

**ARKANSAS CRIME INFORMATION CENTER
SYSTEM SERVICE AGREEMENT**

with the

This Agreement is between the Arkansas Crime Information Center, hereinafter referred to as ACIC, and the _____, hereinafter referred to as the User Agency. The purpose is to specify the standards and responsibilities of both ACIC and the User Agency in the operation and use of ACIC services.

ACIC agrees to provide those computerized information services authorized by Arkansas law plus access to the National Law Enforcement Telecommunications System (NLETS) and the FBI's Criminal Justice Information Services (CJIS), which includes the National Crime Information Center (NCIC), or their successors.

The User Agency agrees to abide by ACIC System Regulations, as well as FBI CJIS and NLETS rules and regulations, which are hereby referenced and made a part of this agreement. User Agency specifically agrees to abide by the CJIS Security Policy (see Attachment A). If at anytime ACIC, NCIC/CJIS, NLETS security policies are found to be in conflict, the more stringent policy must be followed.

1. DEFINITION

"Access Device" and "Interface System" refer to computers, workstations, local area networks (LAN's), mobile data terminals (MDT's), mobile data computers (MDC's) or other devices that are used to retrieve or enter data through the ACIC communications network.

2. ACCESS AND USE OF INFORMATION

The ACIC system is restricted to serving the informational needs of governmental criminal justice agencies and others specifically authorized by law. The User Agency agrees that all access to the ACIC system, access devices, and use of information from it, shall be in compliance with state and federal law, as well as, ACIC and FBI CJIS policies and regulations.

Access may be granted to noncriminal justice governmental agencies and private contractors pursuant to a specific agreement for the purpose of providing services for the administration of criminal justice. The agreement must comply with the "CJIS Security Policy" and must incorporate the FBI's "Security Addendum". The agreement, and any subsequent modifications to the agreement, must be approved by ACIC prior to execution. The User Agency agrees to immediately provide ACIC with a copy of such agreement(s) along with an immediate notice and copy of any future amendments thereto.

3. SECURITY

The User Agency agrees that all security requirements defined in ACIC and FBI CJIS policies and regulations will be met. The User Agency agrees to limit access to its own employees and other governmental criminal justice officials with a specific right and need to know. Under no circumstances will non-criminal justice personnel or personnel not under the management control of the User Agency be allowed access to ACIC provided products and services. The User Agency agrees to access and use information from ACIC for official criminal justice purposes. Non-authorized use, under Arkansas Code 12-12-212 and 12-12-1002(b), is a felony. Misuse of the ACIC system, and/or information obtained from it, may be a violation of other applicable state or federal laws.

State and national fingerprint-based record checks must be conducted within 30 days upon initial employment or assignment for all personnel, including appropriate IT personnel, vendors, and service providers having access to ACIC systems information. Appropriate background investigations must be conducted on personnel with access to ACIC record information, including submission of a completed applicant fingerprint card to the FBI CJIS Division through the State Identification Bureau. If a record of any kind is found, access will not be granted until the User Agency chief official, or his/her designee, can review the matter to decide if access/employment is appropriate. If the background investigation reveals that the applicant has entered a plea of guilty, been found guilty or convicted of a crime which is a felony, access will not be granted. This requirement will be interpreted consistent with A.C.A. § 16-90-902.

The following guidelines shall be followed to assure the security of the ACIC and national systems from unauthorized access via the Internet:

- a) Access through the Internet to ACIC information is prohibited unless specifically approved by ACIC. This includes secondary dissemination of ACIC/CJIS/NLETS information through an inadequately protected communications media such as Internet E-mail facilities and remote access file transfer.

