response will be sent in all HIT confirmation requests regardless if the telephone was used to verify the record with the requesting agency.

V. RELEASE OF CRIMINAL HISTORY

The purpose of this order is to provide guidelines for the release of Criminal History Information as required by Federal and State Laws.

I. RULES

A. Information may be shared with other criminal justice agencies and their personnel by any means necessary including radio transmissions.

B. Information released to other agencies must be entered on a log showing the name of the agency, date, person supplying the information, reason for dissemination, and name of person receiving information.

C. Other individuals or companies may receive criminal justice information only by an agreement with GCIC or court order.

D. No employee of this office shall otherwise confirm or deny the existence of criminal history information on any individual.

E. Requests for Driver's License or Criminal History information are to be submitted in writing to the Special Projects Unit on the **GCIC Driver's License Inquiry Request.**

F. The OIS employee is responsible to keep all CHRI documents and Driver's License information out of public view and secure them in a secure storage area, when not in use. Upon completion of the investigation, all CHRI and Driver's License documents are to be destroyed.

II. COMPLIANCE

A. This order pertains to all employees of the Office of Investigative Services.

B. Any employee violating the above rules may be subject to Federal and State Criminal penalties as well as disciplinary action.

C. If any employee has a question concerning the release of any specific information, he/she shall request instructions from the Division Director.

D. Each employee shall sign a **GCIC Employee Awareness Statement**, which will be kept on file in The Special Projects Unit.

III. RESPONSIBLITIES OF THE GCIC TERMINAL OPERATOR

A. The Terminal Operator is responsible to adhere to all GCIC rules, policies, and procedures.

B. The Terminal Operator is responsible to log all criminal and drivers history requests in the log book kept with the terminal.

C. The Terminal Operator is responsible to list the Requestor's Name/Operator's initials in the "ATN" field for all criminal and drivers history requests.

VI. RECORDS SECURITY DURING NATURAL AND/OR MAN-MADE DISASTERS

A. INTRODUCTION

In the event of a natural or man-made disaster, including, but not limited to, a flood, fire or civil unrest, the potential for the destruction of OIS records is high. The purpose of these procedures is to safeguard Bureau records.

B. RESPONSIBILITIES OF THE IIC, SPECIAL PROJECTS UNIT

1. The IIC of the Special Projects Unit is responsible to ensure that records maintained by the Bureau are secured and not in danger of being damaged or destroyed during civil unrest.

2. In the event that Bureau records are in danger of being, or have been damaged and/or destroyed by flood or fire, the IIC of the Special Projects Unit is responsible to immediately notify the Director of the Office of Investigative Services. If necessary, an Investigator shall be stationed in the area to secure said records until the Director responds.

3. The IIC of the Special Projects Unit is responsible for taking the necessary steps to ensure all records are secured on site and that said records are removed to another location where they can be secured until such time they can be returned and secured within the Office of Investigative Services.

CRIMINAL HISTORY RECORDS CHECK:

All DHR applicants/employees are required to disclose felony convictions on Applications for Employment and convictions and/or pending charges on State Security Questionnaire Loyalty Oath Forms. Refer to DHR Personnel Policy #504.

All OIS employees are further required to present fingerprint cards and are subject to a criminal history records check. Prior to consideration for employment, all OIS applicants are asked to sign the following forms:

- **Criminal History Record Information Consent Form** (Law Enforcement Agency Employees and Sworn Officers – Purpose Code E)

-OR-

- **Criminal History Record Information Consent Form** (Law Enforcement Officers – Purpose Code J)

-AND-

- **Authorization and Release to Obtain information**