RESPONSIBILITIES OF THE TERMINAL AGENCY COORDINATOR (TAC)

The Terminal Agency Coordinator assigned by your department or Agency Head will be responsible for ensuring that all policies and procedures are followed by your agency. This individual must become familiar with all aspects of the operations of NCIC, NLETS and the MJIC Network.

As the CJIS Systems Agency, we are responsible for training and certifying you TAC. In turn you TAC is responsible for training and certifying all personnel with you agency in accordance with MJIC policies. Law enforcement agencies are faced with numerous liabilities, including the operation of the MJIC Network. The individual that is assigned as you TAC can lower the liability for you agency by ensuring that all policies are met, or can increase you liability if these responsibilities are not enforced.

To help you in determining the assignment of you TAC, some of their responsibilities are listed below. These responsibilities are some major areas evaluated during the FBI-NCIC/MJIC audit process.

Maintain System Integrity

Accuracy	-	Double check all entries and modifications made into NCIC.
Timeliness	-	Ensure prompt entry and modification of all NCIC records.
Completeness	-	Ensure that all available information is included in the NCIC record.
Quality Control	-	Routine examination to ensure that errors are corrected.

Validation

Ensure all records contained on validation listings (furnished to you each month) are complete, accurate and still outstanding. Complete instructions are provided to the TAC with each validation listing.

Criminal History

Ensure NCIC – CCH policies required by Federal Statutes are being properly followed. Explicit instructions on NCIC – CCH policies are defined in the CCH-III section of the NCIC Manual. Certain federal mandates such as maintaining a III log, Policies regarding secondary dissemination and authorization policies are critical elements in preventing high risk liability.

Hit Confirmation

Ensure that the TEN (10) Minute hit confirmation policy is understood and complied with by all personnel.

System Security

Ensure that the terminal in located in a secure area and that access is limited to authorized personnel only.

Training and Certification

Provide training and certification to all personnel (including sworn and non-sworn) who operate the MJIC terminal. This training and certification must occur within six (6) months of employment.

Provide MJIC Quality Control staff with documentation verifying that training and certification has been provided to necessary personnel.

PERSONNEL SECURITY – Background Screening

NCIC policy states that your agency should conduct appropriate background investigations on all MJIC/NCIC terminal operators, both full-time and part-time employees. Based on this clearly defined policy, listed below are the minimum steps necessary to comply with this NCIC requirement

1. Fingerprint, on your agency's applicant fingerprint card, all employees that will operate your MJIC workstation.

2. Indicate on cards in the block "Reason Fingerprinted" that the reason is "Law Enforcement Employment / Terminal Operator".

3. Forward the fingerprint card to the MS Criminal Information Center (CIC), noting the date mailed to CIC.

4. Run a Wanted Person check on you MJIC workstation and place the reply in the personnel file. IF you received a "Hit", take appropriate action.

5. When CIC returns the fingerprint card and their findings, study the report and decide what action to take.

6. If the response is a non-ident or no record, forward a copy of this report along with "Terminal Operator Authorization' form to MJIC.

7. If the fingerprint card check response is a "Hit" or a criminal history exists, evaluate the history and if the past arrest and convictions do not, in you opinion, fall within the "serious misdemeanor or a felony" forward copy of RAP sheet with "Terminal Operator Authorization" form to MJIC.

8. If in step 7 (above) you have questions about your employee's record and your agency would like to proceed with certification, forward to MJIC the fingerprint card submitted to CIC and a copy of the RAP sheet along with detailed explanation of why this subject's employment and certification is requested.

9. DPS/MJIC will review documents supplied by requesting agency and a written opinion will be returned to requesting agency.

The above recommended steps should be easy to follow on new employees. However:

What about existing staff?

It would be in the best interest of the MJIC/NCIC Network that all workstation operators backgrounds be screened. You should follow guidelines defined in steps 1 – 5 above. It is imperative that your personnel records reflect that each operator has been screened. MJIC and NCIC Auditors will request evidence that these backgrounds have been conducted.

What happens with a fingerprint check reveals a record?

Follow the instructions listed in step 8 (above).

What about terminal operator transferring from another agency?

Fingerprint cards should be submitted as though they were a new employee.

The steps listed above outline the recommended procedures, however, you may wish to apply additional requirements. MJIC believes that at a minimum, these nine steps must be followed. If you have any questions please contact MJIC at (601) 933-2600 or (601) 933-2651.

DISSEMINATION OF INFORMATION

All data obtained via the MJIC network is confidential sensitive data and is for use by law enforcement or criminal justice agencies only and only for official purposes. This information must not be disseminated outside of the law enforcement or criminal justice community. Violation of this policy is addressed by state and federal laws and can result in immediate removal from the network. (State: Section 45-27-1 through 45-27-17; Federal: CFR, Title 28, Part 20, Subpart A).

III – CRIMINAL HISTORY – DISSEMINATION

Due to the highly sensitive nature of III information, NCIC has established specific policies that must be followed by criminal justice agencies in accessing the disseminating III information.

1. Due to variance in state laws and policies, the III cannot be used for licensing purposes, and cannot be used for non-criminal justice employment purposes.

2. III shall not be used for remotely accessing a record to be reviewed and/or challenged by the subject of the record. Record request for this purpose must be submitted in writing to the FBI Identification Division or the state of record.

3. Copies of criminal history data (III) obtained on the network must be afforded security to prevent any unauthorized access to or use of that data. MJIC requests that this data be destroyed (burned or shredded) after use.

4. A log of criminal history inquiries must be maintained for a minimum of one (1) year. This log must contain at a minimum, the name of the individual making the request for the record, the operator making the inquiry, the specific individual being inquired upon, and the date and time of the inquiry.

III STORAGE AND DESTRUCTION

III records must be maintained in a secure records environment. Such storage of records will be retained for extended periods only when the III records are key elements for the integrity/utility of the case files/criminal records files where they are retained.

When retention of III records is no longer required, final disposition will be accomplished in a secure manner so as to preclude unauthorized access/use.