- b) Access devices having access to both the Internet and the ACIC system are prohibited unless adequately protected by firewall-type devices or other superior methods. Firewalls should be evaluated against the profiles provided in the documents, "U.S. Government Application Level Firewall Protection Profile for Low Risk Environments" and "U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments". In addition, those access devices with this capability must protect residual ACIC data (e.g., by removal, encryption or erasure) from subsequent Internet access.
- c) Networks in which some access devices have ACIC access and some access devices have Internet access, such as peer-to-peer relationships and mainframes or servers that house web sites, must also be protected by firewall-type devices or other superior methods to prevent access to the ACIC system from the Internet.

4. COMMUNICATIONS LINK

ACIC will, in all cases, provide standard communication facilities as described elsewhere in this document. The communications protocol for the ACIC network is TCP/IP, and the interfaced system must appear to the ACIC system as a Datamaxx workstation. The User Agency specifically agrees to make necessary changes in its system to handle changes to the data stream, headers and/or future transport protocols. It is further agreed that "dial-up"(analog line and ISDN line) access to ACIC, must fully comply with ACIC and CJIS security policy and must be approved by ACIC prior to implementation.

5. RESPONSE TIME REQUIREMENTS

The FBI/CJIS agreement signed by ACIC defines certain processing time requirements on systems handling CJIS information. Transactions run on workstations on the interfaced system must be processed within these time limits. Accordingly, it is agreed that a workstation on an interfaced computer system must receive a response to an inquiry within 22 seconds, with 12 of the 22 seconds allocated to transmission and processing by ACIC and NCIC.

6. ACIC NOTIFICATION

In order to ensure uninterrupted service, the User Agency must provide ACIC with at least 90 days notice of changes to the User Agency's interfaced system. This includes relocation of access devices, communication lines or devices, new acquisitions, additions, deletions, as well as modifications of access devices and the selection or change of support agencies/contractors. The User Agency agrees to complete a detailed description of any proposed interface modifications and submit the description to ACIC for review. The description will be submitted in a form designated by ACIC and will include a network diagram. The User Agency agrees not to modify the interface until ACIC has approved the modification description.

7. USE OF ACCESS DEVICES OR SOFTWARE NOT PROVIDED BY ACIC

When installing new access devices, supplied by the User Agency, it is the responsibility of the User Agency, its support agency or contractor, to make any changes needed to communicate with ACIC. As the ACIC system changes, due to advancements in technology and changes in procedures, the User Agency agrees to make any needed changes to equipment and software it supplies in order to maintain communications with ACIC. ACIC will make a concerted effort to provide advanced notice to the User Agency of planned changes to the ACIC system.

ACIC highly recommends that the User Agency supplied access devices be covered by twenty-four hours a day, seven days a week on site maintenance. Acquisition of such maintenance is the responsibility of the User Agency.

The User Agency acknowledges responsibility for all hardware, operating systems, office automation, etc. supplied by the User Agency. The User Agency agrees that ACIC, or its representative support agency or contractor, can disconnect any User Agency supplied hardware or software it believes is interfering with, or prohibiting, access to the ACIC system. Whenever possible, disconnection of hardware or software will be done after consultation with the User Agency.

The User Agency agrees to designate a technical contact person. This person will be ACIC's contact in the event of technical problems or changes. This person can be an employee of the User Agency, the support agency, or a contractor.

8. EQUIPMENT IDENTIFICATION AND LOCATION

The User Agency agrees that no access device on the interfaced system will be allowed access to ACIC unless it has been individually approved in advance by ACIC. The User Agency further agrees that no changes will be made in the locations or accessibility of any workstation without prior approval being given by ACIC. The User Agency shall maintain a site configuration diagram showing the location of all electronic devices with ACIC access. Additionally, a current listing of all electronic devices and software with ACIC access, including the logical unit identifier, must be maintained. This information shall be provided to ACIC upon request.

9. UNAPPROVED EXPANSION PROHIBITED

The User Agency agrees that no expansion allowing direct access to ACIC will be provided to any agency outside of the User Agency, unless such access is specifically approved by ACIC.

10. AUTOMATED ON-LINE TRANSACTIONS PROHIBITED

The User Agency agrees not to develop and implement batch or automated on-line transactions intended to carry out volume inquiries into the state and national systems unless approved by ACIC. Upon request, ACIC will assist the User Agency with off-line processing of high volume inquiries, such as parking ticket lists.

11. TRAINING

The User Agency agrees to comply with all ACIC training requirements. At a minimum, the User Agency will be responsible for training their own operators on the specific and unique aspects of their own interfaced system. The agency may also assume responsibility for training related to ACIC. However, in that event the agency must: (1) develop a training program that complies with ACIC standards, (2) submit a complete description of the training and related materials to ACIC for approval, and (3) maintain records of all training provided, by individual operator, and submit proof of such training to ACIC in a form prescribed by ACIC.

12. QUALITY CONTROL, VALIDATION AND AUDITS

The User Agency agrees to be responsible for the accuracy, completeness and timeliness of all records entered by it into the state and national files and for compliance with ACIC and CJIS record quality controls, validations and audits. To insure the security of the ACIC network, ACIC will conduct technical audits. These audits may or may not be announced and may involve network monitoring and penetration testing of firewalls and other security features.

13. INDIVIDUAL OPERATOR IDENTIFICATION

The User Agency agrees to require all its operators to regularly use the individual authorization procedure developed by ACIC, or by other means approved by ACIC to provide the ability to trace all transactions back to the individual that initiated the transaction.

14. 24 HOUR OPERATION AND HIT CONFIRMATION

User Agency agrees to limit the ability to enter records to only those workstations that will be manned and operational 24 hours a day, or to implement software or other procedures to handle hit confirmations 24 hours a day for any workstations not operational 24 hours a day. All unmanned devices must be logged off.

15. ACIC HELP-LINE ASSISTANCE

ACIC provides a 24-hour toll-free service number for assistance on technical and procedural problems relating to ACIC and NCIC. The User Agency is encouraged to utilize this service. However, it must be understood that ACIC personnel will not be familiar with unique or specialized features of equipment supplied by the User Agency, therefore the assistance provided by ACIC will be very limited. In addition, if a maintenance contractor or phone company representative is dispatched to the User Agency and the problem is determined to be the fault of the User Agency supplied system, there may be a billable call that will be charged to the User Agency.

16. MOBILE DATA TERMINALS/COMPUTERS

ACIC agrees to provide, when requested, assistance on technical and operational requirements necessary to interface mobile access devices (MDT's/MDC's) to ACIC. The User Agency agrees that MDT's/MDC's installed in vehicles are subject to certain restrictions, including but not limited to:

- a. All MDT's/MDC's accessing ACIC will be operated only by authorized criminal justice personnel and that such mobile devices will be kept as physically secure as feasible.
- b. Access by MDT's/MDC's to computerized criminal history records is prohibited.
- c. All MDT's/MDC's accessing ACIC must provide for user authentication, data encryption, and automatic logoff functions.

17. COSTS

The User Agency agrees to pay monthly fees as prescribed by the ACIC Supervisory Board. The User Agency may enter into cost-sharing agreements with other criminal justice agencies. However, the User Agency agrees to submit one consolidated payment for the total amount of the invoice. It is further agreed that both parties to this agreement are obligated only to the extent that funds are made available to them by their governing bodies.

ACKNOWLEDGMENT

We hereby understand and acknowledge the duties, responsibilities and standards set forth in this document, as well as those documents included by reference, and will ensure that all applicable employees and support agencies and/or contractors have a full understanding of this agreement. We acknowledge that a failure to comply with the conditions of this agreement may result in administrative sanctions or penalties of law.

This Agreement will become effective when executed by both parties and shall remain in force until terminated, amended or replaced. This Agreement may be terminated by either party by providing 30 days written notice to the other party.

USER AGENCY CHIEF OFFICIAL:

ACIC DIRECTOR:

By _____

By _____

Title _____

Title Director

Date _____

Date _____

By _____

Title _____

Date _____